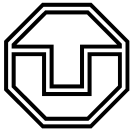




## **Dissertation**

# **Research on the System Safety Management in Urban Railway**

**Tuan Anh Luong**



## **Dissertation**

zur Erlangung des akademischen Grades eines Doktors  
der Ingenieurwissenschaften (Dr.-Ing.)

# **Research on the System Safety Management in Urban Railway**

eingereicht von Tuan Anh Luong

geb. am 18.07.1988 in Vietnam

Betreuer:

- Prof. Dr.-Ing. Jochen Trinckauf

Promotionskommission:

- Prof. Dr. rer. nat. Habil. Tibor Petzoldt
- Prof. Dr-Ing. Jochen Trinckauf
- Prof. Dr-Ing. Elena Queck
- Dr-Ing. Sven Hietzschold
- Prof. Dr. Meng Wang

Dresden, den 30.12.2022

.....

Tuan Anh Luong

## ACKNOWLEDGEMENT

This dissertation would not have been possible without the guidance and the help of many individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this study.

First and foremost, I would like to express my deepest gratitude to my supervisors, Prof. Dr.-Ing. Jochen Trinckauf. With his enthusiasm, inspiration and sense of humor, he has turned my dissertation into an interesting and relaxing journey. Prof. Trinckauf's direction and ideas were vital in achieving and expanding my System Safety expertise. Professors' sharing of his knowledge has really assisted me in comprehending how high standards might be implemented to a system with limited technical and management abilities. His contribution is absolutely vital.

I am grateful to many technical experts who have provided guidance and advice in order to improve the quality of the thesis. Especially, I would like to send many thanks to PD. Dr.-Ing.habil. Ulrich Maschek, Dr.-Ing. Michael Kunze and Dr.-Ing. Nguyen Thi Hoai An for time to time corrections and many valuable advises about how to improve the work.

I also want to thank my colleagues at Professur für Verkehrssicherungstechnik. Five and a half years is a very long period, a very long and tough journey to the end. Lucky for me, you've been here for me like a family, and your encouragement and support have been invaluable as I've worked to finish my thesis.

Special thanks to the Vietnamese Department of Education and Training who sponsors my study. Furthermore, I want to express my gratitude to my teacher and colleagues in Vietnamese University of Transport and Communications – Prof. Sua Tu, Dr. Huong Tran, Dr. Mai Nguyen, Dr. Truong Le, Dr. Tan Doan for teaching and supporting me to complete.

Financial support for this study was provided by the Vietnam Scholarship Program from 2017 to 2020 and scholarship for wrap-up phase by Technical University of Dresden is valuable support for me to complete this dissertation.

I am grateful for the support of my friends in TU Dresden – Minh Quang Pham, Trong Hung Dinh, Chi Khiem Cao, Hoai Nga Le, Hieu Le, Duc Nguyen who have spent hours and hours in the working with me and sharing unforgettable memories together.

I also wish to thank my wife, Van Anh Le and my daughter, Ngoc Vy An Luong for your continuous support, encouragement, patient waiting and love. Without you, it is definitely difficult to complete this Dissertation.

Lastly but most importantly, I am indebted my family – my grandparents, mom, dad and my younger brother, for their unconditional caring, supports and love. To them I dedicate this Dissertation.

## DECLARATIONS

I declare that to the best of my knowledge the research work presented in this thesis is original except as acknowledged and cited in the text, and that the material has not been submitted, either in whole or part, for another degree at any university elsewhere. This thesis is prepared on my own.

I accept the regulations of the Fakultät Verkehrswissenschaften "Friedrich List" of Technische Universität Dresden that are applicable to a German PhD degree.

Dresden, den 30.12.2022

.....

Tuan Anh Luong

# LIST OF CONTENTS

|  |           |
|--|-----------|
| ACKNOWLEDGEMENT.....   | i         |
| DECLARATIONS.....  | ii        |
| LIST OF CONTENTS .....   | iii       |
| LIST OF TABLES .....   | vii       |
| LIST OF FIGURES.....   | viii      |
| LIST OF ABBREVIATIONS .....  | ix        |
| <b>1. INTRODUCTION .....</b>   | <b>1</b>  |
| <b>1.1 Necessity of the dissertation .....</b>   | <b>1</b>  |
| <b>1.2 Goals and scope of work .....</b>   | <b>2</b>  |
| <b>1.3 Outline of dissertation .....</b>   | <b>4</b>  |
| <b>2. LITERATURE REVIEWS .....</b>   | <b>5</b>  |
| <b>2.1 Concept of RAMS.....</b>  | <b>5</b>  |
| 2.1.1 The developing of railway RAMS .....   | 5         |
| 2.1.2 Elements of railway RAMS .....   | 6         |
| 2.1.3 Life cycle management and RAMS requirements .....                                      | 7         |
| <b>2.2 Risk management.....</b>  | <b>11</b> |
| 2.2.1 Definitions of risk, hazard and risk management.....                                   | 11        |
| 2.2.2 Risk assessment – Procedure and process .....  | 14        |
| 2.2.3 Risk acceptance principle and Safety Integrity levels .....                            | 18        |
| <b>2.3 Risk assessment methods .....</b>   | <b>22</b> |
| 2.3.1 Risk Matrices.....   | 22        |
| 2.3.2 Preliminary Harzard Analysis - PHA.....  | 23        |
| 2.3.3 Failure Mode Effects Analysis - FMEA .....   | 24        |
| 2.3.4 Fault Tree and Event Tree Analysis.....  | 25        |
| 2.3.5 Markov´s chains .....  | 27        |
| 2.3.6 Petri Net .....  | 29        |
| 2.3.7 Bayesian Network .....   | 30        |
| <b>2.4 Safety management system.....</b>   | <b>32</b> |
| 2.4.1 Safety management cocept .....   | 32        |
| 2.4.2 Safety Management System in Railway.....   | 33        |
| 2.4.3 Structure of Safety Management System .....  | 34        |
| <b>3. ANALYSING THE SAFETY-RELATED ISSUES IN IMPLEMENTING URBAN RAILWAY PROJECTS .....</b>   | <b>39</b> |
| <b>3.1 Rationale of Vietnam Urban Railway .....</b>  | <b>39</b> |
| 3.1.1 Planning and existing work of Hanoi urban railway project.....                         | 39        |
| 3.1.2 Current Vietnamese stadards and regulations .....                                      | 42        |
| <b>3.2 Several significant problems in environmental and operational condition.....</b>      | <b>43</b> |
| 3.2.1 The climate conditions in Hanoi.....   | 43        |
| 3.2.2 Hydrogeological conditions .....   | 43        |
| 3.2.3 Operational conditions.....  | 44        |
| <b>3.3 Assessing The Safety Culture In The Vietnamese Railway Industry .....</b>             | <b>45</b> |
| 3.3.1 Methodology.....   | 45        |
| 3.3.2 Result Description.....  | 47        |
| 3.3.3 Key Findings.....  | 54        |
| <b>3.4 System description of Hanoi Metro Line HN2A. Cat Linh – Ha dong Station .....</b>     | <b>56</b> |
| 3.4.1 Overview of metro lines .....  | 56        |
| 3.4.2 Infrastructure .....   | 57        |
| 3.4.3 Power supply characteristics .....   | 57        |
| 3.4.4 Rolling stocks .....   | 58        |
| 3.4.5 Signalling and Controlling system.....   | 59        |
| <b>3.5 Safety-related issues in System Acceptance phase of Metro Line HN2A projects ....</b> | <b>64</b> |
| 3.5.1 Safety-related key issues founding in System Acceptance phase.....                     | 64        |
| 3.5.2 Outline the solutions for System Safety of Metro Line HN2A .....                       | 65        |
| <b>4. SAFETY SOLUTIONS FOR OPERATED LINE – RISK ASSESSMENT .....</b>                         | <b>68</b> |

|            |   |            |
|------------|---|------------|
| <b>4.1</b> | <b>Purpose and scope of Risk assessment in HanoiMetro.....</b>                              | <b>68</b>  |
| <b>4.2</b> | <b>The Preliminary Hazard Analysis of metro operation.....</b>                              | <b>69</b>  |
| 4.2.1      | General method requirements .....   | 69         |
| 4.2.2      | Identification of hazards .....   | 70         |
| 4.2.3      | Hazard analysis and mitigation measures identification .....                                | 71         |
| 4.2.4      | Risk resolution measures.....   | 71         |
| <b>4.3</b> | <b>The Fault Tree Analysis of Metro Line HN2A .....</b>                                     | <b>73</b>  |
| 4.3.1      | Overview of Fault Tree Analysis method.....   | 73         |
| 4.3.2      | Method and procedure of a Fault Tree Analysis .....   | 73         |
| 4.3.3      | Risk analysis for Train-to-train Collisions hazards .....                                   | 76         |
| 4.3.4      | Risk analysis for Train derailments hazards .....   | 81         |
| 4.3.5      | Incidents leading to people injured in urban railway operation.....                         | 86         |
| <b>4.4</b> | <b>The Bayesian Network application for Metro Line HN2A .....</b>                           | <b>89</b>  |
| 4.4.1      | Methods and Procedure of establishing the Bayesian Network.....                             | 89         |
| 4.4.2      | Example of BN risk assessment .....   | 92         |
| <b>5.</b>  | <b>SAFETY SOLUTIONS FOR OPERATED LINE – RAILWAY VEHICLE MAINTENANCE AND OPERATIONS.....</b> | <b>96</b>  |
| <b>5.1</b> | <b>Railway Vehicle - Operating, Maintenance and Inspection .....</b>                        | <b>96</b>  |
| 5.1.1      | Purpose and Scope .....   | 96         |
| 5.1.2      | Management structure of Hanoi Metro Company. ....   | 96         |
| 5.1.3      | Procedures of Operating Rolling Stocks.....   | 97         |
| 5.1.4      | Vehicle Monitoring, Maintenance and Repair Requirements.....                                | 100        |
| 5.1.5      | Calculation of Maintenance and Repair Demand .....  | 103        |
| 5.1.6      | Vehicle Modification / Renovation Procedure .....   | 106        |
| 5.1.7      | Rolling stocks inspection .....   | 107        |
| <b>5.2</b> | <b>Railway Equipment – Inspection and Maintenance.....</b>                                  | <b>118</b> |
| 5.2.1      | Purpose and Scope .....   | 118        |
| 5.2.2      | Maintenance schedule planning .....   | 118        |
| 5.2.3      | Communication equipment inspection contents .....   | 119        |
| 5.2.4      | Railway Signal equipment inspection contents.....   | 120        |
| 5.2.5      | Electric power equipment inspection contents.....   | 121        |
| <b>6.</b>  | <b>SAFETY SOLUTIONS FOR OPERATED LINE – TRACK AND CIVIL STRUCTURE MAINTENANCE...</b>        | <b>123</b> |
| <b>6.1</b> | <b>Purpose and Scope.....</b>   | <b>123</b> |
| <b>6.2</b> | <b>Maintenance plan of Track and Civil Structures .....</b>                                 | <b>123</b> |
| 6.2.1      | Track Maintenance Plan.....   | 123        |
| 6.2.2      | Civil structure inspection cycle .....  | 124        |
| <b>6.3</b> | <b>Track Inspection methods .....</b>   | <b>125</b> |
| 6.3.1      | Track patrol.....   | 125        |
| 6.3.2      | Patrol on foot.....   | 125        |
| 6.3.3      | Inspection of structure gauge .....   | 126        |
| 6.3.4      | Measure the four items (gauge, cross level, longitudinal level, alignment).....             | 126        |
| 6.3.5      | Inspection of rail crack or rail damage .....   | 127        |
| 6.3.6      | Inspection of Turnouts and crossings .....  | 127        |
| 6.3.7      | Inspection of Joints .....  | 128        |
| 6.3.8      | Inspection of sleeper .....   | 128        |
| 6.3.9      | Inspection of fastening system .....  | 129        |
| 6.3.10     | Inspection of track bed.....  | 129        |
| 6.3.11     | Inspection of train stop .....  | 129        |
| <b>6.4</b> | <b>Track Repair Guidelines .....</b>  | <b>130</b> |
| 6.4.1      | Correction of alignment .....   | 130        |
| 6.4.2      | Gauge adjustment .....  | 131        |
| 6.4.3      | Rail Renewal.....   | 131        |
| 6.4.4      | Sleeper renewal.....  | 133        |
| <b>6.5</b> | <b>Civil structure Inspection methods .....</b>   | <b>134</b> |
| 6.5.1      | Appearance inspection of viaducts and tunnels - Monthly .....                               | 134        |
| 6.5.2      | Appearance inspection of viaducts and tunnels - Yearly .....                                | 134        |

|            |   |            |
|------------|---|------------|
| 6.5.3      | Appearance inspection of tunnels – Ten-yearly .....   | 135        |
| 6.5.4      | Buildings appearance and building equipment inspection .....  | 135        |
| <b>6.6</b> | <b>Civil structure Repair methods .....</b>   | <b>136</b> |
| 6.6.1      | Viaducts.....   | 136        |
| 6.6.2      | Open-cut tunnel .....   | 136        |
| 6.6.3      | Repair of structure .....   | 137        |
| <b>7.</b>  | <b>SAFETY SOLUTIONS FOR OPERATED LINE - INCIDENT MANAGEMENT PROCESS .....</b>   | <b>138</b> |
| <b>7.1</b> | <b>Incident Management Purpose and Scope .....</b>  | <b>138</b> |
| <b>7.2</b> | <b>The general procedure and guidelines for accident responding.....</b>  | <b>140</b> |
| 7.2.1      | Accident Treatment Structure .....  | 140        |
| 7.2.2      | The procedure of warning classification and information reporting .....   | 142        |
| 7.2.3      | The general procedure of Accident Responding.....   | 143        |
| <b>7.3</b> | <b>The accident responding procedure relating to Rolling Stocks.....</b>  | <b>146</b> |
| 7.3.1      | The procedure of Initial Action responding to the accidents: .....  | 146        |
| 7.3.2      | The procedure of Work Assignment at accident site.....  | 147        |
| 7.3.3      | The Procedure of Restoring the Rolling Stock Failure after Returning to Depot .....   | 148        |
| <b>7.4</b> | <b>The accident responding procedure relating to Passenger injuries .....</b>   | <b>150</b> |
| 7.4.1      | Responsibilities in an accident relating to passenger injuries.....   | 150        |
| 7.4.2      | The procedure of passenger injuries treatment.....  | 151        |
| 7.4.3      | The typical procedures relating to people injuries .....  | 152        |
| <b>7.5</b> | <b>The accident responding procedure relating to vandalisms or terrorities.....</b>   | <b>153</b> |
| 7.5.1      | Purpose and classification of protecting from vandalisms or terrorities .....   | 153        |
| 7.5.2      | Regulation for safety and security in station areas and track sections.....   | 153        |
| 7.5.3      | Regulation for safety and security in train.....  | 154        |
| 7.5.4      | Regulation for safety and security in Dispatching Centre, Vehicle Maintenance<br>Centre and Maintenance Material Centre ..... | 154        |
| 7.5.5      | The general procedure for terrorism attack occurrences .....  | 155        |
| <b>7.6</b> | <b>The accident responding procedure relating to fire and explosion.....</b>  | <b>156</b> |
| 7.6.1      | Purpose and Clarification of Fire and Explosion accidents.....  | 156        |
| 7.6.2      | Fire and explosion safety instructions.....   | 157        |
| 7.6.3      | Principle of Fire and Explosion accident responding.....  | 158        |
| 7.6.4      | The process of fire and explosion incident responding .....   | 158        |
| <b>7.7</b> | <b>The accident responding procedure relating to disaster .....</b>   | <b>159</b> |
| 7.7.1      | Purpose and classifications of disaster warnings. ....  | 159        |
| 7.7.2      | The procedure for natural disaster responding.....  | 160        |
| <b>8.</b>  | <b>SOLUTIONS FOR LONG-TERM DEVELOPMENT- SAFETY CULTURE.....</b>   | <b>161</b> |
| <b>8.1</b> | <b>Human factors in Railway Accident.....</b>   | <b>161</b> |
| 8.1.1      | Concept of Human factors in railway system failures.....  | 161        |
| 8.1.2      | Factor influencing to Human performance in railway system .....   | 162        |
| <b>8.2</b> | <b>The role of Safety Culture in System Safety Improvement.....</b>   | <b>165</b> |
| 8.2.1      | Concept of Safety Culture .....   | 165        |
| 8.2.2      | The influences of safety culture in operational safety .....  | 165        |
| 8.2.3      | The principle and methods of applying Safety Culture .....  | 166        |
| 8.2.4      | A practice to establish and improve the safety culture.....   | 168        |
| <b>8.3</b> | <b>Human resources management .....</b>   | <b>171</b> |
| 8.3.1      | Safety Training.....  | 171        |
| 8.3.2      | General Contents of Safety training .....   | 172        |
| 8.3.3      | Stress and fatigue management.....  | 174        |
| 8.3.4      | Drug and Alcohol control .....  | 175        |
| <b>8.4</b> | <b>Leadership and Staff Involments.....</b>   | <b>176</b> |
| 8.4.1      | Purpose of Leadership and Staff Involments in Safety Culture .....  | 176        |
| 8.4.2      | Leadership to develop and sustain a safety culture .....  | 176        |
| 8.4.3      | Improve the Staff Involvement in Safety Culture .....   | 178        |
| <b>9.</b>  | <b>SOLUTIONS FOR LONG-TERM DEVELOPMENT – DATA MANAGEMENT .....</b>  | <b>180</b> |
| <b>9.1</b> | <b>Analysis and Reporting .....</b>   | <b>180</b> |
| 9.1.1      | Data management regulations .....   | 180        |

---

|             |  |            |
|-------------|--|------------|
| 9.1.2       | Internal assesement and Safety Audit.....                                    | 182        |
| <b>9.2</b>  | <b>Establishing a Railway Accident Database .....</b>                        | <b>184</b> |
| 9.2.1       | Problem of Railway Accident data in Vietnam.....                             | 184        |
| 9.2.2       | Category and report contents in accident database. ....                      | 185        |
| 9.2.3       | Traffic accident data management.....  | 186        |
| <b>10.</b>  | <b>DISCUSSIONS AND CONCLUSION.....</b>                                       | <b>187</b> |
| <b>10.1</b> | <b>Discussion on Risk assessment calculations .....</b>                      | <b>187</b> |
| <b>10.2</b> | <b>Limitations and Recommendations .....</b>                                 | <b>190</b> |
| <b>10.3</b> | <b>Conclusions .....</b>   | <b>191</b> |
|             | <b>REFERENCES .....</b>  | <b>193</b> |
|             | <b>APPENDIX.....</b>   | <b>199</b> |
|             | Appendix 1: Questionnaire for railway worker attitudes on safety risks ..... | 199        |
|             | Appendix 2 : Risk matrix analysis of HN Line 2A .....                        | 202        |
|             | Appendix 3: Checklist of Railway Vehicle Mobilisation .....                  | 225        |
|             | Appendix 5: Typical accident reaction plans.....                             | 227        |
|             | Appendix 4: Example of Inspection plan .....                                 | 229        |
|             | Appendix 6: Contents of Internal Assessment and Safety Audit .....           | 232        |



---

**LIST OF TABLES**

|  |     |
|--|-----|
| TABLE 2.1 OVERALL PROJECT PHASE TASKS .....  | 8   |
| TABLE 2.2 QUANTITATIVE SIL REQUIREMENTS .....  | 20  |
| TABLE 2.3 EXAMPLE OF FMCEA OF TRACK FAILURE .....                                      | 25  |
| TABLE 2.4 STRUCTURE OF BAYESIAN NETWORK .....  | 30  |
| TABLE 2.5 SAFETY MANAGEMENT SYSTEM REQUIREMENTS.....                                   | 35  |
| TABLE 3.1 SUMMARY OF METRO LINES PLANNED IN HANOI .....                                | 40  |
| TABLE 3.2 AVERAGE MEAN VALUE OF CURRENT SAFETY RISK PROBLEMS.....                      | 48  |
| TABLE 3.3 AVERAGE MEAN VALUE OF CURRENT SAFETY RISK PROBLEMS (CONT.).....              | 49  |
| TABLE 3.4 ITEM-TOTAL STATISTICS IN STRESS AND FATIGUE PROBLEM.....                     | 49  |
| TABLE 3.5 ITEM-TOTAL STATISTICS IN PROBLEMS OF VIOLATION.....                          | 50  |
| TABLE 3.6 MODEL SUMMARY FOR CURRENT SAFETY RISKS INDEX.....                            | 50  |
| TABLE 3.7 LINEAR REGRESSION COEFFICIENTS FOR SAFETY RISKS INDEX .....                  | 50  |
| TABLE 3.8 AVERAGE MEAN VALUE OF POTENTIAL SAFETY PROBLEM.....                          | 51  |
| TABLE 3.9 AVERAGE MEAN VALUE OF POTENTIAL SAFETY PROBLEM (CONT.).....                  | 52  |
| TABLE 3.10 MODEL SUMMARY FOR POTENTIAL SAFETY PROBLEM INDEX.....                       | 53  |
| TABLE 3.11 LINEAR REGRESSION COEFFICIENTS FOR SAFETY RISKS INDEX .....                 | 53  |
| TABLE 3.12. MAIN FEATURES OF TRAIN TRACTION AND PERFORMANCE.....                       | 59  |
| TABLE 4.1 RISK CLASSIFICATION BASED ON SEVERITY AND FREQUENCY OF METRO LINE 2A.....    | 72  |
| TABLE 4.2 PROBABILITY OF TOP EVENTS MISCOMMUNICATION AND FAILURE IN ATP.....           | 77  |
| TABLE 4.3 PROBABILITY OF TOP EVENTS: DRIVER ERRORS LEADING TO COLLISIONS.....          | 78  |
| TABLE 4.4 PROBABILITY OF FAILURE OF VEHICLE AND FAILURE OF INFRASTRUCTURE.....         | 79  |
| TABLE 4.5 PROBABILITY OF TRAIN COLLISION WITH INACTIVED/OR A PART OF TRAIN.....        | 81  |
| TABLE 4.6 PROBABILITY OF PEOPLE FALLS IN THE TRAIN .....                               | 87  |
| TABLE 4.7. PROBABILITY OF PEOPLE FALLS ON THE TRACK.....                               | 87  |
| TABLE 4.8. PROBABILITY OF PEOPLE FALLS ON PLAFORM AND GRIPPING BY TRAIN DOOR .....     | 88  |
| TABLE 4.9 EXAMPLE OF CONDITIONAL PROBABILITY TABLES FOR BN IN FIGURE 33 .....          | 91  |
| TABLE 5.1 THE NUMBER OF PERSONEL REQUIRED FOR DAILY INSPECTION AND MAINTENANCE .....   | 105 |
| TABLE 7.1 INVESTIGATION LEVEL AND NOTIFICATION LEVEL OF AN ACCIDENT/INCIDENT .....     | 139 |
| TABLE 8.1 REQUIREMENTS FOR A POSITIVE SAFETY CULTURE .....                             | 168 |
| TABLE 8.2 THREE SOLUTION GROUPS FOR IMPROVE SAFETY CULTURE.....                        | 169 |
| TABLE 10.1 COMPARING THE HAZARD RATES IN THEORICAL CALCULATIONS AND TESTING DATA ..... | 187 |

## LIST OF FIGURES

|  |     |
|--|-----|
| FIGURE 1. V MODEL REPRESENTATION OF THE LIFECYCLE MANAGEMENT OF RAILWAY SYSTEM.....                | 7   |
| FIGURE 2 THE RISK MANAGEMENT PROCESS .....   | 13  |
| FIGURE 3 RISK ASSESSMENT PROCEDURE .....   | 14  |
| FIGURE 4 ALARP ACCEPTANCE REGION .....   | 19  |
| FIGURE 5 A RISK GRAPH TO DETERMINE SIL LEVEL .....   | 21  |
| FIGURE 6 COMPLEX 14x14 MATRIX .....  | 22  |
| FIGURE 7. EXAMPLE OF FTA: DRIVER ERRORS LEADING TO TRAIN COLLISION .....                           | 26  |
| FIGURE 8. EXAMPLE OF ETA – FAILURE OF AUTOMATIC TRAIN CONTROL SYSTEM .....                         | 27  |
| FIGURE 9 HOURGLASS MODEL FOR RISK MANAGEMENT WITHIN RAILWAY .....                                  | 36  |
| FIGURE 10 METRO LINE NETWORK MAPS IN HANOI .....   | 39  |
| FIGURE 11. METRO LINE HN2A. HA DONG STATION – CAT LINH (OPERATED) .....                            | 41  |
| FIGURE 12. METRO LINE HN3. NHON – HANOI RAILWAY STATION (IN CONSTRUCTION) .....                    | 41  |
| FIGURE 13 OVERVIEW OF HANOI URBAN RAILWAY LINE HN2A .....  | 56  |
| FIGURE 14. MAIN DIMENSIONS FOR ROLLING STOCKS OF METRO LINE HN2A .....                             | 58  |
| FIGURE 15 ZONE OF INTERLOCKING CONTROL FOR UMRT LINE HN2A SUB-SYSTEM.....                          | 61  |
| FIGURE 16 FUNCTION OF SIGNAL SYSTEM OF LINE HN2A .....   | 63  |
| FIGURE 17 OUTLINE OF SAFETY MANAGEMENT SYSTEM IMPLEMENTING PROCESS IN VIETNAM METRO PROJECTS ..... | 66  |
| FIGURE 18 SYSTEM BREAKDOWN STRUCTURE.....  | 68  |
| FIGURE 19 IDENTIFICATION OF THE BREAKDOWN OF HAZARDS .....   | 70  |
| FIGURE 20 THEORETICAL CALCULATION OF EVENT TREE ANALYSIS .....                                     | 75  |
| FIGURE 21 FAULT TREE ANALYSIS OF TRAIN COLLISIONS.....   | 76  |
| FIGURE 22 FTA OF TOP EVENTS MISCOMMUNICATION AND FAILURE IN ATP .....                              | 77  |
| FIGURE 23 FTA OF TOP EVENTS: DRIVER ERRORS LEADING TO COLLISIONS .....                             | 78  |
| FIGURE 24 FTA TOP EVENTS: FAILURE OF VEHICLE AND FAILURE OF INFRASTRUCTURE .....                   | 79  |
| FIGURE 25 FTA TOP EVENTS TRAIN COLLISION WITH INACTIVED/OR A PART OF TRAIN .....                   | 80  |
| FIGURE 26. FTA OF TOP EVENT 1 – DERAILMENT DUE TO SPAD .....                                       | 82  |
| FIGURE 27 FTA OF TOP EVENT 2 – DERAILMENT BY SIGNALLING AND DISPATCHING ERRORS.....                | 83  |
| FIGURE 28 FTA FOR TOP EVENT – DERAILMENT DUE TO TRACK FAILURE .....                                | 84  |
| FIGURE 29. FTA FOR TOP EVENT – DERAILMENT DUE TO WHEELSET FAILURE .....                            | 85  |
| FIGURE 30 FTA FOR TOP EVENT – PEOPLE FALLS IN THE TRAIN .....                                      | 86  |
| FIGURE 31 FTA FOR TOP EVENT – PEOPLE FALLS ON THE TRACK .....                                      | 88  |
| FIGURE 32. FTA FOR PEOPLE FALLS ON PLAFORM AND GRIPPING BY TRAIN DOOR.....                         | 89  |
| FIGURE 33. SIMPLE STRUCTURE OF BAYESIAN NETWORK .....  | 91  |
| FIGURE 34. BN OF DERAILMENT DUE TO SIGNALLING AND DISPATCHING ERROR .....                          | 92  |
| FIGURE 35 CPT OF ERROR MADE BY SIGNALLER .....   | 93  |
| FIGURE 36 PROBABILITIES OF DERAILMENT DUE TO SIGNALLING AND DISPATCHING ERROR.....                 | 93  |
| FIGURE 37 BAYESIAN NETWORK OF ERROR MADE BY SIGNALLER .....  | 95  |
| FIGURE 38 NODE PROBABILITIES OF ERROR MADE BY SIGNALLER .....                                      | 95  |
| FIGURE 39. HANOI METRO COMPANY STRUCTURE .....   | 97  |
| FIGURE 40 PROCESS OF MAINTENANCE AND REPAIR PLANNING.....  | 102 |
| FIGURE 41 FLOW OF PREPARING TRAIN ALLOCATION AT DEPOT .....  | 103 |
| FIGURE 42 OFFSET MEASURED AT THE POSITIONS OF 1/4, 1/2 AND 3/4 (A1, A2 AND A3).....                | 132 |
| FIGURE 43 GENERAL DRAWING OF REPAIR OF ELEVATED CONCRETE BRIDGE.....                               | 136 |
| FIGURE 44 ACCIDENT TREATMENT STRUCTURE .....   | 141 |
| FIGURE 45 CLASSIFICATION OF WARNING .....  | 143 |
| FIGURE 46 THE GENERAL PROCEDURE OF ACCIDENT RESPONDING .....                                       | 145 |
| FIGURE 47 RESPONSIBILITIES OF EACH PERSONNEL IN COMMUNICATION AND REPORTING.....                   | 148 |
| FIGURE 48 SEVERAL TYPES OF FAILURE, AND COUNTERMEASURES FOR ROLLING STOCKS .....                   | 149 |
| FIGURE 49 PRINCIPLE EVENT TREE ANALYSIS FOR FAILURE IN ATC INPUT.....                              | 189 |

## LIST OF ABBREVIATIONS

| <b>Abbreviations</b> | <b>Meaning(s)</b>   |
|----------------------|---|
| AC/DC                | Alternating Current / Direct current                                  |
| ADB                  | Asian Development Bank  |
| ALARP                | As low as reasonably practicable                                      |
| AM                   | Automation driving under ATP supervision                              |
| ATO                  | Automatic Train Operation   |
| ATC                  | Automatic Train Control   |
| ATP                  | Automatic Train Protection  |
| ATS                  | Automatic Train Supervision   |
| BN                   | Bayesian Network  |
| CBTC                 | Communication-based train control                                     |
| CCF                  | Common causes failures  |
| CCTV                 | Closed Circuit Television   |
| CM                   | Manual train driving mode under the supervision of ATP                |
| CPT                  | Conditional probability table   |
| CTC                  | Centralised Train Control   |
| CSM                  | Common Safety Methods   |
| EU/EC                | European / European Union / European Commission                       |
| ETA                  | Event Tree Analysis   |
| FMEA/FMCEA           | Failure Mode Effects Analysis/ Failure Mode Critical Effects Analysis |
| FTA                  | Fault Tree Analysis   |
| GAMAB                | Globalement au moins aussi beau/Globally at least as excellent        |
| Hanoi Metro          | Hanoi Metro Company   |
| HN                   | Hanoi   |
| HCMC                 | Ho Chi Minh City  |
| MRT                  | Mass Rapid Transit  |
| No.                  | Number  |
| NRM                  | Non Restricted Manual Mode  |
| IEC                  | International Electrotechnical Commission                             |
| ISO                  | International Organization for Standardization                        |
| MEM                  | Minimum endogenous mortality  |
| PHA                  | Preliminary Harzard Analysis  |
| PT                   | Petri Net   |
| QCQG                 | Vietnamese regulated norms  |
| QD-TTg               | Decision of Prime Minister (in Vietnamese)                            |
| QD-BGTVT             | Decision of Ministry of Transport (in Vietnamese)                     |
| QD-UBND              | Decision of People ´ s Committee of a province (in Vietnamese)        |
| RAMS                 | Reliability, Availability, Maintainability, and Safety                |
| RM                   | Restricted manual train driving mode                                  |
| RU                   | Railway Undertaking   |
| SIL                  | Safety Integrity levels   |
| SMS                  | Safety Management System  |
| SPAD                 | Signal Passed at Danger   |
| TCCS                 | Vietnam Basic Standards   |
| TCVN                 | Vietnamese Standards  |
| TFFR                 | Tolerable Functional Failure Rate                                     |
| UMRT                 | Urban Mass Rapid Transit  |
| UIC                  | International union of railway  |
| UK                   | United Kingdoms   |
| US                   | United States of America  |
| VR                   | Vietnam Railway   |

# 1. INTRODUCTION

## 1.1 Necessity of the dissertation

Nowadays, rail transport has become one of the most widely utilised forms of transport thanks to its high safety level, large capacity, and cost - effectiveness. With the railway network's continuous development including urban rail transit, one of the major areas of increasing attention and demand is ensuring safety or risk management in operation long-term remains for the whole life cycle by scientific tools, management of railway operation (Martani 2017), specifically in developed and developing countries like Vietnam. The situation in Vietnam demonstrates that the national mainline railway network has been built and operated entirely in a single narrow gauge (1000mm) since the previous century, with very few updates of manual operating technology. This significantly highlights that up to now the conventional technique for management the safety operation in general, and collision in particular, of the current Vietnamese railway system, including its subsystems is only accident statistics which is not scientific-based tool as the others like risk identify and analyse methods, risk mitigation..., that are already available in many countries.

Accident management of Vietnam Railways is limited and responsible for accident statistics analysis to avoid and minimise harm caused by phenomena that occur only after an accident. Statistical analysis of train accident case studies in Vietnam railway demonstrates that, because hazards and failures that could result in serious system occurrences (accidents and incidents) have not been identified, recorded, and evaluated to conduct safety-driven risk analysis using a well-suited assessment methodology, risk prevention and control cannot be achieved. Not only it is hard to forecast and avoid events, but it may also raise the chance and amount of danger, as well as the severity of the later effects. As a result, Vietnam's railway system has a high number of accidents and failure rates. For example Vietnam Railways' mainline network accounts for approximately 200 railway accidents in 2018, a 3% increase over the previous year, including 163 collisions between trains and road vehicles/persons, resulting in more than 100 fatalities and more than 150 casualties; 16 accidents, including almost derailments, the signal passed at danger... without fatality or casualty, but significant damage to rolling stock and track infrastructure (VR 2021).

Focusing and developing of a new standardised framework for safety management and availability of the railway operation in Vietnam is required in view of the rapid development of rail urban transport in the country in recent years (VmoT 2016; VmoT 2018). UMRT Line HN2A in southwest Hanoi is the country's first and elevated light rail transit line, which was completed and officially put into revenue service since November 2021. This greatly highlights that up to the current date, the UMRT Line HN2A is the first and only railway line in Vietnam with operational safety assessment launched for the first time and long-term remains for the whole life cycle. The fact that the UMRT Hanoi has a large capacity, more complicated rolling stock and infrastructure equipment, as well as a modern communication-based train control (CBTC) signaling system and automatic train driving without the need for operator intervention (Lindqvist 2006), are all advantages.

Developing a compatible and integrated safety management system (SMS) for adaption to the safety operating requirements of this UMRT is an important major point of concern, and this should be proven. In actuality, the system acceptance and safety certification phase for Metro Line HN2A prolonged up to 2.5 years owing to the identification of difficulties with noncompliance to safety requirements resulting from inadequate SMS documents and risk

assessment. These faults and hazards have developed during the manufacturing and execution of the project; it is impossible to go back in time to correct them, and it is also impossible to ignore the project without assuming responsibility for its management. At the time of completion, the HN2A metro line will have required an expenditure of up to \$868 million, thus it is vital to create measures to prevent system failure and assure passenger safety.

This dissertation has reviewed the methods to solve the aforementioned challenges and presented a solution blueprint to attain the European standard level of system safety in three phase as in the following:

- Phase 1: applicable for lines that are currently in operation, such as Metro Line HN2A. Focused on operational and maintenance procedures, as well as a training plan for railway personnel, in order to enhance human performance. Complete and update the risk assessment framework for Metro Line HN2A. The dissertation's findings are described in these applications.
- Phase 2: applicable for lines that are currently in construction and manufacturing, such as Metro Line HN3, Line HN2, HCMC Line 1 and Line 2. Continue refining and enhancing engineering management methods introduced during Phase 1. On the basis of the risk assessment by manufacturers (Line HN3, HCMC Line 2 with European manufacturers) and the risk assessment framework described in Chapter 4, a risk management plan for each line will be developed. Building Accident database for risk assessment research and development.
- Phase 3: applicable for lines that are currently in planning. Enhance safety requirements and life-cycle management. Building a proactive Safety Culture step by step for the railway industry. This material is implemented gradually throughout all three phases, beginning with the creation of the concept and concluding with an improvement in the attitude of railway personnel on the HN2A line.

In addition to this overview, Chapters 4 through Chapter 9 of the dissertation include particular solutions for Risk assessment, Vehicle and Infrastructure Maintenance method, Incident Management procedure, and Safety Culture installation. This document focuses on constructing a system safety concept for railway personnel, providing stringent and scientific management practises to assure proper engineering condition, to manage effectively the metro line system, and to ensure passenger safety in Hanoi's metro operation.

## **1.2 Goals and scope of work**

The purpose of this study is to examine the RAMS railway management approach and implement the Safety Management System to Vietnam's first urban rail system. The dissertation focuses on enhancing the literature study on risk management, risk assessment methodologies, and SMS procedure in order to construct the SMS system.

The dissertation attempts to respond to the following research questions:

1. Current study in risk management processes and approaches is the subject of these questions. What modifications will these studies necessitate when applied to Vietnam's operating conditions?

Question 1: What is state-of-art knowledge of risk management and safety management system?

Question 2: Why RAMS can support more efficient urban rail operations?

Question 3: What are the system, technical, and business conditions of urban railways in Vietnam that are different from those of the world?

2. Analysis of system specifications and safety-related issues in implementing metro line projects in Vietnam.

Question 4: What are the limitations of VN urban railway projects?

Question 5: What is the safety gaps between VN current situation and requirements of a good SMS plan ?

Question 6: How many steps and which strategies for each step to achieve EU safety standards?

3. Solutions for each development phase to ensure the system safety

Question 7: In completed Project, are the operational condition analysis and risk assessment consistent with the actual operational data of the line HN2A?

Question 8: What are the requirements for testing and maintaining rolling stock, track and infrastructure and equipment?

Question 9: What are the steps to perform emergency response to accidents and what are the responsibilities of each unit in HanoiMetro in typical accidents?

Question 10: In constructing Projects and planning Project, how can improve the system safety to meet requirements of a good safety practice?

Based on an examination of the Metro Line HN2A specifications and safety-related concerns in the system approval and safety certificate processes, the thesis proposes Fault Tree Analysis with a connection to Preliminary Hazard Analysis and Bayesian Network as a viable risk assessment approach.

These findings significantly highlight that this is a straightforward method for safety assessment suitable and started to be applied for the first time in Vietnam, approved through application to the Line HN2A, despite that these methods are being applied commonly in some developed-railways countries . it is a basic calculations, are easily applicable, and could be standardised for technical management of other railway lines in Vietnam.

Based on the The Preliminary Hazard Analysis of Metro Line HN2A and the general knowledge of railway accident, the dissertation concentrated on 04 types of generic and significant accident such as Train Collisions, Train Derailment, and Incidents leading to people injured in urban railway operation. These types of accidents are similar in low frequency but serious severity and complex interactive failures. Therefore, it is necessary to analyse the root reasons leading to accidents. The other types of high frequency and low severity incidents could be controlled by engineering maintainance procedure, railway staff regulations and accident training.

In two parts, Chapter 5 and Chapter 6, the dissertation explains the inspection and maintenance plan for railway vehicle, track and infrastructure, and railway equipment. These protocols outline the maintenance cycle, inspection methods, and maintenance contents. This article aims to illustrate stringent requirements to maintain the best technical condition of the system and the railway staff's ease of use.

The remainder of the discussion focuses on the creation of a proactive Safety Climate and Safety Culture inside the organisation, as well as the impact of safety culture on the leader

and railway workers. Consequently, the effectiveness of safety management is enhanced by shifting from passively complying with rules to actively influencing system safety. Problems pertaining to Data Management and the development of an Accident Database can also contribute to the expansion and improvement of the system.

### **1.3 Outline of dissertation**

Chapter 1 is the introduction of the thesis, clarify the necessity of research, the overall research targets and research methodology.

Chapter 2 is a Literature review, which summarised the current ideas and research development of railway RAMS, procedure and methodology of risk management and analysis. The final part of this chapter has been reviewed the concept and guidelines to establish the Safety Management System in the railway industry.

Chapter 3 is Analysing the Safety-related issues in implementing Hanoi urban railway projects, which clarifies the current status of Hanoi metro projects. This chapter has provided an overview of the current situation and the negative factors influencing these projects. This chapter also describes the interview survey carried out to assess the safety perception of railway staff and experts to clarify the safety culture in Vietnam. In the final section of this chapter, safety-related problems in the system acceptance and safety certification phase are described and suggested in outlined solution groups.

Chapter 4 to Chapter 9 has been established a Safety Management System for Hanoi Metro Company and several solutions for long-terms development. Chapter 4 is Safety Solutions for Operated line – Risk assessment. This Chapter is the main part of this research, described how to establish the Preliminary Hazard Analysis, Fault Tree Analysis and example of Bayesian Network for each project phase, each safety management purpose. The Hazard Identification and Risk assessments are applied and calculated for Hanoi Metro Company by these methods.

Chapter 5 is Safety Solutions for Operated line – Railway Vehicle Maintenance and Operations and Chapter 6 is Safety Solutions for Operated line – Track and Infrastructure Maintenance. They clarify the Procedure of Process Control Inspection and Testings, Maintenance of vehicle, track and infrastructure and equipment. The inspection checklists and maintenance process has also referred to this part.

Chapter 7 is Safety Solutions for Operated line – Incident Management process. This Chapter is concentrated on explaining several typical emergency response such as rolling stock related accidents, fire and explosion, people evacuation and disasters. This Chapter indicates the requirements and former procedures for unit collaboration in emergency situation.

Chapter 8 is Safety Solutions for long-term development – Safety Culture. This Chapter concentrated on the establishment of Safety Culture in the company and reducing Human failure by Human resource management, Employee Involvement.

Chapter 9 is Safety Solutions for long-term development – Data Management focused on the data analysis and Safety Audit in the company to ensure the accuracy of failure data and implementation testing. It also suggests the outline of accident database establishment.

Chapter 10 is Conclusion and Discussion. This Chapter will conclude the research problems, key findings and solutions. It will suggest to the national authority the problem of accident data publishing and accessibility improve the research quality of safety.

## 2. LITERATURE REVIEWS

### 2.1 Concept of RAMS

#### 2.1.1 The developing of railway RAMS

Safety assessments were first performed by the nuclear industry in the 1950s and 1960s (Beckerley, 1957). By 1970 comprehensive safety reports were produced, US Nuclear Regulatory Commission (1975). A spate of accidents such as Flixborough (1974), Three Mile Island (1975) and Chernobyl (1986) led to stricter safety guidelines. Early examples of RAM analysis can also be found in the nuclear industry, Cleveland et al. (1985). Other industries using RAM analysis include aerospace (Cole, 1998), plants (Rotab Khan and Zohrul Kabir, 1995), and telcoms (Hamersma and Chodos) (1992).

It is important to note that safety and reliability analysis did not emerge as a single field but rather as a result of the integration of many activities such as reliability modeling (Smith, 2017). RAM analysis evolved into RAMS analysis as a result of this development. Initially, there was some debate about what the letter 'S' should stand for, with some arguing that it should stand for survivability (Hamersma and Chodos, 1992), while others argued that supportability (Markeset and Kumar, 2003) would be a more appropriate designation (as opposed to the standard, safety) (Zoeteman and Braaksma, 2001; Breemer, 2009) would be more appropriate. However, there is now widespread agreement that the letter S stands for safety; the industry standard for railway safety is already in place.

Using the state-of-art definition, railway standards define concepts such as reliability, availability, maintainability, and safety (also called RAMS). The RAMS performance required to meet a system's operational objectives can be accomplished by successfully integrating RAMS characteristics into the system's product design and manufacturing throughout the system life cycle (Pasquale et al. 2003, Madu, 2005). While RAMS often provides a full view of the system, it may be essential to incorporate extra factors in some situations. Wagner and Van Gelder (2013) expanded the RAMS framework; RAMS was renamed RAMSSHE, RAMS+ security, health, and environment, and lastly RAMSSHEeP (RAMSSHE+ economics and politics).

RAMS management has recently grown in popularity due to its ability to deliver a defined rail traffic service on schedule, safely, and affordably. It can also help railways compete with other modes of transit. Thus, RAMS management has become an important issue in today's worldwide railway industry, and it is gradually spreading to domestic railways (CENELEC - EN 50126, 2018). RAMS implies a safe, dependable, high-quality service for rail system operators, as well as decreased operating and maintenance expenses. Besides, RAMS represents a high-quality system and product for the rail system supplier. Therefore, it will be the foundation of many businesses' competitive advantage.

European railway groups have previously implemented RAMS management in their projects. However, most railways are still in the early stages of RAMS management and systems engineering. However, even though the systems engineering that was utilised in the railway design and development project was based on RAMS, the system engineering as a significant aspect of engineering management has not yet been implemented. As a result, RAMS management is incomplete. Integrating RAMS management into the railway systems engineering process becomes a major difficulty (Ju et al., 2011).



Many attempts have been made to integrate RAMS management into the railway systems engineering process, but few organisations have succeeded due to the lack of a systematic approach based on proven engineering principles, methods, techniques, and tools (Valkokari et al., 2012).

In order to effectively integrate RAMS management into the railway systems engineering process, this research project will survey existing problems and challenges of railway companies connected to RAMS management, thus, discusses the ideas of risk-based RAMS management and the different approaches and strategies for implementing them.

### 2.1.2 Elements of railway RAMS

The concept of Railway RAMS is perfectly defined in CENELEC EN 50126 Standard, which develops specification and demonstration of **Reliability**, **Availability**, **Maintainability** and **Safety** (RAMS) of Railway Applications. The definition of these elements are described as in the following (CENELEC, 2018, Braband, et al., 2006, Sapoznikov, et al., 2009, Maboob, 2012)

**Reliability** ( $R_t$ ) is in terms of: (i) all potential system failure modes in the given application and environment; (ii) the likelihood of each failure occurring or, the rate of each failure occurring; and (iii) the effect of each failure on the system's functioning. The likelihood that an object will fulfil a specified function under certain conditions during a certain time interval, expressed mathematically as in the following with  $F_t(t)$  is the distribution function for failure probability in time  $t$ :

$$R(t) = 1 - F_t(t) \quad (2.1)$$

**Maintainability** ( $M_t$ ) is based on knowledge of: (i) time for planned maintenance; (ii) time for fault detection, identification, and location; (iii) time for system restoration (unplanned maintenance). Thus, it is the probability that a specific active maintenance operation for an item may be completed within a certain time span when executed under specified conditions and utilizing specified methods and resources.

Assuming that all external resources are available, **Availability** ( $A_t$ ) is defined as a product's capacity to fulfill a necessary function under certain conditions at a specific time or period. A non-repairable system's availability equals its reliability. In the case of a repairable system, availability can be calculated as

$$A(t) = 1 - F_t(t) - M_t(t) \quad (2.2)$$

**Safety**/safety-related failures are defined as (i) All system failure modes that potentially result in danger (safety-related failure modes) under all operating, maintenance, and environmental conditions. (ii) The possibility of each safety-related system failure mode occurring; (iii) The sequence and/or concurrence of events, failures, operational states, and environmental conditions, among others, in the application which might result in an accident. (i.e. a danger that results in an accident); (iv) The probability of occurrence of each application's events, failures, operational states, and environmental conditions.

A reliable system may be established by identifying, assessing, and managing the many variables that might affect the RAMS of the system. There are three ways that the RAMS of a railway system are affected:

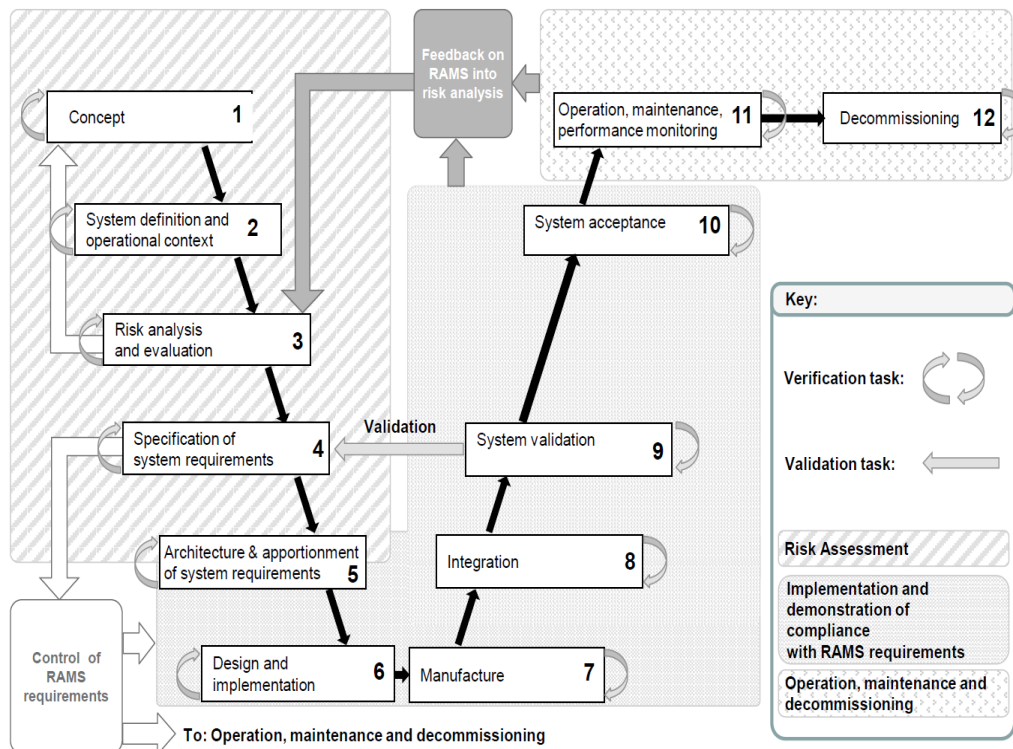
- **System conditions:** When failure causes are introduced internally inside the system, they might occur at any point during the life cycle of the railway system. Component or system failures are caused by mistakes made during the design and manufacturing processes.

- Operating conditions: The operating status is responsible for the origins of problems that occur. Environmental factors are also a contributing factor to these failures.
- In the case of maintenance circumstances, the sources of failures are caused by the actions of the maintenance team. Failures in the railway infrastructure, for example, can be caused not only by maintenance operations on the infrastructure, but also by the maintenance of rolling stock on the railway infrastructure.

RAMS's fundamental properties are influenced by the variables listed above. Similarly, the quality of RAMS data has an impact on the accuracy of the RAMS estimation. Reliability, availability, and maintainability are essential factors to consider when estimating and forecasting their respective levels. In many cases, not all of the information is gathered, and the lack of data can be a significant problem in RAMS analysis at times (Blischke and Murthy, 2003). According to Markeset and Kumar (2003), some of the elements that influence the handling of RAMS data have been identified. In addition to the data kind, data format, and detail level, these considerations included operator skills and capabilities, as well as location and other factors.

### 2.1.3 Life cycle management and RAMS requirements

The systems development life cycle is a method for planning, developing, testing, and deploying large technical systems. Systems engineers and developers employ a systems development life cycle to plan, design, create, test, and deliver information systems. The systems development life cycle seeks to offer systems that progress through each clearly defined step within scheduled periods and cost projections to build high-quality systems that meet or exceed customer expectations. From a management point of view, a project has two distinct life cycles: the project life cycle and the systems development life cycle. The project life cycle encompasses all project activities, whereas the systems development life cycle is focused on the needs of a specific product or service (Taylor, 2004).



**Figure 1.** V model representation of the lifecycle management of railway system

The life cycle management technique is being used in the railway industry to create reliable, safe, cost-effective, and enhanced quality railway systems. This life cycle method provides the fundamental principles and framework for planning, managing, implementing, controlling, and monitoring of all parts of a railway project, including the incorporation of RAMS, as the project progresses through the many phases of the life cycle approach.

This application is describe in V-model as in the Figure 1. The V-Model is an approach model established for planning and implementing system development initiatives. The 'Das V Modell' is the official German project management approach for planning and executing projects, considering the complete lifecycle of a system, which is very systems engineering (Childs, 2019). The V Model defines who does what and when in a project and uses decision gates to mark a milestone in the project's progress. In the V Model, test cases are used to check conformance between equivalent activities on either side of the V.

The next section provides a short explanation of the life cycle stages shown in the V diagram. The following are the overall project phase tasks, as well as the main task of the railway RAMS and the safety purpose (CENELEC EN 50126, 2018):

**Table 2.1** Overall project phase tasks (EN 50126, 2018)

| Life Cycle Phases                         | General Tasks  | RAM Tasks  | Safety Tasks   |
|---|--|--|--|
| Concept                                   | <ul style="list-style-type: none"> <li>• Establish and define the scope and purpose of project</li> <li>• Define project concept</li> <li>• Carry out financial analysis and feasibility studies</li> <li>• Set up management</li> </ul>   | <ul style="list-style-type: none"> <li>• Consider previously achieved RAM performance of similar projects</li> <li>• Consider and define RAM implications of new project</li> <li>• Review RAM targets</li> </ul>  | <ul style="list-style-type: none"> <li>• Consider previously achieved safety performance of similar project and application conditions</li> <li>• Consider and define safety implications of new project</li> <li>• Safety policy and safety targets are reviewed</li> </ul>   |
| System definition and operational context | <ul style="list-style-type: none"> <li>• Define system mission-profile</li> <li>• Prepare system-level technical description</li> <li>• Identify operation and maintenance strategies</li> <li>• Identify operating and maintenance conditions</li> <li>• Identify influence of existing interfaces of infrastructure and local constraints</li> </ul> | <ul style="list-style-type: none"> <li>• Perform preliminary RAM analysis, based on historical data of RAM</li> <li>• Define RAM policy</li> <li>• Identify life cycle-based operation and maintenance conditions</li> <li>• Identification of the influences on RAM of existing interfaces of infrastructure and other constraints</li> </ul> | <ul style="list-style-type: none"> <li>• Perform preliminary hazard analysis, based on th historical data of safety</li> <li>• Create safety plan</li> <li>• Define risk acceptance criteria</li> <li>• Identification of the influences on safety of existing interfaces of infrastructure and further constraints</li> </ul> |
| Risk analysis and evaluation              | <ul style="list-style-type: none"> <li>• Project-level risk analysis (may have to be repeated at several stages)</li> </ul>  | <ul style="list-style-type: none"> <li>• Not relevant</li> </ul>   | <ul style="list-style-type: none"> <li>• Perform systematic hazard analysis and safety risk analysis on system level</li> <li>• Set up central hazard log</li> <li>• Make complete risk assessment (= risk analysis + risk evaluation)</li> </ul>  |
| Specifications of System requirements     | <ul style="list-style-type: none"> <li>• Requirements analysis</li> <li>• System specific</li> <li>• Specify local environment</li> </ul>  | <ul style="list-style-type: none"> <li>• Specify system RAM requirements</li> <li>• Define RAM acceptance criteria</li> </ul>  | <ul style="list-style-type: none"> <li>• Specify system safety requirements</li> <li>• Define safety acceptance criteria</li> </ul>  |

|   |  |   |   |
|---|--|---|---|
|   | <ul style="list-style-type: none"> <li>• Define system assurance, demonstration, and acceptance criteria</li> <li>• Establish verification and validation plan</li> <li>• Establish management, quality, integration, and organization requirements</li> <li>• Introduce and implement change control procedure</li> </ul> | <ul style="list-style-type: none"> <li>• Define system functional concept and structure</li> <li>• Establish RAM program on system level</li> <li>• Establish RAM management on system level</li> </ul>   | <ul style="list-style-type: none"> <li>• Define safety-related functional concept and requirements</li> <li>• Establish safety management on system level</li> </ul>  |
| Architecture and Appointment of system requirements | <ul style="list-style-type: none"> <li>• Apportionment of system requirements</li> <li>• Define subsystem and components requirements and acceptance criteria</li> </ul>   | <ul style="list-style-type: none"> <li>• Apportionment of system RAM requirements to the specific subsystem and component RAM requirements</li> <li>• Define subsystem and components RAM acceptance criteria</li> </ul>  | <ul style="list-style-type: none"> <li>• Apportionment of system safety targets and requirements for specific subsystems and components</li> <li>• Define subsystem and components safety acceptance criteria</li> <li>• Update system safety plan, if necessary</li> </ul>   |
| Design and implementation                           | <ul style="list-style-type: none"> <li>• Planning</li> <li>• Design and development</li> <li>• Design analysis and testing</li> <li>• Design certification</li> <li>• Implementation and validation</li> <li>• Design of logistic support resources</li> </ul>   | <ul style="list-style-type: none"> <li>• Implement RAM program by review, analysis, testing and data assessment, reliability, availability, maintainability and maintenance, and analysis logistic support</li> <li>• Control programs: RAM program management, control of suppliers and contractors</li> </ul> | <ul style="list-style-type: none"> <li>• Implement safety plan by review, analysis, testing, and data assessment. It includes: <ul style="list-style-type: none"> <li>• Hazard log</li> <li>• Hazard analysis and risk assessment</li> </ul> </li> <li>• Undertake program control for safety management and supplier control</li> <li>• Preparation of generic safety case</li> <li>• Preparation of generic application safety case, if required</li> </ul> |
| Manufacturing                                       | <ul style="list-style-type: none"> <li>• Production planning</li> <li>• Manufacture</li> <li>• Manufacture and test subassembly of components</li> <li>• Documentation management</li> <li>• Design associated trainings</li> </ul>  | <ul style="list-style-type: none"> <li>• Requires environmental stress screening</li> <li>• Requires RAM improvement testing</li> <li>• Initiate failure reporting and corrective action system (FRACAS)</li> </ul>   | <ul style="list-style-type: none"> <li>• Implement safety plan (by following review, analysis, testing and data assessment)</li> <li>• Use and update hazard log</li> </ul>   |
| Integration   | <ul style="list-style-type: none"> <li>• Subsystem assembly and system-level integration</li> <li>• Multiple subsystem installations</li> </ul>  | <ul style="list-style-type: none"> <li>• Start trainings for the maintenance people from a maintainer</li> <li>• Establish spare parts and tool provisionrelated (inventory) lists</li> </ul>   | <ul style="list-style-type: none"> <li>• Establish installation program</li> <li>• Implement installation program</li> </ul>  |
| System validation                                   | <ul style="list-style-type: none"> <li>• System-level commissioning</li> <li>• Perform transition or probationary period of operation</li> </ul>   | <ul style="list-style-type: none"> <li>• RAM demonstration (and evaluation in reference to the penalty criteria, e.g., trip losses during operation times)</li> </ul>   | <ul style="list-style-type: none"> <li>• Establish and then commission program</li> <li>• Preparation of application-specific safety case begins</li> </ul>   |

|   |   |   |   |
|---|---|---|---|
|   | <ul style="list-style-type: none"> <li>• Carry out related trainings</li> </ul>   |   |   |
| System-acceptance                                 | <ul style="list-style-type: none"> <li>• Observe acceptance procedures, based on acceptance criteria</li> <li>• Documented evidence for acceptance</li> <li>• System bringing into service</li> <li>• Continue transition or probationary period of operation, if necessary</li> </ul>                              | Assess RAM demonstration in reference to the acceptance criteria  | Assess application specific safety case in reference to the given acceptance criteria   |
| Operation and maintenance, performance monitoring | <ul style="list-style-type: none"> <li>• System operation for long-term basis</li> <li>• Maintenance activities based on system-level considerations</li> <li>• Collect operational performance statistics and analyze and evaluate collected data</li> <li>• Record of changes request and modification</li> </ul> | <ul style="list-style-type: none"> <li>• Implement and maintain FRACAS process for the acquisition and recording of RAM performance data.</li> <li>• Maintain FRACAS and periodically review FRACAS records.</li> <li>• Establish records to trace the RAM tasks undertaken.</li> <li>• Reports of RAM performance analysis and evaluation</li> </ul> | <ul style="list-style-type: none"> <li>• Implement and maintain process for the acquisition and recording of safety performance data.</li> <li>• Perform an impact analysis in case of changes and reapply process if needed.</li> <li>• Records to trace the safety tasks undertaken.</li> <li>• Establish reports of safety performance analysis and evaluation.</li> </ul> |
| Decommissioning and disposal                      | <ul style="list-style-type: none"> <li>• Planning and procedure of decommissioning and disposal</li> </ul>  | Identify the RAM impact of decommissioning and disposal.  | <ul style="list-style-type: none"> <li>• Identify Safety impact for the decommissioning and disposal and its implementation</li> </ul>  |

The responsibilities for the tasks in the different life cycle stages are determined by the contractual and, in certain cases, legal relationships that exist between the stakeholders concerned. It is critical that the associated obligations be defined and agreed upon. The RAMS management process must be carried out under the supervision of an organisation, with qualified employees allocated to RAMS-related duties. Personnel competency, comprising technical knowledge, credentials, relevant experience, skill, and appropriate training, shall be selected, assessed, and documented in line with the provided requirements to be set by the project-specific safety management organisation (Mahboob, 2018).

## **2.2 Risk management**

### **2.2.1 Definitions of risk, hazard and risk management**

Throughout the lifecycle of a project, risk management is a vital and helpful instrument. To comprehend the method's content and requirements, it is important to study several risk and safety definitions.

Risk is defined as "the frequency and severity of accidents and events resulting in injury (caused by hazards)" (ORR, 2015). Overall, the risk is not undesirable, but the negative impacts of risk must be weighed against the possible advantages of the accompanying opportunity (Van Scoy, 1992).

Technical approaches assume the basic unit of risk is the average expected probability of events that negatively impact humans and their environment. In this case, the risk is quantified by applying probability weights to the negative effects. This approach is used in actuarial, healthcare, environmental, and probabilistic risk measurement, as well as risk analysis in general. An important flaw in this approach is that it relies on subjective decisions to define undesirable effects and probabilities. However, this is one of the main criticisms of risk analysis techniques. Technically, the world is predetermined, and while the probability and risk of events can be predicted, they will inevitably occur. Achieve perfect foresight. This approach is less viable when low probability events have severe consequences. Also, reducing risk to a single dimension may be misleading: our assessment of a low-probability risk with a severe effect may be different from a higher-probability risk with a milder effect (Bernstein 1996).

All social science approaches consider the causality of risks through social processes. The economy still resembles technology. The subjective utility replaces the undesirable effect. It expresses satisfaction or dissatisfaction with an event. The advantage is that, in addition to negative effects, the possibility of profit (positive utility) is also measurable, replacing pure risks (Vasvari, 2015). In this case, expected utility measures risk. It is possible to retain benefits to the greatest extent possible while mitigating risk through the most efficient allocation of available resources. However, an individual utility cannot be aggregated due to subjective scale differences and ethical issues. Probability judgment remains technical and objective.

Unlike economics, psychological approaches value subjective judgment more. They do so in three ways. There are biases in assessing probability information and thus risk even when decisions are based on quantified values. Finally, context influences risk perception. Inconsistencies in decisions result. Possibly, along with effects, probabilities and aggregation methods are also subjective in psychological approaches. The result is a subjective expected value based on perceived probability (Renn 1992). This approach's focus on personal, subjective risk perception is a disadvantage. Personal preferences are difficult to aggregate, and individual decisions do not evaluate social effects. Nonetheless, the value of this technique stems from the application of human attitude and response mechanisms in complex engineering systems (Aven, 2015).

In the field of system engineering, Chapman and Ward (1997) defined project risk as to the consequences of considerable uncertainty regarding the degree of project performance attainment. Project risks include danger, loss, and vulnerability to mischance (Turner, 1993). To summarise, the risk is an inherent part of each project, varying in frequency and intensity with each stage, and it is critical to analyse and manage risk to keep damages and investment costs in control.

Often, risk, danger, and threat are used interchangeably. Risk has been defined as the possibility that someone or anything of value may be harmed or damaged as a result of a hazard (Woodruff, 2005), whereas "hazard" refers to any hazardous situation or possible cause of an unwanted occurrence with the potential for injury or damage (Reniers, Dullaert, Ale, & Soudan, 2005). According to Garland (2003), risk, unlike hazards, never exists outside of our awareness. Risk is only 'known' probabilistically because it concerns the future. Risk analysts like Kaplan & Garrick (1981), as well as social scientists, admit that danger is contingent on what you know and don't know, and so subjective. Adams (2003) raises an essential point about how you learn about risk. Some are obvious (vehicle accidents), others are scientifically proven (cholera), while a third set of virtual risks escapes scientific consensus (global warming). Adams' central tenet is that the meaning and management of risk rely on how future knowledge is inferred. Additionally, risk has been defined as a measure of the severity of a hazard in conditions of uncertainty, or as a measure of the likelihood and severity of unfavourable consequences (Haimes, 2009). By and large, the term "hazard" should be defined as a property of substances or processes that has the potential to cause harm (Høj & Kröger, 2002).

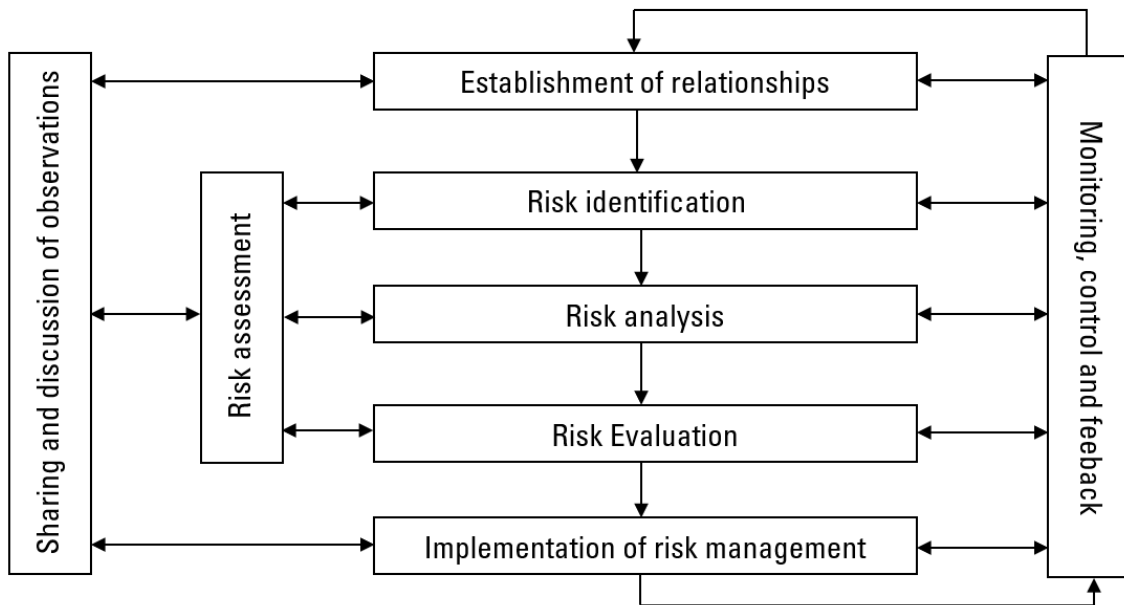
To be more detailed, as a scientific endeavour, hazard is a process, phenomenon or human activity that may cause loss of life, injury or other health impacts, property damage, social and economic disruption or environmental degradation (UNGA, 2016, 2017). Historically, there was a tendency to associate the term 'hazards' with 'natural phenomena', often with a sudden or acute impact, and 'hazardous materials'. However, the current reflects the evolution over several decades of the field of disaster risk reduction to a broader scope of hazards leading to events with both short- and long-lasting effects. It is important to recognise that the expanded definition of hazard as a process, phenomenon or human activity, requires an examination of the relationship between the concepts of hazard, exposure, vulnerability and capacity, where 'hazard' is the potential occurrence of an event within a prescribed time and space; 'exposure' constitutes the assets of interest and at risk (such as the environment, the economy, buildings, or people); 'vulnerability' is the susceptibility of those assets to damage or impact to a hazard; and 'capacity' is the combination of all the strengths, attributes and resources available within an organisation, community or society to manage and reduce disaster risks and strengthen resilience (UNDRR, 2020, RSSB, 2002).

Risk management is the process of identifying and evaluating risks and taking steps to eliminate or reduce them (to the extent that it is reasonably practicable) through the implementation of control measures. Risk management refers to the process of reducing risks to a level deemed tolerable by society while also ensuring the controlling, monitoring, and public communication of risks and their effects on society (Morgan, 1990). It is also possible to describe risk management as a collection of cultural norms, practices, and organisational structures geared toward exploiting prospective opportunities while simultaneously controlling undesirable consequences (Galante et al., 2014).

Burke R. (1999) defined risk management as "the processes concerned with identifying, analysing, and responding to uncertainty throughout the project life cycle"; this was nearly identical to the summary provided by Dey (1999), who stated that there are threefold in the risk management process, including (i) identifying risk factors, (ii) analysing their effects, and (iii) responding to risk factors.

The risk management process, according to Turner (1993), is divided into five stages: (i) identifying the source of risk, (ii) determining the impact of individual risks, (ii) assessing the overall impact of risks, (iv) determining what risks can be reduced, and (v) controlling the identified risks.

## THE RISK MANAGEMENT PROCESS



**Figure 2** The Risk management process (Turner, 1993)

According to ISO 31000: 2018, risk management encompasses any efforts that are undertaken to lower the likelihood of a risk occurring or the severity of its consequences being reduced to an acceptable level. The risk management process described in this study is divided into six major phases as in the Figure 2.

First phase of risk management is to identify the relationships that have an impact on the operation of the system. The process can be thought of as a first scenario evaluation, during which a review of the internal and external surroundings, as well as their characteristics, is conducted as part of the process. Additionally, it is at this stage that the ultimate purpose of risk management should be determined. Secondly, risk assessment which included three sub-steps such as risk identification, risk analysis and risk evaluation are implemented. Risk identification is the process of finding, listing, and characterizing hazards. CSM RA defined risk analysis as the process of accounting every piece of information to identify and measure the hazards affecting the project better to understand the concepts of risk assessment and risk management. The risk evaluation is the final stage of risk assessment and it is used to determine the risk acceptance level (ORR, 2015).

They conclusion that risk management is the systematic application of management rules, procedures, and practices to the task of analysing, evaluating, and controlling risks in an organisation. To summarise, there was an actual, one-of-a-kind risk management theory divided into three stages: analysis, evaluation, and response to risks. When a functional failure has a genuine clear potential for a catastrophic effect during the risk responding phase, the linked risk does not need to be decreased if the failure rate is less than or equal to  $10^{-9}$  per operating hour and can be established as risk acceptance criterion (EC, 2009).

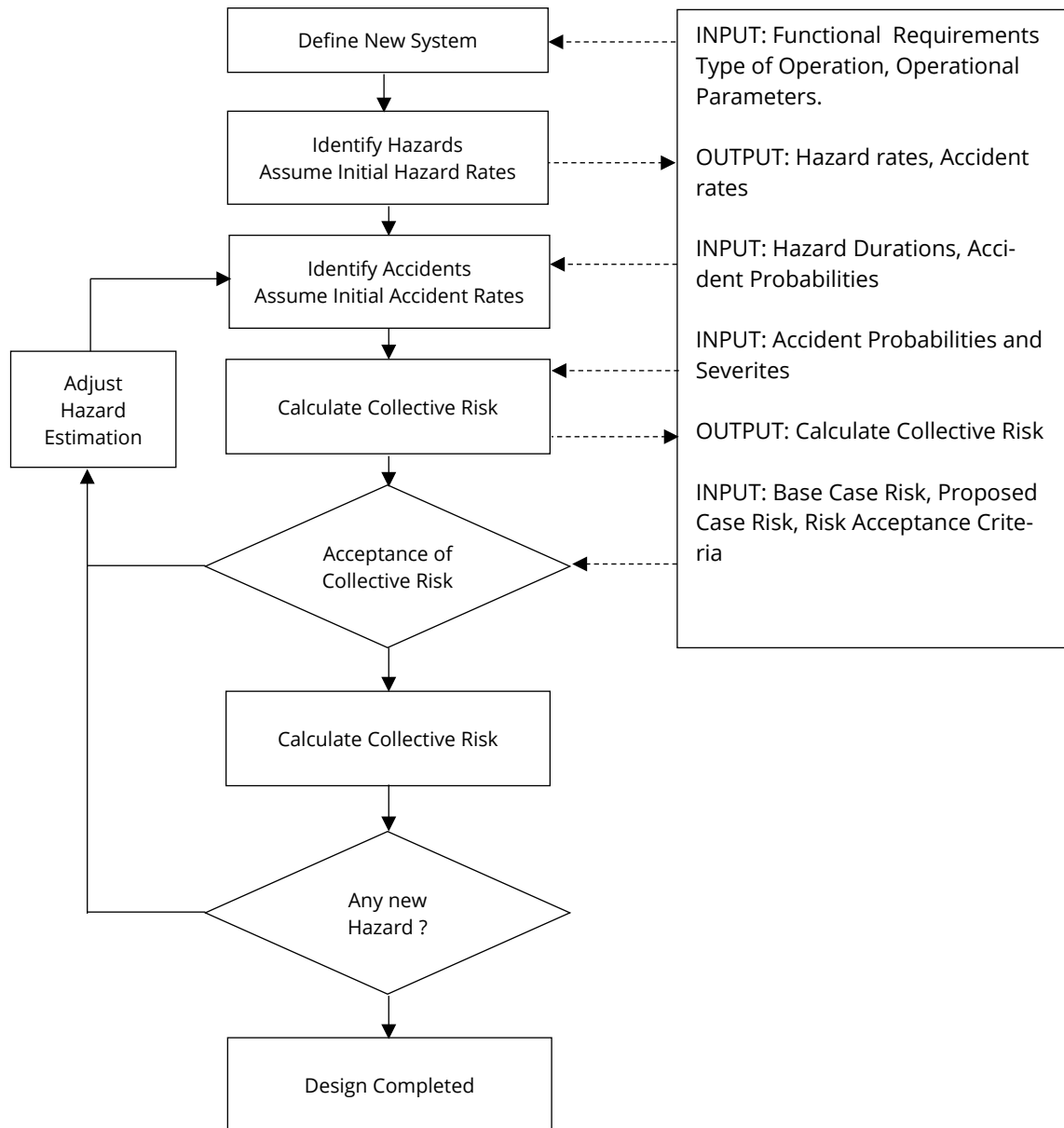
These other parts of these process is aim to to reduce the magnitude of risk or eliminate it if possible. To be more detailed, risk mitigation is the process of developing plans to manage, eliminate, or reduce risk to an acceptable level. Once a plan is implemented, it is continually evaluated for effectiveness with the goal of revising the course of action as necessary. Among the risk mitigation strategies available are the following: (i) Assume/Accept, (ii) Prevent, (iii)



Control, (iv) Transfer, (v) Monitor/Observe. Each of these options requires the development of a plan, its implementation, and subsequent evaluation of its effectiveness.

### 2.2.2 Risk assessment – Procedure and process

According to USDT (2009), primary steps in the risk assessment can be summarized in the 7 steps in this following figure:



**Figure 3** Risk Assessment Procedure (EN 50126:2018)

1. Adequately define and design the proposed system.
2. Identify key hazards and the consequence of corresponding failure to gain hazard rates (HR) and accident rates (AR). The hazard rates must be adjusted and classified to various subsystems to ensure the adequacy.

3. Identify comprehensive accidents and calculate accident rates which concentrate on the interaction between system and operational environment. The results of this step are accident probabilities and accident severities.

4. Analyse and calculate collective risks including accidents.

5. Compare the value of collective risks and risk acceptable criteria. If the value of collective risks is lower than or equal to risk acceptable criteria, changing to next step; vice versa, adjusting the hazard rate estimation.

6. Compare the value of initial hazard rates and tolerable hazard rates. If the value of collective risks is lower than or equal to tolerable hazard rates, continuing with system design; vice versa, adjusting the hazard rate estimation.

7. If one cannot indicate any new hazards, the design will be completed. Because of the changing or expanding the function or the operational method after the new system is set up, additional hazards are likely to be diagnosed during the design phase and therefore, the risk assessment is then repeated the assessing loop.

To be more detailed for important steps, ORR (2015) indicated the fundamental contents of risk identification, risk analysis and risk evaluation as the following:

1. Risk and hazard identification:

The purpose of risk identification is to compile a list of risk variables that may fail and result in safety breaches and quantify the significance of each risk factor and their interactions (Redmill, 2002, Shen, 1997). As a result, risk identification is particularly pertinent to the following activities:

- Identify or validate (if necessary) all significant types and sources of risk as extensively as feasible.
- As certain the likely causes of these risks.
- Classify the risks into theme families.

The purpose of hazard identification is identifying and listing all reasonably predictable risks associated with the intended operation of the system, in its normal operational environment, that are analysed and measured further in next steps (ORR, 2015, USDT, 2009).

Based on the guidelines of CSM RA (2015), to identify hazard systematically it is decisive to take into accounts these following factors:

- System requirement specification and system design description.
- System life cycle including the maintenance.
- Operational and maintained conditions
- Human factors influencing to operation.
- Relevant foreseeable failures.

Using the information gained from the context, this is accomplished through a structured study with several well-known techniques including:

- Structured group discussions / brainstormings.
- Risk matrices, risk graphs or risk priority numbers.
- Failure mode and effects analysis (FMEA).

- Fault trees and event trees and the simulation approaches for
- Bayesian Networks, Markov's Chain or Petri Nets.

Diverse and comprehensive Risk Identification investigations are a prominent topic of research in railway operations studies. These studies are conducted on several subsystems of the railway system or a particular generic accidents, for instance: tracks and infrastructure (Sadeghi et al., 2015, Matsumoto et al., 2016, Sun, 2018), rolling stocks (Dinmohammadi et al., 2016, Souza et al., 2019), derailments and train collisions (IRICEN, 2014, Britton et al., 2017, Anderson and Barkan, 2004, Hou et al., 2020, Wu et al., 2015), signalling and controlling system (Jurtz, 2019, Dodgson et al., 2003, Yang and Wang, 2000), railway staffs and safety culture (NTC, 2017). In general, these studies are conducted in one of two ways:

- by providing an overview of accident statistics and analysing types of generic hazards, or
- by modelling a subsystem or a typical failure/accident using quantitative methods such as Petri Nets, Bayesian Network, or Monte Carlo simulation.

The outcomes of approach (i) are typically accident patterns and the proportion of common safety hazards, from which you may derive a strategy, regulation, or processes for safety management in the national railway sector. The results of approach (ii) are frequently employed at the system or subsystem level to increase the capacity or dependability of a component or subsystem. Although these results are very precise and have tremendous value in technical analysis, the system must be operational or the railway industry must manufacture its own equipment as a prerequisite. From this analysis, it is noticeable that there are fundamental differences between establishing risk analysis research in developed railway industries such as Europe, China, the United States, and Japan, and in lower-level railway systems that have not manufactured their own railway components yet. To be able to manage the imported modern railway system, these countries require more extensive studies than method (i) but they lack the necessary technological basis to conduct studies according to approach (ii).

## 2. Risk analysis

Once the potential risks have been initially identified, an assessment is made for every identified risk. There are various accessibilities for measuring methods such as:

First, a combined - technical and financial - Qualitative Risk Analysis (QRA), as a straightforward and 'easy to use' method, allows to assess and classify the risks according to their criticality, and to find appropriated mitigating measures (Heldman, 2005). The likelihood of a risk event occurring, and the potential impact of that risk on costs, schedules and performances of the system are assessed at this stage. This assessment is initially made by estimating these effects and assigning an order of magnitude scale value for likelihood and severity. The Likelihood of occurrence of a risk is evaluated in function of available and collected data and the local knowledge of the context (feedback on local experiences), and actualised. In case of combined or linked risks, the relationships (conditional sequences, independence, etc) between their related probability laws are studied and characterised in different scenarios, permitting to approach the global risk of the project in each case. The risk severity is an assessment that defines the negative impact of the feared event in case it effectively occurs. This impact can be assessed in different terms. The following severity components are considered in the risk matrix: (i) Cost (additional costs supported by one of the stakeholders of the project), (ii) Delay (supplementary delay in any of the project phase upstream the setting up of the system; (iii) Performances (temporary or permanent impact on

the performances of the system). This method was also described as semi-quantitative of risk assessment in the case studies of Braband (2005, 2012), and research on semi-quantitative graph of Milius (2010).

Second, another method (FTA, ETA, BN, and so on) used to determine the individual and collective risk by assessing:

- the frequency of occurrence of the threat, which can be measured in [events / year];
- the vulnerability of the system with respect to the threat, that is to say the probability that the threat will cause the expected consequences (damage)
- estimate of the measure of the expected damage occurring after a successful attack.

Therefore, it is a quantitative way to express the individual risks in the loss of money and can expand to describe the overall risk by sum of individual risks. Furthermore, by classifying and quantifying all the individual risks, it is possible to determine the risk mitigation (Flammini et al., 2009). In the present study, it is significant to determine relevant and consequential risk factors from risk variables to approach the identification of risk factors. By examining the correlation between variables, factor analysis can classify them into specific groups, consequently, assist in understanding the inherent risk factor structure (Ghosh et al., 2004).

### 3. Risk response

According to their level of criticality, risks will be responded to and thus controlled, in a strategic and efficient manner. The approaches to be adopted are:

- Risk avoidance: changes to eliminate the risk or to protect the project from the risk by changing the scope, adding time or resources.
- Risk transfer: transfers the impact of risk by contracting out several aspects of the work.
- Risk mitigation: applies preventive actions or decisions are identified as convenient to minimize the level of criticality of a defined risk, mitigate its severity or/and decrease its probability of occurrence.
- Risk monitoring: measures aim to assure the follow-up of a specific parameter of event that could release a certain risk.
- Risk acceptance: does not change the project to deal with the risk and agrees to address the risk in the case of occurring

Overall, based on the particular project, the assessment of the criticality of risks permits to arrange them hierarchically and to classify them into three categories with the correspondent solutions, according to their criticality level:

- Acceptable risk: (i) Do not implement any measure; (ii) Implement monitoring to avoid escalation of risk; (iii) When the risk is monetarily assessed, application of the provision for contingencies in cost assessment and financial analysis.
- Risk to follow-up: (i) Do not implement any mitigating measure; (ii) Study of possible and appropriate mitigating measures in case of an increase of the criticality of the risk; (iii) Implementation of appropriated monitoring measures in order to detect changes in the criticality of the risk; (iv) Research of supplementary information or ordering of new studies; When the risk is costly assessed, application of the provision for contingencies in cost assessment and financial analysis.

- Risk to treat: (i) Identification of the appropriate avoidance, transfer, mitigating or monitoring measures; (ii) Identification of the most appropriate responsibility of the implementation of such measures for each scenario, in relation with the partition of risks between project stakeholders; (iii) Definition of an action plan to implement the measures. Designation of a pilot responsible for the implementation of such plan.

### 2.2.3 Risk acceptance principle and Safety Integrity levels

#### Risk acceptance principle

According to numerous points stated previously, it is critical to ascertain the risks, implement risk-reducing measures, and so improve the situation. However, there is a challenge in balancing two conflicting objectives: (i) a desire to eliminate all risks through all possible means and (ii) limited resources to deal with all predictable risks. As a result, there are two unavoidable questions: how much risk can we remove before stopping, and how do we balance these two objectives.

For complex systems, risks will often be introduced to the general public as well as to a special group of individuals, typically workers or nearby residents, and both criteria for societal risk and individual risk will have to be complied with. Often, special consideration is given to the risk of events with low frequency but high severity, as addressed in Henselwood and Phillips (2009).

CMS RA report (ORR, 2015) proposed a notion of "risk acceptance criteria" that would be used to assess if the risk level is sufficiently low that no urgent action to lower it is required. To be more specific, tolerating a risk implies that we do not consider it as insignificant or something we can disregard, but rather as something we need to monitor and minimise further if and when possible.

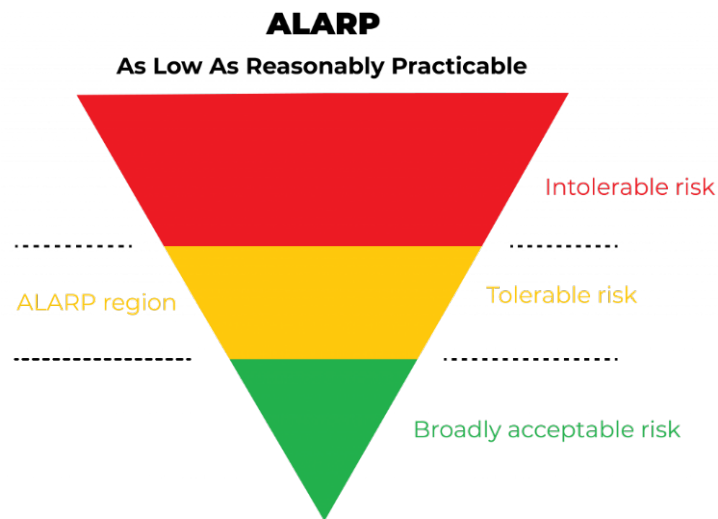
The approach to risk acceptance principles (Vanem, 2012, Ditlevsen, 2003) can be gained from several perspectives, including:

- the benefits gained from taking the risks,
- the degree of control over the risk,
- risk aversion – one catastrophic event is worse than a series of minor accidents,
- the time until effects are felt, and
- the time since the risk was realised

Several common used principles for risk acceptance are:

**ALARP** – As low as reasonably practicable: Both the risk level and the cost of mitigating the risk are examined, and all risk reduction measures should be undertaken if the cost is reasonable achievable in light of cost-effectiveness factors. This principle is widely accepted, reflected in the risk matrix and lead to continuously reduce risk.

This approach introduces the concept of three different risk zones such as: (i) Unacceptable region – risk is too high to be acceptable and risk reducing measures must be introduced; (ii) ALARP-region – risk is below the unacceptable level, but is not acceptable either without considering further measures to reduce risk; and (iii) Broadly acceptable region – risk is broadly acceptable and no further measures are considered necessary.



**Figure 4** ALARP acceptance region

The Gross Cost of Averting a Fatality (GCAF) and the Net Cost of Averting a Fatality (NCAF) are two alternative criteria frequently used in safety regulation to establish the limits of what is reasonably achievable in conjunction with the ALARP concept. These are cost-effectiveness measurements that are used to compare the increased cost of risk control choices to the risk reduction in terms of deaths saved. Additionally, the NCAF criterion considers the potential economic advantage of the risk control solution (Bowles, 2003, HSE 2001b).

**GAMAB** - is an abbreviation for the French phrase 'Globalement au moins aussi beau', which translates as 'Globally at least as excellent'. The principle establishes the minimum level of risk that a new transportation system in France must meet, requiring new systems to have a total risk level that is as low as any existing equivalent system globally (EN 50126, 2018). By applying this approach, the decision-maker is relieved of the responsibility of developing a risk acceptance criterion, as one is already provided by the current level of risk. However, in order to make the criterion operational, it is necessary to define what constitutes a globally good and equivalent system. EN 50126 (2018) states that the GAMAB-analyst is free to choose both the approach and the comparison metrics. This necessitates the assessment of the risk posed by both systems, which results in extra work if the reference system lacking risk data (Schäbe and Wigger, 2000, Schäbe, 2001).

Johansen (2010) suggests that a new solution should not result in an increase in risk when compared to current practise. This is similar to the concept of 'good practise' used in simplified ALARP evaluations, with the belief that generally accepted rules of conduct provide acceptable risk. GAMAB's 'at least' criteria goes beyond this, assuring not only that state-of-the-art information is considered, but also that additional learning is encouraged. Due to the requirement that new systems perform as well as or better than the best system on the market, GAMAB is a learning-oriented bootstrapping approach. However, it cannot overcome bootstrapping's core flaw, which is the erroneous assumption that the current level of risk is acceptable. Additionally, Rausand & Utne (2009) draw parallels between GAMAB and the EU directive, questioning the validity of comparing a low-cost gadget to a much more expensive counterpart. Because GAMAB does not involve cost-benefit analysis, Trung (2000) asserts that unrealistic safety objectives may be established. In this regard, one can wonder whether GAMAB is impeding rather than fostering improvement by rejecting alternatives based on erroneous reference standards.

**MEM** - is an abbreviation for minimum endogenous mortality,' a German principle mandating that new or updated technological systems do not result in a considerable increase in Potential Loss of Life to any person (Schäbe, 2001). The likelihood of dying from natural causes is used as a reference level for risk acceptance. MEM is based on the fact that death rates vary with age and the idea that technology systems contribute to a fraction of each death rate (Nordland, 2001). In contrast to ALARP and GAMAB, MEM provides a universal quantitative risk acceptance criterion derived from the least endogenous mortality rate.

MEM, unlike GAMAB, can be assigned to subsystems (Schäbe, 2001). It may thus incorporate both distributional and global risk issues, depending on the pragmatic apportionment of risk. The explicit idea of MEM, like GAMAB, is rarely found outside of its nation of origin, while comparable notions are employed by numerous authorities. Skjong et al. (2007) outline the commonly used approach of 'comparison with recognised hazards,' in which risk criteria are established by comparing technical risk to those implicit in human activity.

**The precautionary principle** - states that "where there is a risk of substantial or irreversible environmental damage, a lack of full scientific knowledge may not be used as an excuse to postpone appropriate measures to avert degradation" (UN, 1992). The precautionary principle should be applied when there is solid cause to suspect, based on empirical data or reasonable causal hypotheses, that substantial harm may occur, even if the risk of harm is distant. The scientific data acquired at this level of consequences and likelihood reveals so much uncertainty that it is impossible to evaluate conjectured outcomes with enough confidence to proceed to the following phases of the risk assessment procedure.

To summarise, ALARP identified the maximum tolerated level and attempted to ameliorate conditions below this level. GAMAB emphasised that the new system should be at least as excellent as old systems, whereas MEM emphasised that new systems should not considerably increase technological risk.

### Safety Integrity levels - SIL

The safety integrity level (SIL) indicates the degree to which an electrical/ electronic/ programmable electronic system mitigates risk (Marszal, 2001).

Functional safety, as defined by IEC 61508:2010 (2010), is the level of protection provided by control systems for an entire process or plant. Functional Safety was developed in response to an increasing demand for increased confidence in safety systems. Historically, safety standards have been largely prescriptive in nature, rather than performance-based. Functional Safety is a term that refers to a safety system that is reliant on the logic solver, sensors, and final elements operating properly in order to achieve a desired level of risk reduction. Functional Safety is achieved when all safety functions are carried out successfully and the process risk is reduced to an acceptable level.

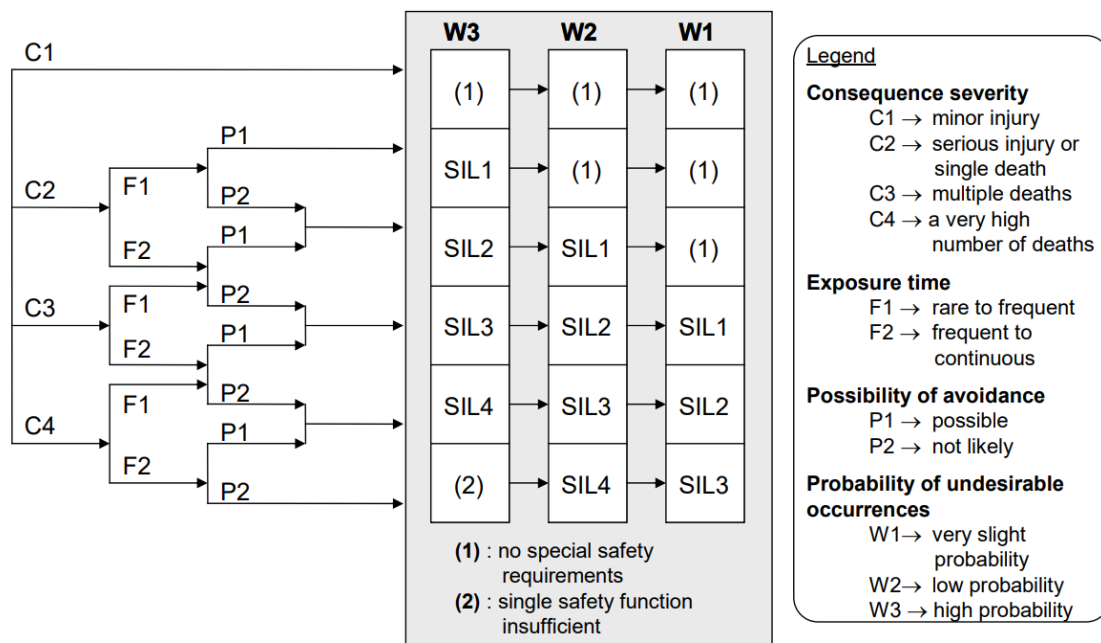
**Table 2.2** Quantitative SIL requirements (EN 50129, 2018)

| Safety Integrity Level | Tolerable Functional (unsafe) Failure Rate – TFFR (per hour) |
|------------------------|--|
| <b>SIL 4</b>           | $10^{-9} \leq \text{TFFR} \leq 10^{-8}$                      |
| <b>SIL 3</b>           | $10^{-8} \leq \text{TFFR} \leq 10^{-7}$                      |
| <b>SIL 2</b>           | $10^{-7} \leq \text{TFFR} \leq 10^{-6}$                      |
| <b>SIL 1</b>           | $10^{-6} \leq \text{TFFR} \leq 10^{-5}$                      |

A SIL criterion, i.e. the required risk reduction, is characterised as the difference between the risk prior to the installation of a safety instrumented system (SIS) and the risk that is bearable. Safety integrity is defined in IEC 61508 (1998, p.31) as the probability of a safety-related

system/SIS satisfactorily performing the required functions under all stated conditions within a specified period of time.

Safety integrity is classified into four distinct categories, ranging from SIL 4 to SIL 1. The levels are defined by the maximum permissible failure frequency and the needed range of risk reduction. When determining whether a SIL 1, SIL 2, or SIL 3 system is required, the first step is to conduct a Process Hazard Analysis to ascertain the functional safety requirement and to establish the acceptable risk level. After accounting for all risk reduction and mitigation effects of the Basic Process Control System (BPCS) and additional layers of protection, comparing the residual risk to their risk tolerance. If the level of risk remains unacceptably high, a risk reduction factor (RRF) is calculated, and a SIS / SIL requirement is calculated.



**Figure 5** A risk graph to determine SIL level (Beugin et al., 2006)

SILs associated with certain safety functions can be assigned to only one function. Typically, the safety integrity of a system or piece of equipment is listed as the highest SIL of the functions it performs. However, it is extremely rare for all functions within a system or piece of equipment to satisfy the highest SIL required. Recently, some clients have demonstrated a proclivity for requesting that a system or piece of equipment meet a specific SIL, despite the fact that, if this is required at all, just one or two functions inside that system may require a SIL. This is especially true for systems such as CTC (Centralised Train Control) or ATO (Automatic Train Operation).

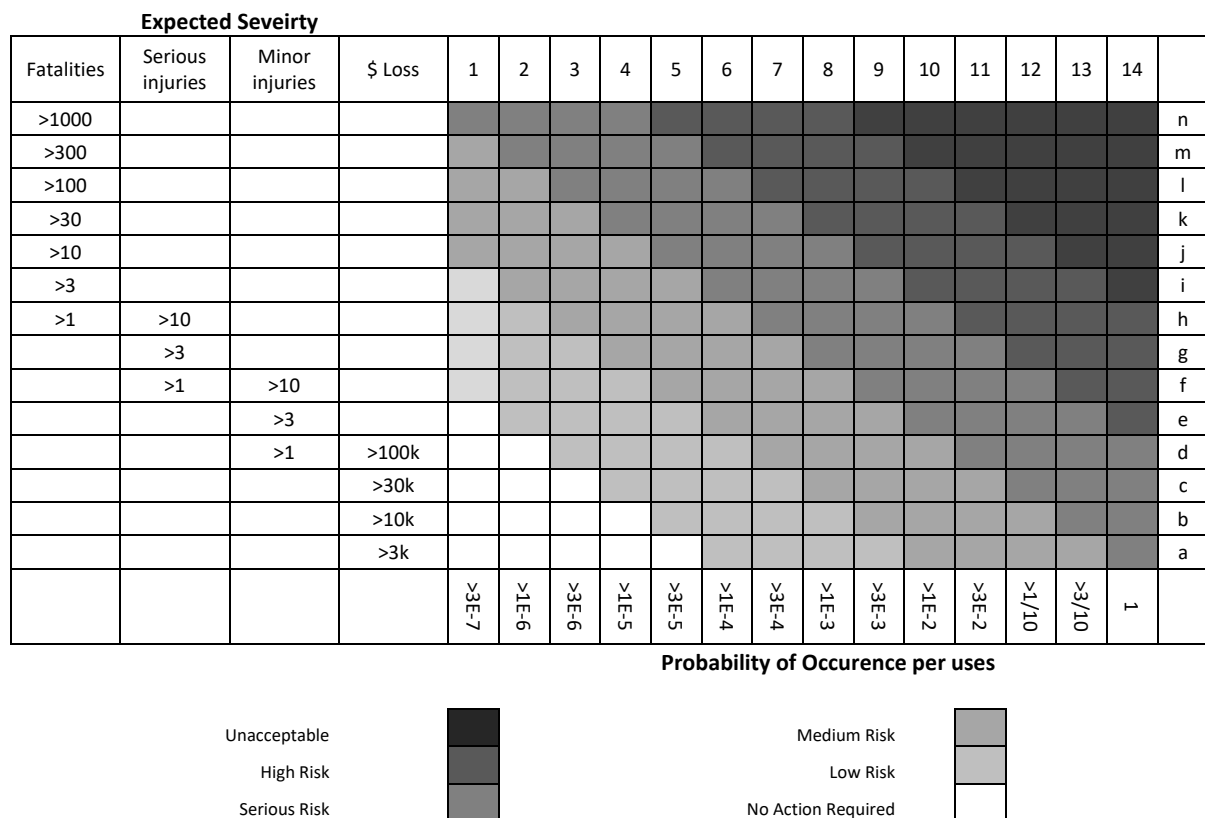
In certain circumstances, Safety Integrity Levels (SILs) for equipment and subsystems are specified without regard for actual safety needs, functions, or system architecture, solely because of the false idea that a high SIL must be a 'good thing' and represents the 'state of the art'. Regrettably, some suppliers contribute to this SIL rise by advertising their products as 'superior' because they have been assessed to a specific SIL in specific markets and configurations. These suppliers choose to disregard any deficiencies in their architecture or subsystems that result in the requirement for any of their specific subsystems to carry a specific SIL, as well as differences in the application and/or the fact that other suppliers' architectures may be different but equally satisfactory (IRSE, 2015).



## 2.3 Risk assessment methods

### 2.3.1 Risk Matrices

Risk matrices are a frequently used tool in the Risk Evaluation phase of the Risk Management process. Cook (2008) defined the risk matrix as a tool or technique for assigning a risk level to an event's outcomes based on scales for the event's consequences and their likelihood or probability. Risk matrices can be used to (i) articulate the level of risk associated with an identified hazard; (ii) rank risks and thus propose actions; (iii) justify a proposal or action; and (iii) re-evaluate risk to demonstrate the effectiveness of a control (Cook et al., 2008; Cox et al., 2008).



**Figure 6** Complex 14x14 Matrix (David & Wilkinson, 2009)

In general, risk matrices are designed to enable the classification of risks as high, medium, or low, or at a more detailed level in a number of specific cases. Risk is generally considered to be derived from an estimate of probability or likelihood and consequence or severity; consequently, the x and y axes of most matrices are probability and consequence, and it is widely accepted that

$$\text{Risk (R)} = \text{Likelihood (L)} \times \text{Consequence (C)}$$

The risk matrix can condense the risk continuum into risk levels denoted by numerical bands or ranges (Cagno et al., 2000, Middleton and Franks, 2001, Cox, 2009).

Risk matrices have been widely praised and adopted as straightforward, effective risk management tools. This method establishes a clear framework for conducting systematic reviews of individual risks and risk portfolios in order to generate convenient documentation for risk

ranking and priority setting rationales. As a result, risk matrices have enabled decision-makers to concentrate on the most critical risks while maintaining consistency and establishing a shared understanding of risk levels across an organisation. Additionally, the inputs and outputs can be displayed in a straightforward manner to imply rapid ranking and comparison of risks requiring attention. As a result, it provides an opportunity for numerous stakeholders to contribute to the customization of category definitions and action levels, as well as for consultants to train various levels of an organization's staff on "risk culture" concepts.

On the other hand, there is a dearth of rigorous empirical or theoretical research on how well risk matrices actually improve risk management decisions; consequently, they frequently cannot represent a broad range of consequences or likelihoods and thus provide an inappropriate numerical scoring of risk levels. Additionally, risk matrices frequently lack or are insufficiently aligned between risks with varying consequences and frequently use uncertain, ambiguous, or obscure descriptions. Ball and Watt (2013) noted that while it can be challenging to define qualitative scales precisely and unambiguously, issues can arise when numerical matrix scales are not linear and users are unfamiliar with such scales.

### **2.3.2 Preliminary Harzard Analysis - PHA**

Preliminary hazard analysis (PHA) is used in the early stages of system design to identify hazards and potential accidents. It is essentially a review of where energy or hazardous materials can be released in an uncontrollable manner (FAA, 2000). The PHA technique was developed by the United States Army (MIL-STD-882D) and has been used successfully for both defence safety analysis and machinery and process plant safety analysis. A preliminary health assessment (PHA) is so named because it is usually refined through additional and more thorough research.

The overall goal of a PHA is to identify potential hazards, threats, and hazardous events early in the system development process so that they can be removed, reduced, or controlled in the project's subsequent development (Kovács et al., 2021). A PHA's more specific goals are as follows:

- Identify the assets that must be protected.
- Recognize the hazardous events that could occur.
- Identify the primary causes of each hazardous event.
- Determine the frequency with which each hazardous event may occur.
- Assess the seriousness of each hazardous event.
- Determine the appropriate safeguards for each hazardous event.
- Evaluate the risk associated with each hazardous event.
- Identify the most significant risk contributors.

The main benefits of PHA are that it:

- is simple to use and requires little training;
- is a necessary first step in most risk analyses and has been extensively used in defence and process applications;
- identifies and provides a log of hazards and their corresponding risks;
- can be used in early project phases, allowing for design changes; and

- is a versatile method that can cover a wide range of risks.

The main limitations of PHA are that it:

- is difficult to use to represent events with widely varying consequences;
- fails to assess risks of combined hazards or coexisting system failure modes;
- may be difficult to use to illustrate the effect of safeguards and provide a basis for prioritising safeguards.

### **2.3.3 Failure Mode Effects Analysis - FMEA**

Failure Mode Effects Analysis - FMEA is an analysis technique that identifies all possible failure modes for a particular component and the resulting effects on the subsystem and, ultimately, on the system. FMEA is opposed to fault tree analysis. Fault tree analysis is a top-down examination of a system's faults. FMEA is a bottom-up analysis technique that identifies system failures (not necessarily faults).

The fault tree begins with the highest-level or system-level concern (top event) and descends to the events that preceded that top event. FMEA does the exact opposite: it begins with the system's components and analyses failures and their impact on the subsystem in which they are housed and the propagated effects throughout the system. (Bahr, 2015; Reicht, 1966; Mahboob, 2014).

The objectives of an FMECA are to:

- Identify the possible failure modes of each system component.
- Determine the reasons of these failure modes.
- Identify the possible consequences of each failure scenario on the remainder of the system.
- Describe the methods for detecting failure modes.
- Determine the frequency with which each failure mode will occur.
- Assess the severity of the various failure modes.
- Determine the risk associated with each mode of failure.
- Identify potentially applicable risk-reducing actions/features.

FMECA is primarily used during the system's design phase to identify and analyse potential failures. Although the study is qualitative, several quantitative aspects may be included, such as a specification of the failure rate of the failure modes and a grading of the severity of the failure impacts. Additionally, FMECA can be used at later stages of a system's life cycle. The purpose is then to identify system components that should be modified to fulfil specific safety or reliability requirements, or as input to maintenance planning (Rausand, 2011).

The primary benefits of FMECA are that it:

- is widely used and easy to understand and interpret; - provides a comprehensive hardware review;
- is suitable for complex systems;
- is flexible in that the level of detail can be adapted to the objectives of the analysis; - is systematic and comprehensive, and should be able to identify all failure modes with an electrical or mechanical basis;

**Table 2.3** Example of FMCEA of Track failure (Mahboob, 2014)

| Identifi-<br>cation   | Function   | Failure<br>mode                              | Effect on<br>other units   | Effect on system  | Failure fre-<br>quency  | Ran-<br>king     | Comments   |
|---|--|--|--|---|---|------------------|--|
| Name:<br>Rail<br>sleeper<br>for bal-<br>lasted<br>track.<br>Type: B70 | Handling of<br>loads acti-<br>vated by<br>train Dura-<br>ble guaran-<br>tee of<br>gauge. | Sleeper<br>does<br>not sup-<br>port<br>load. | Shift of load<br>on neigh-<br>bouring<br>track<br>compo-<br>nents. | Deflection rises<br>in track. In-<br>creased vibra-<br>tions in track &<br>train. Rise in<br>horizontal and<br>vertical forces. | 1 / year<br>3% of total<br>number of<br>loaded de-<br>mands.<br>1/ month<br>1% of total<br>load demands | 4<br>2<br>3<br>1 | All other track<br>components<br>such as rail<br>fastening and<br>sub-grade are<br>working fine. |

The main limitations of FMECA are as follows:

- its benefits are dependent on the experience of the analyst(s);
- it requires a hierarchical system drawing as the basis for the analysis, which the analysts usually have to develop before the analysis can begin;
- it considers hazards arising from single-point failures and will normally fail to identify hazards arising from combinations of failures; and
- it can be time consuming.

Bahr (2015) also emphasised the importance of using FEMA as a reliability engineering tool rather than a primary safety tool. A significant risk associated with FMEA is that the engineer will believe that by identifying failures, they have identified hazard causes; in other words, FMEA was used to investigate how a specific failure that results in a hazard occurs. FMECA has the ability to subdivide component failures into component-part level failures as necessary in order to ascertain root causes and comprehend how to control a hazard. However, the FEMA should not be the primary analysis tool due to the laborious effort required to determine potential risks and the ease with which one can become bogged down.

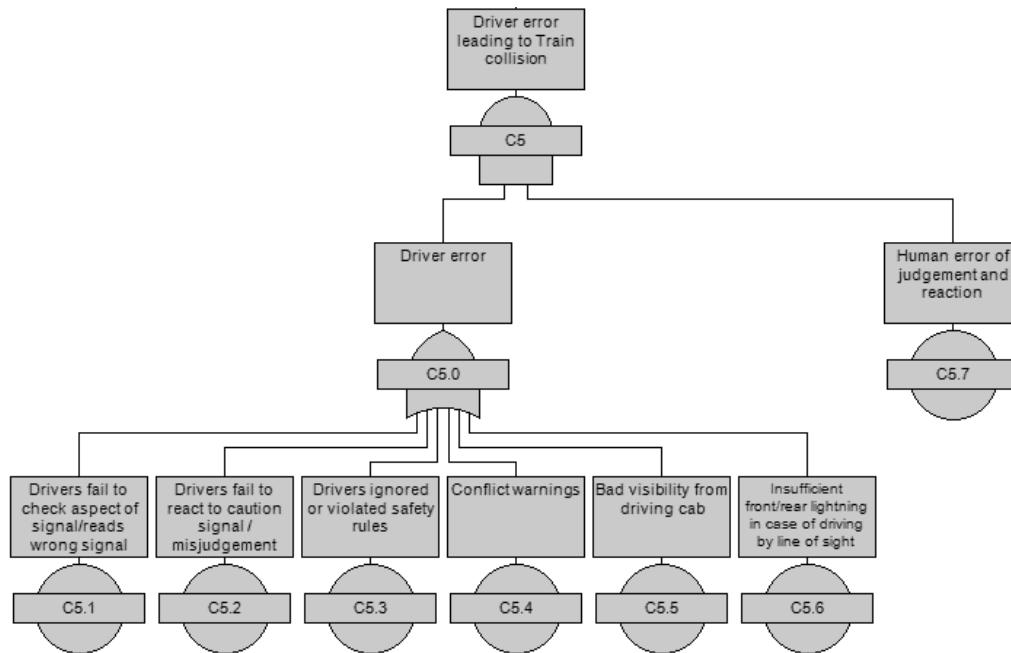
### 2.3.4 Fault Tree and Event Tree Analysis

An accident is a direct result of one certain failure or a consequence of a chain of failure including internal errors (component errors, breakdown of infrastructure, signal failure,...) and external errors (human errors, maintenance and testing errors, suicide or lost-control situation of human,...). There are many ways to display the cause-and-effect relation of these failure scenarios as in discussion above: risk matrices or FMECA. However, one significant disadvantage of these identification and assessment is only the qualitative or semi-quantitative analysis, therefore the accuracy and sensitive of analysis is not praiseworthy.

Paté-Cornell (1984) indicated that one convenient structure to overcome this problem and enclose a family of scenarios is tree-structure which established consecutive developments from each branching point defined by the prediction of several possibilities. Two particular methods using this structure is fault tree and event tree which used for logical representation of a railway system for the purpose of risk and reliability analysis (Chen et al., 2006, Braband et al., 2007).

Fault Tree Analysis (FTA) is based on top-down logic, starting from the hazard, called the Top Event, and looking downwards at all possible combinations of causes of that hazard. Event

Tree Analysis (ETA) establishes the scenarios following the hazard and leading to different consequences such as property losses and fatalities. Khakzad (2013) pointed out Fault Tree Analysis can associated Event Tree Analysis to compose one of the best graphical methods, named bow-tie model, for illustrating a thorough accident scenario starting from accident causes and ending with its consequences. In this model, the critical event is in the centre, a fault tree on the left side identifying the possible events causing the critical event, and an event tree on the right-hand side showing the possible consequences of the critical event based on the failure or success of safety functions.



**Figure 7.** Example of FTA: Driver errors leading to Train Collision

FTA's strengths include the fact that it is a systematic, logical technique that can account for a wide range of failure reasons, including human interactions, and that it is particularly beneficial for studying systems with many interfaces and complicated combinations that lead to system failure. Furthermore, the graphical depiction simplifies understanding of the system behaviour and the components incorporated. Its shortcomings include the fact that event sequences are not addressed, and the FTA only works with binary states (Lisnianski, Frenkel, and Ding, 2010). Furthermore, FTAs analyse only one failure mode at a time. However, subsequent adaptations of classical FTA, such as component fault trees (CFTs), have been developed to circumvent this restriction (Adler et al., 2010). Furthermore, CFTs enable the compositional development of FTAs and the systematic reuse of their elements.

ETAs' strengths are that they allow an organised and methodical analysis and assessment of different scenarios following a beginning event, as well as the influence of subsequent, potentially mitigating factors, which ultimately lead to diverse outcomes. The applicability of ETAs is limited if the probabilities of the events under consideration are time-dependent; in this situation, Markov models may be more appropriated. Furthermore, event trees might be challenging to build for large, sophisticated systems (Mahboob & Zio, 2018).

|                           | ATC fails to take correct data |      | Driver errors in evaluation |     | Both service brake and emergency brake failure to stop the Train in safe area |      | Trigger event: Presence of another train, people or objects on track |     | Assessment |               | Probability leading to Hazards |           |
|---------------------------|--------------------------------|------|-----------------------------|-----|---|------|--|-----|------------|---------------|--------------------------------|-----------|
|                           |                                |      |                             |     | Success   | 0.98 |  | No  | 0.95       |               |                                |           |
|                           |                                |      |                             |     |   |      |  |     |            |               |                                |           |
|                           |                                |      | Success                     | 0.9 |   |      |  |     |            |               |                                |           |
|                           |                                |      |                             |     | Failure   | 0.02 |  | Yes | 0.05       | Castastrophic |                                | 0.000855  |
|                           | Success                        | 0.95 |                             |     |   |      |  |     |            |               |                                |           |
| Failure in ATC input data |                                |      |                             |     | Success   | 0.98 |  | No  | 0.95       |               |                                |           |
|                           |                                |      | Failure                     | 0.1 |   |      |  |     |            |               |                                |           |
|                           |                                |      |                             |     | Failure   | 0.02 |  | Yes | 0.05       | Catastrophic  |                                | 0.000095  |
|                           |                                |      |                             |     |   |      |  |     |            |               |                                |           |
|                           |                                |      | Success                     | 0.9 | Success   | 0.95 |  | No  | 0.95       |               |                                |           |
|                           |                                |      |                             |     |   |      |  |     |            |               |                                |           |
|                           |                                |      |                             |     | Failure   | 0.05 |  | Yes | 0.05       | Catastrophic  |                                | 0.0001125 |
|                           | Failure                        | 0.05 |                             |     |   |      |  |     |            |               |                                |           |
|                           |                                |      |                             |     | Success   | 0.9  |  | No  | 0.95       |               |                                |           |
|                           |                                |      | Failure                     | 0.1 |   |      |  |     |            |               |                                |           |
|                           |                                |      |                             |     | Failure   | 0.1  |  | Yes | 0.05       | Catastrophic  |                                | 0.000025  |
|                           |                                |      |                             |     |   |      |  |     |            |               |                                |           |
|                           |                                |      |                             |     |   |      |  |     |            | Total         |                                | 0.0010875 |

**Figure 8.** Example of ETA – Failure of Automatic Train Control system

Fault Tree and Event Tree Analysis is widely used in cause-effect analysis of railway accident. It is possible to mention the studies of Dindar et al. (2017), Ruijters (2018), Bearfield and Marsh (2005), Liu et al. (2015), Lin et al. (2012, 2016), Doytchev and Szwillus (2009), Li et al. (2013). However, few studies have been conducted on urban railway systems, with the majority of research focusing on risk analysis for high-speed railways or intercity railway lines. Additionally, there are few case studies for growing countries with obsolete railway infrastructure and a lack of managerial expertise.

### 2.3.5 Markov's chains

A Markov chain or Markov process is a stochastic model that depicts a succession of potential occurrences where the probability of each event relies solely on the state of the preceding event (Gagniuc, 2017). The discrete-time Markov chain describes the chain's state transitions (DTMC) in a countable wireless sequence. Continuous time processes are referred to as Markov chains in continuous time (CTMC). It is named after Andrey Markov, a Russian mathematician (Brooks, 2011).

A Markov process is a stochastic (often "memoryless") process that meets the Markov property (Gagniuc, 2017). Simply said, it is a process that can anticipate future events given its current state, and more significantly, these forecasts are as accurate as if the whole history of the process were known. A Markov chain is a sort of discrete spatial state or discrete index set Markov process (usually representing time). Nonetheless, the precise definition of a Markov chain varies (Asmussen, 2003). It is common to define a Markov chain as a Markov process with a countable state space in discrete or continuous time (and thus independent of the nature of the event) (Parzen, 1999), but it is also common to define a Markov chain as a discrete-time Markov process with a countable or continuous state space (and therefore related to the state space).

In Markov's chain assessment method, a discrete random process (a random sequence)  $X(t)$ ,  $t \in T = \{0, 1, 2, \dots\}$  is considered with a finite number of states  $E = \{1, 2, \dots, N\}$ . The states of  $X(t)$  can be different risk situations.

The future development of the process at time  $t + 1$  depends only on state of the process at time  $t$ , and does not depend on past development at times  $t - 1, t - 2, \dots, 2, 1, 0$ . We can describe is as follows: for all  $t = 0, 1, 2, \dots$  and all states  $i, j, i_{t-1}, \dots, i_0 \in E$  is

$$P(X_{t+1} = j | X_t = i, X_{t-1} = i_{t-1}, \dots, X_0 = i_0) = P(X_{t+1} = j | X_t = i) \quad (2.3)$$

We introduce notation

$$p_{ij}(t, t + 1) = P(X_{t+1} = j | X_t = i) \quad (2.4)$$

Probabilities  $p_{ij}(t, t + 1)$  are called the transition probabilities from the state  $i$  at time  $t$  to state  $j$  at time  $t + 1$ . Probabilities  $p_{ij}(t, t + s) = P(X_{t+s} = j | X_t = i)$ , are called transition probabilities from the state  $i$  at time  $t$  to state  $j$  at time  $t + s$ .

Instead of  $p_{ij}(t, t + 1)$ , we can for homogeneous Markov chain write  $p_{ij}(1) = p_{ij}$ . The probability  $p_{ij}$  we call transition probability after one step and the matrix

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1N} \\ \vdots & \ddots & \vdots \\ p_{N1} & \cdots & p_{NN} \end{pmatrix} \quad (2.5)$$

we call the transition probability matrix of the homogeneous Markov chain or briefly transition probability matrix. For each row of  $P$  is  $\sum_{j=1}^N p_{ij} = 1$ , the matrix  $P$  is a stochastic matrix.

We can describe dynamics of the process  $X(t)$  using the matrix  $P$  and the vector of initial states  $p(0)$ .

$$P(X(0) = i_0, X(1) = i_1, \dots, X(k) = i_k) = p_{i_0 i_1} p_{i_1 i_2} \cdots p_{i_{k-1} i_k} \quad (2.6)$$

or any states  $i_0, i_1, \dots, i_k \in E$ . We denote  $p_{ij}^{(s)} = p_{ij}(t, t + s)$  for  $s = 1, 2, \dots$  and

$$p_{ij}^{(0)} = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases} \quad (2.7)$$

In terms of long-term of the chain  $X(t)$  it is useful to determine absolute probability of states  $p_i(t)$  for large  $t$  ( $t \rightarrow \infty$ ), we want to find  $\lim_{t \rightarrow \infty} p_i(t)$ .

$$\lim_{t \rightarrow \infty} p_{ik}^{(t)} = \pi_k \text{ and } \lim_{t \rightarrow \infty} p_k(t) = \pi_k \quad (2.8)$$

where  $\pi_1, \pi_2, \dots, \pi_N$  are unique solutions of  $\pi_k = \sum_{j=1}^N \pi_j p_{jk}$  and  $\sum_{j=1}^N \pi_j = 1$ .

The vector  $\pi = (\pi_1, \dots, \pi_N)$  defines so called the stationary probability distribution of the chain  $X(t)$ . If the initial probability distribution is stationary, ie.  $p(0) = \pi$ , then all absolute probability distributions  $p(t)$  are stationary, ie.  $p(t) = \pi$ , and we say that the chain is in the statistic equilibrium.

According to Rausand (2011), the main advantages are that the Markov method:

- is based on a well-documented theory foundation and has been applied and verified extensively in many fields;
- is a suitable tool for analysing small but complex systems with dynamic properties, which cannot be analysed adequately using fault trees;
- provides a state transition diagram with important information that is easy for non-specialists to understand and can provide a deeper understanding of how the system is operated;

And the significant limitations are that the Markov method:

- is restricted to relatively small systems with a limited number of states;
- is time-consuming as the number of states increases;
- is that analysts may have trouble translating their problem into a Markov model (Rausand and Høyland, 2004).

### 2.3.6 Petri Net

A Petri Net, also known as a place/transition (PT) net, is one of several mathematical modeling languages for the description of distributed systems. It is a class of discrete event dynamic system. A Petri net is a directed bipartite graph that has two types of elements, places and transitions, depicted as white circles and rectangles, respectively. A place can contain any number of tokens, depicted as black circles. A transition is enabled if all places connected to it as inputs contain at least one token. Petri nets were invented in August 1939 by at only thirteen years old at the time Carl Adam Petri, for the purpose of describing chemical processes (Petri and Reisig., 2008).

A Petri net is a directed graph consisting of three structural components, places, transitions and arcs. Places, which are drawn as circles, represent possible states or conditions of the system while transitions, which are shown by bars or boxes, describe events that may modify system states (Salimifard and Wright, 2001). The relationships between places and transitions are represented by a set of arcs, which are the only connectors between a place and a transition in either direction. There is no connection between two nodes of the same type. The dynamic behaviour of a system can be represented using tokens, which graphically appear as black dots in places.

A Petri net is a 4-tuple  $N = \langle P, T, F, M_0 \rangle$  (Salimifard and Wright, 2001), where :

- $P = \{p_i : i = 1, \dots, |P|\}$  is a finite set of places,
- $T = \{t_i : i = 1, \dots, |T|\}$  is a finite set of transitions,  $P \cap T = \emptyset$ ,
- $F \subseteq (P \times T) \cup (T \times P)$  is the set of directed arcs representing flow relations, joining places and transitions together.
- $M_0: P \rightarrow \{0, 1, 2, \dots\}$  is the initial marking.

A marking  $M = \{M_{(p_1)}, M_{(p_2)}, \dots, M_{(p_{|P|})}\}$  representing a state of the modelled system, is a distribution of tokens over the set of places. Starting from an initial marking  $M_0$ , a new marking  $M$ , is reachable if it can be reached by means of a change to the state of the system. This is modelled by the @ring of transitions. For a transition  $t \in T$ , the set of its input places is  $\cdot t = \{p \in P : (p, t) \in F\}$  and the set of its output places is  $t \cdot = \{p \in P : (t, p) \in F\}$ . A transition may fire, which changes the current marking  $M$  into a new marking  $M'$ . The effect of firing, a transition  $t$  can be expressed as  $M[t > M' \text{ or } M \xrightarrow{t} M']$ . When a transition fires, it consumes one token from each of its input places and produces one token in each of its output places (Salimifard and Wright, 2001).

In conjunction with Murata's study (Murata, 1989), Petri nets can be described as having different degrees of liveness  $L_1 - L_4$ . A Petri net  $\langle N, M_0 \rangle$  is called  $L_k - \text{live}$  if and only if all of its transitions are  $L_k - \text{live}$ , where a transition is:

- Dead, if it can never fire, i.e., it is not in any firing sequence in  $c$
- $L_1 - \text{live}$  (potentially fireable), if and only if it may fire, i.e., it is in some firing sequence in  $L\langle N, M_0 \rangle$



- $L_2$  – *live* if it can fire arbitrarily often, i.e., if for every positive integer  $k$ , it occurs at least  $k$  times in some firing sequence in  $L(N, M_0)$
- $L_3$  – *live* if it can fire infinitely often, i.e., if there is some fixed (necessarily infinite) firing sequence in which for every positive integer  $k$ , the transition  $L_3$  occurs at least  $k$  times.
- $L_4$  – *live* (live) if it may always fire, i.e., it is  $L_1$  – *live* in every reachable marking in  $R(N, M_0)$

Noteworthy these are increasingly stringent requirements:  $L_{j+1}$  – *liveness*, for  $j \in 1, 2, 3$ .

### 2.3.7 Bayesian Network

A Bayesian Network (BN) is a graphical model which is used to find out relationship between causes and one or more final outcomes in a system. Through modelling of Bayesian Network, the Probabilities of the outcome can also be calculated as has been done in FTA (Raussand, 2011). The theory of probability including Bayes' formula, conditional probability and conditional independence is the fundamental concept of BN (Zheng, 2018). The conditional probability formula  $P(A|B) = x$  refers to the statement, where the probability of event A is x if event B has already occurred. Assume that events  $B_1, B_2, B_3, \dots, B_n$  are mutually exclusive and the condition  $P(B_i) \geq 0, i = 1, 2, 3, \dots, n$  is satisfied. According to the conditional probability theory, probability of the given event A can be expressed as:

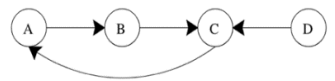
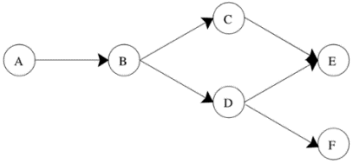
$$P(A) = \sum_{i=1}^n P(B_i) P(A|B_i) \quad (2.9)$$

The posterior probability  $P(B_i|A)$  can be calculated as following according to:

$$P(B_i|A) = \frac{P(B_i)P(A|B_i)}{\sum_{j=1}^n P(B_j)P(A|B_j)} \quad (2.10)$$

BNs are a very useful tool for describing and modeling current knowledge, for example, by providing an initial representation of a system or problem that can provide a better understanding and perspective of uncertainty and complexity, thus helping to advise managers and decision makers (Stephenson, 2000). BNs provide a powerful statistical framework in situations where little data is obtained.

**Table 2.4** Structure of Bayesian Network (Stephenson, 2000)

|   |  |
|---|--|
|  | <p>Chains and paths. The vertex sequence A – B – C – A – B – C is a cycle. The vertex sequence A – B – C – A is a simple cycle.</p>  |
|  | <p>DAGs, parents/children, ancestors/descendants, family. A is the parent of B while B is the child of A; A is the ancestor of B, C, D, E and F while B, C, D, E, F are descendants of A; A possible ancestral ordering is A, B, C, D, E, F; Some sample families are A, B as the family of B; B, C as the family of C</p> |

A BN is a network graph consisting of a directed acyclic graph (DAG) with nodes and arcs. If the two vertices within each edge are ordered, then the edges have a direction assigned to them (Brualdi, 1999). A directed acyclic graph, or a DAG, is a directed graph that has no

cycles. There are three types of nodes in a BN graph: root nodes, end nodes and intermediate nodes. They represent random variables while the arcs represent the causal relationship between these variables. Each node has two or more mutually exclusive states in practice, which means the value of these random variables is a discrete distribution. For each random variable, the sum of probabilities of all possible states must equal one (Rekabi, 2018). A **chain** is a series of nodes where each successive node in the chain is connected to the previous node by an edge. A **path** is a chain with the further constraint for digraphs that each connecting edge in the chain has a directionality going in the same direction as the chain. A cycle is a path that starts and ends at the same node. A simple cycle is a cycle where, except for the start/end node, all nodes are unique. A **parent/child**, the edge points from the parent to the child. An **ancestor/descendant** just like in human genealogies, this relationship extends further than just those two sets of parent/child relationships. An **ancestral ordering** is an ordering of nodes where each ancestor comes before its respective descendants, this is always and only possible in DAGs. A **family** is the set of vertices composed of X and the parents of X (Stephenson, 2000).

Compared with FTA, BN has a few advantages that FTA does not provide. The events with multi-state and dependency can be represented in BN due to application of the conditional probability table (CPT). Rather than AND-gate or OR-gate in FTA, random variables used in CPT can describe the causal relationship between events more effectively. Furthermore, the common causes failures (CCFs) can also be managed by corresponding arcs in a BN-graph (Mahboob, 2014). Another advantage of BN is that it is possible for BN to update probability of occurrence of the primary events in order to perform a dynamic accident analysis (Khakzad et al., 2011). In addition, BN has also been applied for the measure of system uncertainty, which is given by logarithmic measure of available alternatives and probability distribution. Usage of BN makes it more effective to adapt to the complex and practical system feature (Das, 1999).

The method that mapping fault tree into BN was carried out in several studies (Bobbio et al., 2001), (Khakzad et al., 2011), (Zheng, 2018). The rules for converting a static fault tree to a static BN consist of mainly two aspects, the graphical conversion and the numerical conversion. Some basic conversion rules are shown in the figure above. The root nodes in BN are created to represent primary events in fault tree in the first step. The value 0 of the root node means that the component works properly, and the value 1 means that a failure occurs to the component. The prior probability of corresponding primary events is then allocated to these root nodes to establish the basis of quantitative analysis in BN. After that, nodes in BN are connected and equivalent CPTs are created to represent logical gates in the fault tree.

A few studies have been done to explore the application of Bayesian Network in railway risk assessment. A case study of train accidents due to driver errors shows that BN is an appropriate method for causal analysis if factors are not reliably accurate or constant (Rekabi, 2018). S. Dindar et al. introduced a probability analysis method of weather-related train derailments using BN. The authors used BN to model the occurrence of train derailments due to weather factors and introduced the concept of fuzzy numbers for a quantitative analysis. The result indicates that those nodes such as frozen pre-cipitation, liquid precipitation and high wind deserve more attention than other nodes (Dindar et al., 2017). Q. Mahboob et al. compared application of FTA and Bayesian Network on train derailment due to signal passed at danger. The study shows that Bayesian Network can make up for limitations of FTA in complex railway system, such as common cause failures and disjoint events (Mahboob, 2014).

## **2.4 Safety management system**

The technical and operational fragmentation between the railway systems of the Member States is a major hurdle for the development of a single European railway, so the Council Interoperability Directives (96/48/EC, 2001/16/EC) have defined essential requirements and established a mechanism for explaining mandatory technical specifications for interoperability. Furthermore, the European Railway Safety Directive (2004/49/EC) emphasises the development of Safety Management System, Common Safety Indicators, Common Safety Targets and Common Safety Methods through independent technical expertise and requires the development of a harmonised format for safety certificates/authorisations and their applications. In order to be granted the access to a member states railway infrastructure or part of, each Railway Undertaking (RU) is required to obtain safety certification from the relevant safety authority. In order to be allowed to manage and operate a rail infrastructure, the safety management system (SMS) is required to obtain safety authorisation from the relevant safety authority.

The Railway Safety Directive (Directive 2016/798) emphasises this subject even further. In accordance with Article 4(3) of this directive, RUs are required to implement a safety management system (SMS) in order to be held accountable for safe operation. In accordance with Article 9(2) of the Safety Directive, the RU is responsible for controlling any risks associated with the delivery of maintenance and, as such, must establish control measures to ensure that vehicles are maintained in a way that allows them to be used safely in trains.

This part of the research will discuss the concept and structure of a SMS in railway, giving the basic elements for developing the assessment process in order to ensure that the necessary elements of an SMS are available and maintained for all aspects of system operation and they are in accordance with standards, directives and the quality system (e.g. ISO 9000 series) requirements.

### **2.4.1 Safety management concept**

Overall, a safety management system (SMS) is a systematic, accurate and comprehensive process for managing risks and similar to the approach of the International Organization for Standardization (ISO) to safety. The SMS provides a directed and focused approach to safety with a clear process for setting goals, planning, and measuring performance to all management systems. The organisational structures and activities that make up an effective safety management system are found throughout an organization. Both manager and employees have responsibility to contribute to the organisation's safety culture. The SMS philosophy requires that responsibility and accountability for safety be retained within the management structure of the organisation. Senior management should always be ultimately responsible for safety, as they are for other aspects of the enterprise. The SMS approach ensures that authority and accountability always co-exist. In larger organizations, safety management activity will be more visible in some departments than in others, but the system must be integrated into "the way things are done" throughout the establishment. This will be achieved by the implementation and continuing support of a coherent safety policy that leads to well-designed.

Traditionally, in rail and in other safety-critical industries, safety had been pursued through compliance with prescriptive rules and regulations. In the 1990s, however, advancements in safety research demonstrated that organizations could be compliant with prescriptive regulations, yet still be unsafe. More specifically, compliance did not necessarily mean effectively managing risks. James Reason (2003) presented a now well-known model of

accident causation (the Swiss Cheese model) that explained how human beings contribute to the breakdown of complex, interactive and well-guarded systems, such as rail transportation. Most importantly, the model demonstrates that the whole system must be considered when evaluating safety performance. procedures.

SMS is not a completely new system; rather it builds upon the existing safety principles and safety practices in the organisation to manage the safety from a proactive way (Bayuk, 2008). In general, the concept of SMS is represented by 4 aspects as shown in following:

**Philosophy** - SMS starts with management philosophy: (i) recognising that there will always be threats to safety; (ii) setting the organization's standards; and (iii) confirming that safety is everyone's responsibility.

**Policy** – safety will be achieved when SMS has: (i) clear statements of responsibility, authority, and accountability; (ii) development of organisational processes and structures to incorporate safety goals into every aspect of the operation; and (iii) development of the skills and knowledge necessary to do the job.

**Procedures** – What management wants people to do to execute the policy: (i) clear direction to all staff; (ii) means for planning, organising, and controlling; and (iii) means for monitoring and assessing safety status and processes.

**Practices** – What really happens on the job: (i) following well-designed, effective procedures; (ii) avoiding the shortcuts that can detract from safety; and (iii) taking appropriate action when a safety concern is identified.

### 2.4.2 Safety Management System in Railway

Since SMS as a proactive approach to systematically manage the safety throughout the whole organisation is widely required among the rail industry and other safety-critical industries, the benefits of adopting a SMS have been recognised across the industry (Fernández-Muñiz et al., 2007).

The SMS must be in the form approved by the Rail Safety Regulator. This section sets out regulatory requirements regarding the form of the SMS. And furthermore, the SMS should incorporate a safety management plan, which describes and serves as a guide to the SMS. To be more details, the SMS must be prepared in accordance with the regulations and provide a comprehensive and integrated management system for all aspects of control measures adopted in accordance with the legislation. The safety management plan needs to specify the scope of the railway operations to which the SMS applies; states the persons responsible for the development and implementation of the SMS; lists the elements of the safety management system and explains the relationship between the elements of the safety management system; and provides a list of key standards and procedures of the SMS elements to which they relate. (AMTRS, 2006)

SMS Benefits for railway system can be concluded as in the following:

- Improved decision making
- Learning about operations
- Improved safety performance
- Customised mitigation strategies
- Possibly exceeding safety standards set by regulation
- Improved public and customer confidence

- Increased competitive advantage
- Demonstrated due diligence
- Potential for reduced regulatory oversight
- Enhanced relationships and collaboration
- Improved economic performance

According to Railway Safety Act of Canada, SMS is “a formal framework for integrating safety into day-to-day railway operations and includes safety goals and performance targets, risk assessments, responsibilities and authorities, rules and procedures, and monitoring and evaluation processes”. The goals of the Railway SMS Regulations are to ensure that safety is given management time and corporate resources and that safety performance measurement and monitoring are given the same priority as corporate financial and production goals. The regulations do not replace, suppress or precede any existing rules, regulations or standards. Rather, the requirement for a systemic approach to managing safety is integral to the current framework. (Railway Safety Act, 2006).

### **2.4.3 Structure of Safety Management System**

#### ***Setting expectations***

A railway company shall implement and maintain a safety management system that includes: the railway company safety policy and annual safety performance targets and the associated safety initiatives to achieve the targets, approved by a senior company officer and communicated to employees. Firstly, the purpose of this policy is to set out and communicate SMS's approach to ensuring that it operates and assures all safety activity in order to reduce all risks to As Low As Reasonably Practicable (ALARP) and positively manage our impact on the environment. A company's safety policy should: (i) demonstrate senior management's commitment to safety; (ii) set the organisation's safety philosophy and guide the establishment of goals and objectives, policies, procedures, and programs; (iii) be communicated to all employees and to other stakeholders; and (iv) finally, be periodically reviewed and revised.

In addition to a safety policy, the regulations require railways to establish annual safety performance targets and identify initiatives that will be undertaken to achieve those targets. While the ultimate goal is to eliminate accidents, it is useful to have intermediate targets – set annually – against which continual progress toward the ultimate goal can be measured. Annual targets should be associated with planned safety initiatives designed to ensure that the company can meet its safety performance targets. Overall, the annual safety performance targets need to be measurable and realistically obtainable, furthermore, promote continual safety development.

The safety policy and annual safety performance targets should be communicated to all employees. In some circumstances, it may also be desirable to communicate the safety policy to other stakeholders, such as customers, communities through which the railway operates, and the general public.

#### ***Goal Settings – Action Planning***

Under the common understanding or implementation of SMS, it cannot replace or create another understanding the current railway safety, the regulations and the existing railway safety requirements; instead, it only provides a framework for identifying legal obligations, monitoring changes to them, and demonstrating and evaluating compliance. Therefore,

standards and legal requirements are reviewed to establish their potential relevance to and impact on railway system operations; and results of the review are communicated to staff and other relevant interested parties.

The safety management system should include: (i) procedures to ensure that the organization is aware of its legal obligations with respect to rail safety and to monitor changes; (ii) procedures for ensuring compliance with these requirements; and (iii) procedures for evaluating compliance with regulatory requirements, reporting the results of such evaluations and making recommendations.

Due to the understanding of SMS is almost deserted in Vietnam, in order to clarify the SMS designing process, a several of legal requirements and experience with different scope and depth of regulations from Western railway system are reviewed to draw a background of SMS application as in the Table 2.5.

In Canada, Transport Canada's Railway SMS Regulations (Transport Canada, 2001) define the SMS as a formal way to make the operations safely and to establish a safety culture to reduce the railway accidents, which includes safety goals and performance targets, risk assessments, responsibilities, rules and procedures, monitoring and evaluation, and the requirements of documented systems and procedures is enforced in the SMS among the railway companies.

**Table 2.5** Safety Management System Requirements of Railway Safety Standards, Regulations or Guidelines in Different Regions

| Name of Standard/Regulation   | First Issued Year | Scope          |
|---|-------------------|----------------|
| Railway Safety Management System Regulations (Transport Canada, 2001)   | 2001              | Canada         |
| Railway Safety Directive 2004/49/EC (European Union, 2004)  | 2004              | Europe         |
| The Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS, 2006)                                    | 2006              | United Kingdom |
| National Guideline for the Preparation of a Rail Safety Management System (National Transport Commission Australia, 2008) | 2008              | Australia      |

In Europe, European Union defines a railway SMS as "the organisation and arrangements established by an infrastructure manager or a railway undertaking to ensure the safe management of its operations" in the European Union Railway Safety Directive (EC, 2004). A related guidance for SMS has published, based on the directive, representing key elements of the SMS in three groups: processes for design and improvement, processes for implementation and operational activities (Patacchini, 2011). For the sake of interoperability demand, UK has introduced the Railways and Other Guided Transport Systems Regulations (ROGS) since 2006, which prescribes a set of requirements for the SMS in mainline and non-mainline rail network. Four main purposes for the railway SMS are identified in the guidance, defining roles and responsibilities to ensure the transport system can run safely, arranging the managers to control the SMS, showing the involvement of workers and their representatives, and making sure the continuously improvement of the operator (ROGS, 2006).

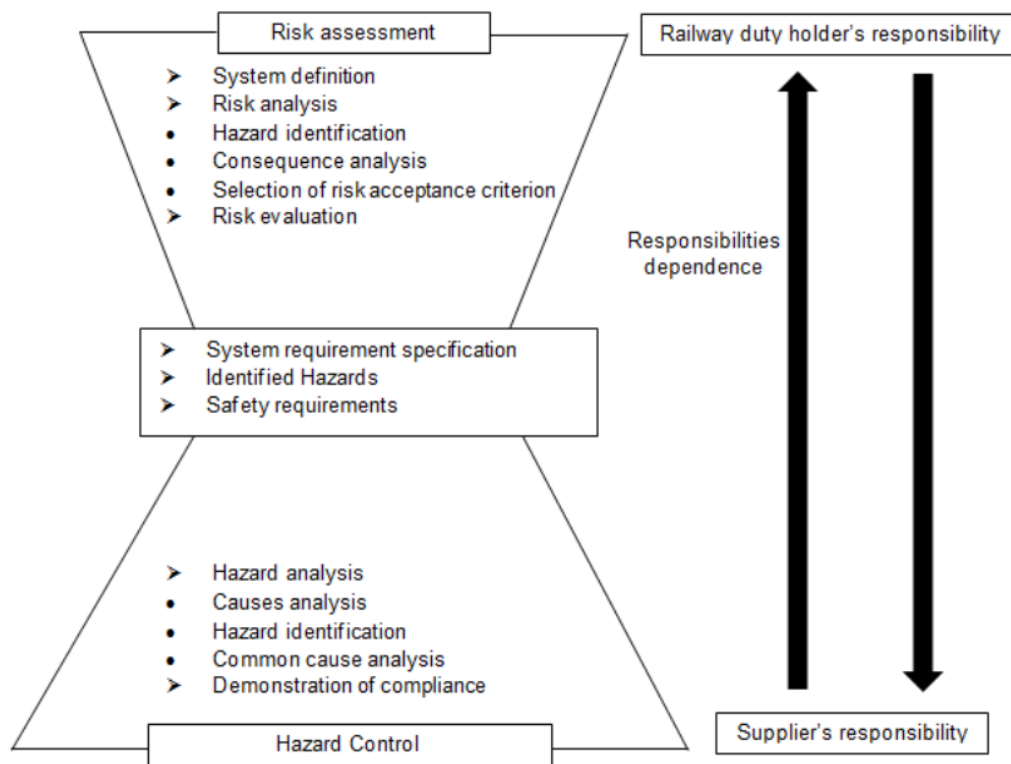
In Australia, National Transport Commission Australia (2008) published the national guidelines to explain the legislative requirements of SMS for rail transport operators contained in the Rail Safety Bill 2006 or Rail Safety Regulations 2006 in Australia, in order to achieve a high

level of safety awareness and commitment throughout all parts of the rail transport operator. The guidelines summarise the requirements in the form of the SMS and the content of the SMS determined by legislation and the rail safety regulator, and highlight the mandatory process of safety management plan and the consultation before designing the SMS (NTCA, 2008).

### **Risk Management**

The process of risk management including 3 steps as in the following:

**Step 1:** Identify the safety issue and concerns. This step have gained the input from incident/accident investigations and safety data collection and analysis, used analytical methods (FMEA, FTA, ETA, Markov model,...) to identify system failures and their influence to our system. Moreover, the influence of human error or safety monitoring technology is also analysed. In the case of new equipment, systems, operations, practices and procedures where experience and a safety history are not available, formal analytical techniques should be applied. These techniques are more demanding in terms of data, time, effort and expertise; however, this extra effort is justified for new equipment, systems, operations, practices and procedures and should be considered a normal part of the process of implementing change.



**Figure 9** Hourglass model for risk management within railway (EN50126, 2018)

**Step 2:** Risk estimation. In this step, quantitative estimates of the probability and severity of the safety issue/concern can sometimes be developed from safety performance data, illness and injury records, etc. Probability estimates based on historical data assume that future conditions will mirror those of the past. Where no relevant historical data are available, other methods such as fault-tree or event-tree analysis may be used to generate estimates.

**Step 3:** Risk response. According to their level of criticality, risks will be responded to and thus controlled, in a strategic and efficient manner. The approaches to be adopted are: (i)

risk avoidance - changes to eliminate the risk or to protect the project from the risk by changing the scope, adding time or resources; (ii) risk transfer: transfers the impact of risk by contracting out several aspects of the work; (iii) risk mitigation: applies preventive actions or decisions are identified as convenient to minimize the level of criticality of a defined risk, mitigate its severity or/and decrease its probability of occurrence; (iv) risk monitoring: measures aim to assure the follow-up of a specific parameter of event that could release a certain risk; (v) risk acceptance: does not change the project to deal with the risk and agrees to address the risk in the case of occurring.

### ***Risk control strategies***

Risk control strategies are required for risks that have been classified as unacceptable or tolerable with mitigation. In generic terms, these strategies can focus on:

- eliminating the situation, substance, condition or activity generating risks;
- reducing the probability of occurrence; or
- mitigating (reducing) the consequences.

For existing operations, many of the risks will have already been considered and risk control strategies will form part of the railway's current rules, standards, procedures and operating practices. In this case, the risk assessment process would document this link and then focus on the results of accident and incident investigations, safety data analysis, complaint follow-up, inspections, and audits to ensure that the risk is being mitigated to an acceptable level. This analysis should point railway companies to areas where they could undertake initiatives beyond their current practices in an effort to improve their overall safety performance.

For new operations, or for changes to technology, staffing levels, types of operation or other areas where a railway company lacks historical data and experience, a formal risk management process should almost always be undertaken. The safety management system should include procedures for the development of the required strategies, approval at an appropriate management level and effective implementation. Employees and their organisations should be involved in the development of risk control strategies, particularly for risks that they have identified, and they should be informed of the actions that are being taken or that are planned.

### ***Responsibilities***

It is essential in any management system that each person responsible for implementation of the system has a clear understanding of their accountabilities, responsibilities and authorities in relation to the system. This should cover the scope of operations at any given time, degraded and emergency situations. Each person needs to understand where they fit in the system, and what other functions are reliant on the role that they undertake. All staff and contractors have a responsibility to report safety risks and incidents and rail transport operators must ensure that there are clear processes and delegations to capture this information and respond accordingly.

To achieve this, the safety management system must include documents that describe the responsibilities, accountabilities, authorities and interrelation of the personnel who manage or carry out rail safety work, or who verify such work. Safety responsibilities, accountabilities, authorities and interrelationships should be determined in accordance with established policies of the rail transport operator. For example, some authorities should only be allocated to a person with appropriate technical qualifications; or a certain level of management seniority. The safety management system must include policies that indicate how safety responsibilities, accountabilities, authorities and interrelationships have been determined. These requirements may be satisfied by organisational charts supported by position descriptions which describe the key dependencies between roles. Safety responsibilities, accountabilities, authorities, interrelationships should be determined in accordance with accepted policies.



Experience has shown that a railway company will be markedly more successful in developing a safety culture if employees and their representatives, where applicable, are involved in the development and implementation of the safety management system. Employee and representative participation in drafting the company safety policy is highly recommended. A collaborative approach helps ensure that significant employee concerns are addressed in the policy and provides an additional vehicle for communicating the railway's commitment to safety to employees.

Often, companies will develop global targets and then have policy committees review and comment on the targets and associated safety initiatives. Consulting with employees and their representatives and linking the target-setting process with the railway's risk management process will help ensure that the most significant outstanding safety issues and concerns are addressed. In addition, the risk management process will include mechanisms for employees to identify safety issues and concerns on a routine and ongoing basis. These mechanisms need a high level of visibility and participation to ensure that all risks are captured. Experienced and knowledgeable employees are a good source of expert judgment for evaluating the probability and severity of safety issues and concerns where quantitative, historical data are not available. Finally, employees and their representatives shall be involved in the development of risk control strategies for risk assessments in which they are involved and where employee safety is impacted.

### ***Measuring Performance***

The safety management system should include for data collection and data analysis:

- (i) identification of the safety data to be collected to assess performance with respect to the company's annual safety targets and to meet other analytical requirements;
- (ii) systems to collect data on accidents and safety-related incidents;
- (iii) procedures for periodic analysis of the data and feedback into the risk management process;
- (iv) analysis of safety data to assess safety performance relative to the organization's annual targets and to identify safety trends using appropriate statistical techniques.

Data collection and analysis should include not only lagging indicators (e.g. accidents), but also leading indicators, such as: incidents; near-misses; rule violations; audit/inspection results; track inspection findings; and train inspection findings. Safety performance data can be captured by automated techniques or through inspection activities and reporting systems. Modern technology, such as test cars, impact detectors and crossing systems, has greatly expanded the type and quantity of safety data that can be captured at a reasonable cost.

Furthermore, safety audits and evaluations of the safety management system are important mechanisms for ensuring that all of the organizational elements, functions and procedures in the system are working well. Internal audits and evaluations are one of the key feedback loops for identifying required changes to the system.

The safety management system should include:

- (i) periodic audits of the performance of the components of the organization's safety management system, including audit frequencies, methodologies, responsibilities and reporting processes;
- (ii) audits by suitably qualified personnel who are impartial and objective;
- (iii) use of recognized audit methodologies;
- (iv) reporting of audit results to senior management;
- (v) consideration and approval of evaluation reports as well as the resulting recommendations by senior management.

### 3. ANALYSING THE SAFETY-RELATED ISSUES IN IMPLEMENTING HANOI URBAN RAILWAY PROJECTS

#### 3.1 Rationale of Vietnam Urban Railway

##### 3.1.1 Planning and existing work of Hanoi urban railway project

Currently, two urban railway lines are under construction in Hanoi: Line 3: Nhon - Hanoi station and Line 2A: Cat Linh - Ha Dong. Other metro lines are being planned for deployment in the near future. According to the Hanoi Capital Construction General Planning to 2030 and a Vision to 2050, approved by the Prime Minister in July 2011 in Decision No. 1259/QĐ-TTg dated July 26, 2011, the UMRT network consists of eight mass rapid transit train (MRT) lines totaling 306.5km in length. Five lines, namely MRT lines 1, 2, 2A, 3, and 5, are now under construction.

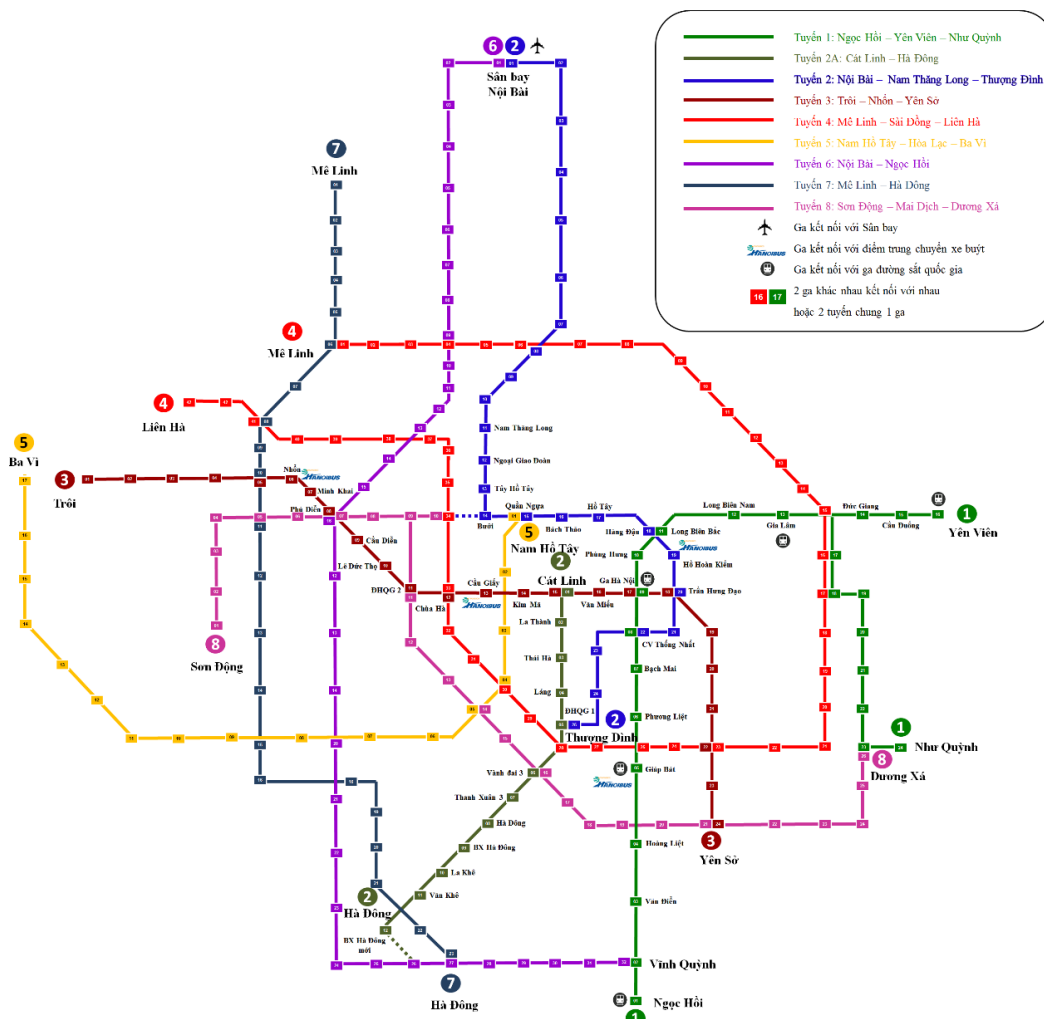


Figure 10 Metro line network maps in Hanoi

The table below will summarised 8 metro lines which are planned for developing in Hanoi capital in the future of 30 years.

**Table 3.1** Summary of metro lines planned in Hanoi

| No | Metro Line   | Route planned            | Route length   |
|----|--------------|--------------------------|----------------|
| 1  | Line 1       | Ngọc Hồi – Yên Viên      | 38.7 km        |
| 2  | Line 2       | Nội Bài – Thượng Đình    | 35.2 km        |
|    | Line 2A      | Cát Linh – Hà Đông       | 14 km          |
| 3  | Line 3       | Trôi – Nhổn – Yên Sở     | 21 km          |
| 4  | Line 4       | Liên Hà – Bắc Thăng Long | 53.1 km        |
| 5  | Line 5       | Nam Hồ Tây – Hòa Lạc     | 34.5 km        |
| 6  | Line 6       | Nội Bài – Ngọc Hồi       | 47 km          |
| 7  | Line 7       | Mê Linh – Ngọc Hồi       | 35 km          |
| 8  | Line 8       | Cổ Nhuế – Trâu Quỳ       | 38 km          |
|    | <b>Total</b> |                          | <b>306.5km</b> |

The projected are in implementation (see in Figure 13, 14):

**Metro Line No.2A:** Ha Dong – Cat Linh.

Decision No. 3136/QĐ-BGTVT dated October 15, 2008, approved the project.

This project has been constructed 13.05 km of urban elevated railway with 12 stations from Cat Linh to Yen Nghia Bus Terminal. Maximum train speed is 80km/h on a double gauge 1435 mm track. Power supplying technology is third rail system

Due to a variety of factors, the project's total investment (which increased by 61%) and progress of implementation were adjusted during its implementation:

Increased costs occurred due to site clearance, relocation of infrastructure works, technical floor delay, policy change, site clearance unit price, additional changes to a number of items compared to Basic Design (change of 2-floor station plan to 3 floors, treatment of soft soil in depot area, etc.), additional supplement funding for training and hull material adjustment (from climate-resistant steel to aluminium).

Presently, the project has been finished, tested, and certified for system safety by the consulting consortium Apave-Certifer-Tricc, and it is awaiting national approval to operation.

**Metro line No.3:** Nhon – Hanoi station. The route length is about 21km, the route is divided into 2 projects:

- Project 1: Nhon – Hanoi Station section with a length of 12.5Km.
- Project 2: Hanoi - Hoang Mai Station section with a length of about 8.5Km. The project is in progress of the Master Planning, Basic Design and Feasibility Study, funded by ADB.

Project 1, section Nhon - Hanoi Railway Station was approved in Decision 1970/QĐ-UBND dated July 24, 2009. Scale of construction: Total length of 12.5km, including 8.5km of elevated section (including 8 elevated stations from Nhon station to Cau Giay station), 4km of underground passage (including 4 underground stations from Ngoc Khanh station to the end of Hanoi Railway Station). Depot area is 15.05ha in Bac Tu Liem district. The maximum speed is 80km/h. The train length is from 60-120m. Axle load 15t/axle. Power supply is third-rail system. System safety is based on the overall monitoring of the ATC system.

The project is adjusted to increase the total investment by 50% and is about 8 years behind schedule compared to the original project due to the following reasons: (1) Change in construction unit price calculation factors, change in volume compared to the original Basic Design of project, (2) Project management apparatus is inexperienced, heavily dependent on

foreign consultants and sponsors, the feasibility study prepared by the consultant is not really suitable with reality, (3) The system of standards and design standards is still incomplete, (4) Investment regulations under Vietnamese law are different from those of sponsors, (5) Difficulty in working area clearance.



**Figure 11.** Metro line HN2A. Ha Dong Station – Cat Linh (operated)

(Source: Hanoimetro.net.vn)



**Figure 12.** Metro line HN3. Nhon – Hanoi Railway Station (in construction)

(Source: Hanoimetro.net.vn)

### **Metro Line No.2:** Noi Bai Airport – Thuong Dinh

The length of the metro line is about 35.2 km, which is the backbone for the current and future urban areas. Connecting with line 2 is the urban railway line 2A Cat Linh - Ha Dong with a length of about 14 km. There are currently 2 projects underway: (i) Project 1: the section Nam Thang Long - Tran Hung Dao is 11.5 km long. Project implementation status: In progress of technical design – Bidding – Construction; (ii) Project 2: Tran Hung Dao - Thuong Dinh 6Km long. Implementation status: is in the process of setting up an investment project. Project 1 was approved in Decision No. 2054/QĐ-UBND dated 13/11/2008. The route length is 11.5 km, of which 8.5 km goes underground, 3km goes overhead. This line used double tracks with gauge of 1435mm. There are 3 overhead stations, 7 underground stations and Depot location at Xuan Dinh, Tu Liem. Top speed will be 120km/h. The operating speed of the elevated section is 110km/h, and the underground section is 80km/h. The axle load is 16t/axle. This metro line will apply CBTC controlling system and third-rail system for power supply. The project has completed and approved the detailed depot planning, the master plan of the elevated section, the master plan of the 3 underground stations. The verification steps of the technical design and cost estimation of the elevated section and the depot are completed. The investor has been approved the results of 4 construction and installation bidding packages and the bidding documents for the equipment package.

The project has an adjustment to the total investment of 164% and the project progress is expected to be delayed about 3 years because (1) the project is first deployed in Vietnam, therefore, the system of standards and standards is incomplete; so it takes a long time for agreement and approval; (2) The design and planning of the total area of the route and stations in the old town area, which is densely populated, is complicated and takes a lot of time for consultation; (3) Adjustment and addition of Basic Design, some technical parameters such as axle load, maximum operating speed, design speed were changed, resulting in adjustment of tunnel structure, overpass, and station. Updating and optimising the system of infrastructure, vehicles and passenger service equipment to ensure safety, comfort, and environmental friendliness; (4) Projects using Japanese ODA loans under STEP loan conditions should be bound to originate from Japan (30% from Japan).

### **3.1.2 Current Vietnamese standards and regulations in implementation of metro projects**

#### ***Standards on train speeds and railway gauge***

QCQG 08:2015/BGTVT : National regulation on railway operation

QCQG 07:2011/BGTVT: National technical regulation on train operation and shunting.

TCVN 8585:2010: National Standard on Urban Railways

#### ***Standards on Railway Infrastructure Construction and Maintenance***

22 TCN 272-05 : Bridge design standards

22 TCN 221-95 : Design standards for traffic works in earthquakes

TCVN 6962-2001 : Vibration along construction activities and industrial production

TCVN 3905-84 : Design standards for Civil engineering.

TCXDVN 375:2006 : Earthquake resistant construction design

#### ***Railway applications – Signalling and Controlling***

TCCS 01:2009/VNRA : Design, construction and acceptance of railway signal works.

TCCS 10:2014/VNRA : Standards of supplies, materials, equipment and components used in the maintenance of works Information on railway signals.

#### ***Railway applications – Rolling stocks***

TCVN 9983:2013 - Standards of Design requirements for wagons operating on railways.

TCVN 9535:2012 - Standards of railway transport - Materials of locomotive.

TCVN 9273:2012 - Standards of urban railway vehicle of 1435mm gauge

TCVN 8546:2010 - Standards for railway transportation.

**To summarise**, it can be seen that Metro projects in Hanoi frequently suffer the same issue due to a lack of experience in conducting mega railway projects and current technology. As a result, from a management standpoint, technical standards are frequently insufficient and must be approved independently for each project, resulting in delays and a lack of coherence in the legal papers and national standards system. Furthermore, the quality monitoring of Basic Design, Technical Design, and Cost Estimation is limited, which frequently necessitates additional labour and increases overall expenditure in project phases. The lack of consistency and synchronisation in quality management from the design and manufacturing steps makes verification and acceptance of the project at the completion and implementation stages challenging. The Metro line 2A project's repeated delays, up to 24 months, are a prominent illustration of this issue.

## **3.2 Several significant problems in environmental and operational condition**

### **3.2.1 The climate conditions in Hanoi**

The climate of Hanoi is hot and humid subtropical with heavy rainfall. The city has a typical northern monsoon climate, hot and humid from May to September, and in winter from November to March it is relatively dry and cold (humidity halved) while light rain in spring (April). The average annual humidity is about 84%. The wettest period is the last months of winter (January, February, March), the average humidity reaches 85 - 87%. In terms of rainfall, Hanoi has an average annual rainfall of 1,676 mm or 140 mm per month. However, these averages do not represent the occasional heavy rains that are the main cause of flooding in Hanoi. Vietnam's National Center for Hydrometeorological Forecasting has documented some of the occasional heavy rains that lead to flooding.

As a result, the general climate of Hanoi is hot and humid, with a lot of rain, particularly from May to September. When operating in such conditions, railway transport trucks will be subjected to severe corrosive effects from the environment, as well as excessive abrasion. Local flooding may occur, especially during the rainy season, if there are no specialised prevention methods that affect the operation and technical condition of the vehicle. Furthermore, in such hot and humid conditions, the electrical equipment of the vehicle, as well as the signal infrastructure, degrades quickly, which must be examined on a regular basis, and adequate moisture-proof solutions are available. In high rain circumstances, including tropical storms, the power supply system uses a range of technologies such as overhead power supply (line 1), third rail power supply (line 2, line 3, line 2A). Special consideration should be given to the safety of the power supply network.

### **3.2.2 Hydrogeological conditions**

Hanoi's topography is relatively flat with an average height of 5-6m. Hanoi has many lakes with West Lake being the largest at 446ha. Small lakes such as Hoan Kiem, Thu Le, Kim Lien, Linh Dam, and Van Tri lagoon. These lakes and lagoons have a depth of about 4m. According to HAIDEP (2007) research, up to 50% of rivers and lakes play an important role in maintaining ecological balance for the region.

SYSTRA Consultants conducted a hydrogeological survey for Metro Line 3. According to this survey, based on data collected from foreign studies and the Northern Department of Planning and Source Survey. It was concluded that most of the groundwater in the Hanoi area contains quaternary sediments and is divided into two main aquifer systems. The upper groundwater aquifer system (UAS) consists of the Holocene qh aquifer separated from the C1 aquiludes aquifer and the C2 aquitard aquifer. The Lower Aquifer (LAS) has two Pleistocene aquifers qp1 and qp2, which are constrained by the lower aquifer "n". The survey report shows that along the alignment of the project, these two aquifers are connected mainly except for the Depot area and the beginning of the elevated section near Cau Giay station, these points are separated by a layer of non-clay clay. wet. However, hydraulic windows have been observed across the clay layer boundary.

**To summary**, despite the fact that Hanoi's environment does not have challenging conditions impacting the functioning of the railway system in winter, such as ice and snow, or substantial temperature changes between periods. High humidity, on the other hand, has a negative impact on the quality of railway equipment, particularly sensor and electromagnetic devices. The equipment in the Railway System, from rolling stock to

signalling system to auxiliary system equipment, is all designed and manufactured in Europe or Japan, and because the average humidity in Europe or Japan is much higher than in Vietnam, moisture-proof requirements are higher in the design and construction of strict equipment inspection and maintenance procedures. Furthermore, with significant rainfall concentrated in the summer, it is easy to create local flooding as well as two to three tropical storms every year. Because of the geological circumstances of low ground and many rivers, Hanoi's geological structure is quite fragile, and scientists anticipate that an earthquake will occur. As a result, when operating Metro lines, thorough and safe solutions for potential disaster conditions such as high winds, floods, and earthquakes are required.

### **3.2.3 Operational conditions**

Currently, because there is no line operated, this part evaluates the management and technical skills of urban railway operators and managers based on the training plan and staffing of the Metro line HN2A. By summarising Line HN2A's overall training plan, the following statements concerning urban railway human resources can be made:

Firstly, the staff is generally well-trained, including all titles and positions required to assure the operation and maintenance of the urban railway system. However, the number of staff, particularly train drivers, remains extremely restricted. In actuality, until December 2015, only 37 train drivers had completed the driver training course and were ready to serve the 2A line by the end of 2016. After completing the driving training, Beijing Railway will deploy personnel to Vietnam to train 421 additional personnel, including twelve train drivers. Although the training time for the train driver course in Vietnam is only 40 days, as opposed to 315 days in China for the first course, the quality of human resources trained in Vietnam can hardly be guaranteed. The situation is similar for maintenance and repair personnel and operation managers; training time in Vietnam is just about 30-40 days, compared to the first course's 80-190 days.

Second, as discussed in the section on natural conditions, due to the differences in natural characteristics, most of the time operating in hot and humid weather with a lot of rain, which differs from the conditions in China. The training in China may also not ensure full compliance with Vietnamese conditions, since the rate of occurrences and frequent breakdowns may differ from those in Vietnam, therefore technical professionals must be retrained on a regular basis in Vietnam.

Third, because the contractor is in charge of staff training, the costs of training, not training, and transferring all technology to the Vietnamese side will be minimised. The metro line's warranty duration is one year, during which time professionals from China will run, maintain, and repair it, and Vietnamese workers will study and practise case by case. After the one-year warranty expires, the full mining work is given over to Vietnam; however, with such a large number of people and training time, it may not be enough to ensure the system's proper operation. Furthermore, the urban train system is highly automated and specialised, with each employee performing distinct responsibilities that necessitate discipline and teamwork. However, the working style of Vietnamese workers is still constrained in this regard, although it has not been addressed in training activities.

Finally, in addition to the problem of inexperience in management and limitations in employee training, the issue of safety-oriented attitude and safety culture is regarded as a significant concern. Assessing the impact of this issue on the operation of a new system and Hanoi Metro's lack of management expertise, the study employed a safety survey to highlight critical topics in section 3.3 in the following.



### 3.3 Assessing The Safety Culture In The Vietnamese Railway Industry

This part of research presented the interview survey which carried out in 2018 regarding to analyse and clarify the safety attitude of railway staff in operation and maintenance the metro lines. The safety survey for Vietnamese metro system are presented in three parts: methodology of survey and questionnaire creation, statistical analysis for survey results and summary of key findings.

#### 3.3.1 Methodology

##### *Survey methods and questionnaire creation*

To assess the safety culture in the Vietnamese railway industry, this research created a rail-specific questionnaire in Vietnamese context including staff's attitude to safety risks, identification of potential safety problems and perception on the safety management system. The questionnaire was created and modified from April to July, 2018 and the survey was carried out in August to October, 2018. This questionnaire is divided into three parts with 75 questions which are described as in the following part. Each question was asked to select their level of agreement from 6-point Likert response scale from "Absolutely disagree" to "Absolutely agree", or their level of the implement from similar 6-point scale ranging from "Never" to "Very frequently".

1. Current status of safety risks under the railway expert's attitude, including 28 questions on six aspects: i) Problems of fatigue and stress; ii) Problems of Medical conditions and Pharmacology; iii) Problems of Violations; iv) Problem of Applicable skills; v) Problem of concentrated ability of workers; and vi) Problem of Organisational requirements. In this part, the question was concentrated on the status-quo of the working environment, labour quality and the relating problems. For example, several sample questions such as "They were encouraged by the employer not to attend work if they had had less than 6 hours sleep in the previous", "They were put under pressure to report for duty despite feeling fatigued", "They performed tasks under the influence of medication (both prescribed and self-administered) which could have potentially compromised rail safety" were used to indicate the problem of working pressure. Alternatively, this survey also tried to clarify the current situation of rule-breaking which is popularly occurred in Vietnamese and classify them into situational violations, routine violations, exceptional violations, or personally optimising violations by using several sample questions such as "They performed tasks under the influence of alcohol or illicit drugs which could have potentially compromised rail safety", "They broke the monotony of the task by engaging in various forms of entertainment while on duty", "They took shortcuts which could have potentially compromised safety because it had become standard practice – everyone does it all the time".

2. Potential safety problem under the railway expert's prediction, including 19 questions on six aspects: i) Communication; ii) Design phase; iii) Maintenance quality; iv) Management; v) Policies, rules and Procedures; and vi) External and environmental factor. In Vietnam, a metro system is absolutely a brand-new concept and none metro line has finished the construction and operated commercially yet. Therefore, there is little experience on metro operation and management; hence, this part of survey attempts to identify the potential safety problem by using expert knowledge and experience. It is only a qualitative assessment, however, in the phase of risk identification, it might be acceptable and an adequate method. Adjacent to prevalent risks in design, construction and maintenance phase, the questionnaire also intensified with potential failure in missing standardised management procedure and lacking of the effort to improve safety compliance, such as



“Lack of standardised approach to safety procedures”, “Lack of the employee’s effort to ensure compliance with safety rules”, “Lack of training in hazard identification before commencing any task”.

3. Expert’s perception on safety management system/procedure, including 28 questions on five aspects: i) Purpose of the safety management system; ii) Safety management procedure and Profitability; iii) Workforce interest in competency and safety training; iv) Workplace safety control; v) Safety audits and reviews. The knowledge on purpose and efficiency of safety management system are reviewed. Therefore, the attitude of railway experts to the necessity of applying the safety management system (or safety management procedure in the lower level of management) was estimated. Sample questions were arranged on an order of ascending consideration and effectiveness in expert’s attention, such as “The overall effect of safety management procedures is NOT necessarily properly considered in detail”, “The safety management procedures spread best practice and are refined for efficiency”, “Safety is seen as an optional expenditure”, “Safety is seen as costing money, and the only priority is to avoid extra costs”, “Training is aimed at changing the employee’s safety attitude rather than technique and procedure”, “There is an extensive internal audit program including cross-auditing within the organisation”.

### ***Sample size determination and classification.***

According to Green (1991), for a medium effect ( $R^2 = 0.7$ ,  $\beta = 0.02$ ) the rule-of-thumb for minimum sample size for a multiple regression is that the number of subject should be  $N \geq 50 + 8 \times m$ , in which,  $m$  is the number of predictors. In this rule, the research has the maximum of six aspects in each survey part, therefore, the minimum sample is 98 answers. For data reservation and improving the accuracy of analysis, the survey was implemented with 120 railway experts.

Each railway expert was recorded by two kinds of information as working position and professional experience. The working position was classified by company or organisation of the respondent: i) Authority (Department of Transport, Metropolitan Railway Management Board, etc.), ii) Operator (Vietnam Railway Company, Metro Company, etc.), iii) Academic/Engineer (University, Railway/Metro Consultant and Construction, Railway System and Equipment Manufacturer, etc.).

The professional experience indicated the professional aspect of respondent such as i) Construction Designer, ii) Construction Maintenance, iii) Controlling – Signalling, iv) Project Manager, v) Financial Manager, vi) Public transport operator, vii) Rolling stocks and railway equipment. These classifications were established in order to identify and assess the divergence on the attitude of experts on different phase or on different responsibility in a metro life-cycle. As a result, the influence of expert to technical solution in separated phase might be investigated.

### ***Statistical testing***

Firstly, the paper carried out the comparison of mean value of each position group or professional group to indicate the most significant risks in each group or the most distinctive trend between groups. Due to many questions in a safety risk group, an average mean value was calculated and called such as Stress and Fatigue Index (SR), Medical condition and Pharmacology Index (MR), Violation problem Index (VP), Applicable skills Index (AS), Concentrated ability Index (CA), Organizational requirement Index (OM). These indicators will be used in the following part of regression. In the part of Potential Safety Problem, the research tried to assess several reasons leading to urban railway incidents based on estimation and prediction of railway experts. These potential risks might be divided into 6

groups such as Communication Problem (CP), Design Problem (DP), Maintenance Problem (MP), Management Problem (MaP), Rule and Procedure Problem (RP) and External and Environmental Problem (EP). At the end of two parts, the research established a question which focus on the general assessment of railway experts in Current Safety Risks (CR) and Potential Risk Problems (PR). Both two variables are used in regression models as the dependent variables.

To analyse the scale reliability, the research considered the Cronbach's alpha test which is a measure of internal consistency. It describes how closely related a set of items are as a group. The formula for the standardised Cronbach's alpha:

$$\alpha = \frac{N \cdot \bar{c}}{\bar{v} + (N-1) \cdot \bar{c}} \quad (3.1)$$

Here N is equal to the number of items, c-bar is the average inter-item covariance among the items and v-bar equals the average variance. According to Nunnally (1978), the observed variable is accepted and retained in the model analysis when Corrected Item – Total Correlation  $\geq 0.3$ . The meaning of Cronbach's alpha value for separated variable is indicated that: (i) Value from 0.7 to 1.0: high reliability, (ii) Value from over 0.6: acceptable, (iii) Value lower 0.6: reject the variable from scale.

Finally, the research conducted the Multiple Regression to estimate the indexes of Current status of safety risks (CR), Potential safety problem (PR) by other independent observed variables; and furthermore, to assess influence of each observed variables to the final index. The general formula for final indexes were show as:

$$CR = \alpha 1. SF + \alpha 2. MF + \alpha 3. VP + \alpha 4. AS + \alpha 5. CA + \alpha 6. OM \quad (3.2)$$

In which: SF – Stress and Fatigue Index, MF – Medical condition and Pharmacology Index, VP – Violation problem Index, AS – Applicable skills Index, CA – Concentrated ability Index, OM – Organizational requirement Index.

Potential safety problem Index (PR)

$$PR = \beta 1. CP + \beta 2. DP + \beta 3. MP + \beta 4. MaP + \beta 5. RP + \beta 6. EP \quad (3.3)$$

In which: CP – Communication Problem Index, DP – Design Problem Index, MP – Maintenance Problem Index, MaP – Management Problem Index, RP – Rule and Procedure Problem Index, EP – External and Environmental Problem Index.

### 3.3.2 Result Description

#### *Worker's perception of safety risks*

Firstly, in the part of stress and fatigue problem, the problem of workload is usually a noticeable issue when the mean value indicated in several cases, the worker needs to work a long time and face to sleep disorders, especially in group of academic/engineer (value of 3.02 means that they rarely were encouraged to not to attend work after a long working shift or rarely have medical or psychological supports). For more details, construction designer and public transport operator had to face up to working pressure and long working period (3.23 and 3.21) more than the others. In the responding of the question "...encouraged by the employer not to attend work if they had had less than 6 hours sleep in the previous 24 hours...", 73/120 (60%) respondent said that never or rarely which illustrated the working pressure. However, most workers have not need to work on a night shift after a long waking time or they also had the good experienced advice to overcome stress problem.

Secondly, in the part of the medical condition, construction maintenance worker and financial managers sometimes worked under the influence of medication (4.00 and 4.30) or performed tasks despite sudden sickness. The problem of financial managers in this case, is not a serious issue influencing to railway safety, however, in the case of maintenance workers, it could affect to the quality of railroad which leads to derailment or infrastructure degradation.

Thirdly, the issue of rule-breaking seemed to be satisfied when the mean value is significantly low in every group, especially in controlling-signalling workers and rolling-stocks-related workers (value of 2.58 and 2.43 means that very rarely violated). However, when focusing on individual questions, there are several meaningful results:

- Question 13: "They performed tasks under the influence of alcohol or illicit drugs which could have potentially compromised rail safety". The result pointed out that 33/120 (28%) respondents answered "Very frequently" in general, and 6/15 (40%) construction-maintenance respondents, 4/17 (24%) controlling-signalling respondents, 4/19 (21%) rolling-stocks-related respondents answered "Very frequently" in particular.
- Question 18: "They broke the monotony of the task by engaging in various forms of entertainment while on duty". The result expressed that 48/120 (40%) respondents answered using a form of entertainment while on duty. It could lead to the worker distraction and limit the estimating and assessing ability, hence, an accident could happen.
- Question 20 "They took shortcuts which could have potentially compromised safety because it had become standard practice", 42/120 (35%) answered from "Almost agreed" to "Absolutely agreed", therefore, it could lead to routine violations explained in Paragraph 2.1. It might not cause a high risk but usually happen in high frequencies.

**Table 3.2** Average mean value of Current safety risk problems

| <b>Group</b>                      | Stress and Fatigue |                       | Medical condition |                       | Violation problem |                       |
|-----------------------------------|--------------------|-----------------------|-------------------|-----------------------|-------------------|-----------------------|
|                                   | <i>Mean</i>        | <i>Std. Deviation</i> | <i>Mean</i>       | <i>Std. Deviation</i> | <i>Mean</i>       | <i>Std. Deviation</i> |
| <b>Position</b>                   |                    |                       |                   |                       |                   |                       |
| <i>Authority</i>                  | 3.68               | 1.07                  | 3.54              | 1.61                  | 2.89              | 1.01                  |
| <i>Operator</i>                   | 3.91               | 0.95                  | 2.77              | 1.71                  | 2.64              | 1.04                  |
| <i>Academic/Engineer</i>          | 3.02               | 1.04                  | 3.55              | 1.07                  | 3.07              | 1.15                  |
| <b>Professional</b>               |                    |                       |                   |                       |                   |                       |
| <i>Construction Designer</i>      | 3.23               | 1.06                  | 3.32              | 1.24                  | 2.99              | 1.30                  |
| <i>Construction Maintenance</i>   | 3.50               | 1.04                  | 4.30              | 1.52                  | 3.00              | 1.20                  |
| <i>Controlling-Signalling</i>     | 3.90               | 0.89                  | 2.44              | 1.48                  | 2.58              | 1.09                  |
| <i>Financial Manager</i>          | 3.40               | 0.50                  | 4.00              | 1.49                  | 3.13              | 0.95                  |
| <i>Project Manager</i>            | 3.54               | 1.48                  | 3.38              | 1.40                  | 2.43              | 1.05                  |
| <i>Public transport operation</i> | 3.21               | 1.12                  | 3.35              | 1.11                  | 3.28              | 0.90                  |
| <i>Rolling stocks</i>             | 3.89               | 1.11                  | 2.50              | 1.63                  | 2.67              | 0.89                  |

Fourthly, it is a similar phenomenon to violation problem in the part of applicable skills issue when the mean value which is around 2.50 to 3.00 is acceptable. Notwithstanding, in question 21 that "They performed tasks that they had NOT been fully trained in" or question 23 that "They made potentially unsafe compromises because of equipment failure/mismatch", there is high level of agreed response (35% and 42% respondents) concentrated in group of controlling-signalling workers, rolling-stocks-related workers and construction maintenance workers.

Finally, in the part of concentrated ability problem and organisational requirements, the workers tried to accommodate the requirement of the working schedule, to comply with working regulation. However, they occasionally had trouble with rushing to complete tasks to stay on schedule or to a timetable (45%) or be under pressure to perform duties beyond the personal limits (40%).

**Table 3.3** Average mean value of Current safety risk problems (cont.)

| <b>Group</b>                      | Applicable skills |                       | Concentrated ability |                       | Organizational requirement |                       |
|-----------------------------------|-------------------|-----------------------|----------------------|-----------------------|----------------------------|-----------------------|
|                                   | <i>Mean</i>       | <i>Std. Deviation</i> | <i>Mean</i>          | <i>Std. Deviation</i> | <i>Mean</i>                | <i>Std. Deviation</i> |
| <b>Position</b>                   |                   |                       |                      |                       |                            |                       |
| <i>Authority</i>                  | 2.72              | 1.22                  | 3.12                 | 1.19                  | 2.51                       | 1.08                  |
| <i>Operator</i>                   | 2.85              | 1.11                  | 3.16                 | 1.49                  | 2.43                       | 1.15                  |
| <i>Academic/Engineer</i>          | 2.89              | 1.30                  | 3.50                 | 1.24                  | 3.13                       | 1.23                  |
| <b>Professional</b>               |                   |                       |                      |                       |                            |                       |
| <i>Construction Designer</i>      | 2.48              | 1.33                  | 3.20                 | 1.42                  | 2.90                       | 1.33                  |
| <i>Construction Maintenance</i>   | 2.53              | 1.12                  | 3.60                 | 1.16                  | 2.43                       | 1.37                  |
|                                   |                   |                       |                      |                       |                            |                       |
| <i>Controlling-Signalling</i>     | 2.78              | 0.99                  | 3.31                 | 1.66                  | 2.35                       | 1.09                  |
| <i>Financial Manager</i>          | 3.49              | 0.97                  | 3.03                 | 0.80                  | 2.73                       | 0.86                  |
| <i>Project Manager</i>            | 2.40              | 1.27                  | 2.79                 | 1.11                  | 2.59                       | 1.42                  |
| <i>Public transport operation</i> | 3.18              | 1.23                  | 3.60                 | 1.21                  | 3.28                       | 0.98                  |
| <i>Rolling stocks</i>             | 3.00              | 1.21                  | 3.28                 | 1.57                  | 2.53                       | 1.10                  |

The following step in the statistical test is Cronbach's alpha test which is a measure of internal consistency, that is, how closely related a set of items are as a group. As using SPSS, the research indicated several questions need to be deleted from the questionnaire in order to improve the reliability of scale as in the Table 3.4.

**Table 3.4** Item-Total Statistics in Stress and Fatigue Problem

|            | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|------------|----------------------------|--------------------------------|----------------------------------|----------------------------------|
| Question 1 | 27.36                      | 40.198                         | 0.432                            | 0.586                            |
| Question 2 | 27.18                      | 43.260                         | 0.322                            | 0.836                            |
| Question 3 | 26.45                      | 42.804                         | 0.400                            | 0.598                            |
| Question 4 | 27.38                      | 53.885                         | -0.158                           | 0.714                            |
| Question 5 | 27.57                      | 53.071                         | -0.122                           | 0.706                            |
| Question 6 | 26.55                      | 39.981                         | 0.490                            | 0.572                            |
| Question 7 | 26.29                      | 36.780                         | 0.680                            | 0.522                            |
| Question 8 | 26.40                      | 36.208                         | 0.656                            | 0.522                            |
| Question 9 | 26.55                      | 39.107                         | 0.503                            | 0.567                            |

- Group of questions in Stress and Fatigue problem: Number of questions are 9, Cronbach's Alpha value is 0.642 higher than 0.6 means that acceptable scale. The value of Corrected Item - Total Correlation of Question 4 and Question 5 are negative values. Therefore, they

have very little relative to the other observed variables, and we need to delete these answered results to increase the reliability of scale and improve the accuracy of the regression model in the next step.

**Table 3.5** Item-Total Statistics in Problems of Violation

|             | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|-------------|----------------------------|--------------------------------|----------------------------------|----------------------------------|
| Question 13 | 19.07                      | 52.978                         | 0.361                            | 0.840                            |
| Question 14 | 20.03                      | 52.932                         | 0.572                            | 0.797                            |
| Question 15 | 20.12                      | 53.825                         | 0.689                            | 0.785                            |
| Question 16 | 20.10                      | 51.924                         | 0.244                            | 0.834                            |
| Question 17 | 19.67                      | 52.560                         | 0.725                            | 0.779                            |
| Question 18 | 19.34                      | 52.597                         | 0.505                            | 0.807                            |
| Question 19 | 19.55                      | 53.695                         | 0.624                            | 0.791                            |
| Question 20 | 19.56                      | 53.744                         | 0.568                            | 0.797                            |

- Group of questions in Problems of Violation: Number of questions are 8, Cronbach's Alpha value is 0.821 higher than 0.7 means that high reliability scale. The value of Corrected Item – Total Correlation of Question 16 is lower than 0.3 values. Therefore, they have little relative to the other observed variables and we need to delete these answered results to increase the reliability of scale and improve the accuracy of regression model in the next step.

The research has highlighted that the Current Safety conditions are represented by Problem of Stress and Fatigue, Medical condition, Problem of Violation, Problem of Applicable skills, Problem of Concentrated Ability and the Organizational requirements, therefore the regression of Current Safety Risks Index will be as the following:

$$CR = \alpha_1. SF + \alpha_2. MF + \alpha_3. VP + \alpha_4. AS + \alpha_5. CA + \alpha_6. OM \quad (3.4)$$

To begin of regression model, the data of each observed variables were tested to ensure the independence. The dependent variable is the Current Safety Risks Index, giving in Table 3.6:

**Table 3.6** Model Summary for Current Safety Risks Index

| Model | R     | R square | Adjusted R square | Std. Error | Change Statistics |          |     |     |               |
|-------|-------|----------|-------------------|------------|-------------------|----------|-----|-----|---------------|
|       |       |          |                   |            | R square          | F change | Df1 | Df2 | Sig. F change |
| 1     | 0.883 | 0.694    | 0.678             | .46725     | 0.694             | 42.691   | 6   | 113 | .000          |

Predictors: SF, MF, VP, AS, CA, OM

Dependent Variables: CR

The table given an  $R^2$  value of 0.694 which shows that this model is relatively respectable representation of data, as almost 70% of variation can be explained by 6 variables. -The Coefficients in the regression model for Current Safety Index are shown in the following table:

**Table 3.7** Linear Regression Coefficients for Safety Risks Index

| Model      | Unstandardized Coefficients |            | Standardized Coefficients | t      | Sig.  | 95.0% Confidence Interval for B |       |
|------------|-----------------------------|------------|---------------------------|--------|-------|---------------------------------|-------|
|            | B                           | Std. Error |                           |        |       | Lower                           | Upper |
| (Constant) | -0.114                      | 0.230      |                           | -0.498 | 0.019 | -.569                           | .341  |
| SF         | 0.333                       | 0.041      | 0.440                     | 8.071  | 0.000 | .252                            | .415  |
| MF         | 0.048                       | 0.030      | 0.088                     | 1.601  | 0.012 | -.011                           | .108  |
| VP         | 0.478                       | 0.066      | 0.626                     | 7.230  | 0.000 | .347                            | .609  |
| AS         | 0.056                       | 0.056      | 0.081                     | 0.997  | 0.021 | -.055                           | .166  |
| CA         | 0.044                       | 0.046      | 0.070                     | 0.959  | 0.039 | -.047                           | .134  |
| OM         | 0.062                       | 0.050      | 0.090                     | 1.234  | 0.020 | -.038                           | .162  |

This table show that all 6 independent variables affect the Current Safety Risks index because all the p-values are below 0.05. It is also show that the linear equation of Current Safety Risks index is:

$$CR = -0.114 + 0.44SF + 0.088MF + 0.626VP + 0.081 AS + 0.070CA + 0.090OM \quad (3.5)$$

In which: SF – Stress and Fatigue Index, MF – Medical condition and Pharmacology Index, VP – Violation problem Index, AS – Applicable skills Index, CA – Concentrated ability Index, OM – Organizational requirement Index.

### **Potential safety problem**

In this part of the research, the survey tried to determine the railway worker/expert on potential of safety problem for the establishing metro system in Vietnam, particularly for Metro Line 2A in Hanoi which is planed for operation in December, 2021.

Firstly, in the part of potential communication failure, a significant response from direct worker suggested the problem of lack information about railway incidents from upper-level managers or other colleagues. Around from 20% to 30% workers in fields of controlling-signalling, rolling-stocks-related or maintenance workers have occasional mistakes when "...changes of operational/infrastructure circumstances had not been communicated to them...". The survey also indicated the similar percentage of workers having trouble with lack of "...information about potential safety risks such as observed defect in track, equipment and rolling stock from colleagues..." The valuable facts from this case are the high value of average mean in group of academic staffs/engineers or in group of designers and project managers. It indicated the attention in communication problem and potential solutions in design and management from these group staffs.

**Table 3.8** Average mean value of Potential Safety Problem

| <b>Group</b>                      | Communication |                       | Design      |                       | Maintenance |                       |
|-----------------------------------|---------------|-----------------------|-------------|-----------------------|-------------|-----------------------|
|                                   | <i>Mean</i>   | <i>Std. Deviation</i> | <i>Mean</i> | <i>Std. Deviation</i> | <i>Mean</i> | <i>Std. Deviation</i> |
| <b>Position</b>                   |               |                       |             |                       |             |                       |
| <i>Authority</i>                  | 2.59          | 1.29                  | 2.34        | 1.28                  | 2.90        | 1.24                  |
| <i>Operator</i>                   | 2.61          | 1.37                  | 2.66        | 1.24                  | 3.29        | 1.22                  |
| <i>Academic/Engineer</i>          | 3.09          | 1.47                  | 3.09        | 1.18                  | 3.42        | 1.11                  |
| <b>Professional</b>               |               |                       |             |                       |             |                       |
| <i>Construction Designer</i>      | 2.73          | 1.39                  | 2.60        | 1.39                  | 3.05        | 1.39                  |
| <i>Construction Maintenance</i>   | 2.37          | 1.58                  | 2.62        | 0.94                  | 2.93        | 0.84                  |
| <i>Controlling-Signalling</i>     | 2.50          | 1.38                  | 2.61        | 1.28                  | 3.18        | 1.25                  |
| <i>Financial Manager</i>          | 2.92          | 0.93                  | 2.08        | 0.90                  | 3.54        | 0.83                  |
| <i>Project Manager</i>            | 3.06          | 1.38                  | 3.00        | 1.32                  | 3.09        | 1.58                  |
| <i>Public transport operation</i> | 3.23          | 1.41                  | 3.43        | 1.20                  | 3.70        | 1.08                  |
| <i>Rolling stocks</i>             | 2.61          | 1.55                  | 2.53        | 1.31                  | 3.08        | 1.12                  |

Secondly, in the part of potential design failure, there is a noticeable value of the average mean value in group of public transport operators (3.43) and project managers (3.00) who usually faced with general limitations in metro lines in establishment phase and operating phase. For more details, approximate 35% respondents agreed with the problem of "...inadequate protection at level crossings..." and 13/20 (65%) public transport operation staffs recognised this failure in particular. In addition, 38% project-manager respondents indicated

the potential incidents when a system error happened, because of inadequate measures against error or inadequate train protection. Also, 11/20 (50%) public transport staffs complained about the poor design of equipment or rolling stock which might lead to operational risks.

The problem of potential designs are based on the lack of experience in metro system design and poor quality of design assessment. For example, based on author's experience in risk assessment of the technical design phase, there are few problems in the standard of anti-corrosion coating for railway track that was not compliance to the environmental condition, therefore, there is a need for surface treatment measures but not really guarantee the quality of rails. Or another example, the Automatic Protection System had mistakes in identified hazard of collisions in testing operation. Therefore, due to major problems in design and manufacture, the question of system reliability has raised in the experts' opinion.

Thirdly, in the case of potential maintenance, the high value of average mean in all groups (second ranking in the whole sex groups of potential risks) expressed the anxiety over maintenance quality of every respondent. Particularly, approximately 50% staff out of construction maintenance and the controlling-signalling group announced the equipment failure, poor condition of the track, rolling stock and/or signalling. Furthermore, the similar percentage of public transport operators and rolling stock workers argued about inadequate housekeeping (cleaning of facilities/operating equipment, tidy working environment, recovery from vandalism and ensuring clear track/signal sightings).

**Table 3.9** Average mean value of Potential Safety Problem (cont.)

| <b>Group</b>                      | Management  |                       | Policies, Rules, Procedures |                       | External factor |                       |
|-----------------------------------|-------------|-----------------------|-----------------------------|-----------------------|-----------------|-----------------------|
|                                   | <i>Mean</i> | <i>Std. Deviation</i> | <i>Mean</i>                 | <i>Std. Deviation</i> | <i>Mean</i>     | <i>Std. Deviation</i> |
| <b>Position</b>                   |             |                       |                             |                       |                 |                       |
| <i>Authority</i>                  | 2.99        | 1.31                  | 2.57                        | 1.34                  | 3.10            | 1.52                  |
| <i>Operator</i>                   | 2.49        | 1.27                  | 2.60                        | 1.26                  | 3.04            | 1.58                  |
| <i>Academic/Engineer</i>          | 3.32        | 1.01                  | 3.39                        | 1.24                  | 3.63            | 1.24                  |
| <b>Professional</b>               |             |                       |                             |                       |                 |                       |
| <i>Construction Designer</i>      | 3.20        | 1.33                  | 2.89                        | 1.45                  | 3.14            | 1.40                  |
| <i>Construction Maintenance</i>   | 2.37        | 1.17                  | 2.75                        | 1.23                  | 2.65            | 1.12                  |
| <i>Controlling-Signalling</i>     | 2.21        | 1.43                  | 2.15                        | 1.15                  | 3.34            | 1.53                  |
| <i>Financial Manager</i>          | 3.63        | .75                   | 2.92                        | .83                   | 3.42            | 1.32                  |
| <i>Project Manager</i>            | 3.11        | 1.26                  | 3.27                        | 1.57                  | 3.14            | 1.79                  |
| <i>Public transport operation</i> | 3.51        | .68                   | 3.61                        | 1.10                  | 4.11            | 1.22                  |
| <i>Rolling stocks</i>             | 2.54        | 1.19                  | 2.50                        | 1.34                  | 2.95            | 1.51                  |

In the Problem of Management and Rule Compliance, the low value of average mean in group of authority (2.99 and 2.57) and operator (2.49 and 2.60) pointed out the high expectation on management quality and adequacy of policies and regulations. However, there are several points need to improve as in the following: 46/120 (38%) staffs thought that the training in hazard identification was not enough, especially in group of public transport

operator (55%). 39/120 (32.5%) respondents indicated that it is lack of standardised approach to safety procedures. The same percentage experts reported the problem of inadequate safety standards and procedures (including those for operations, signalling, inspection, maintenance). In addition, 32/120 (26%) staffs assumed that procedure manuals and checklists were hard to understand or not available. In the Problem of external and environmental factors, 65/120 (54%) respondents suggested that the reckless behaviour of pedestrians and vehicle drivers at level crossings could lead to accidents. Furthermore, 55/120 (46%) staffs indicated there might be unexpected intrusion across the track by people, animals and other object.

The following step in the statistical test is Cronbach's alpha test which is a measure of internal consistency, that is, how closely related a set of items are as a group. As using SPSS, the research indicated all of the questions are highly related to the others in the same group, satisfying the testing conditions of Cronbach-Alpha test.

The research has highlighted that the Potential Safety Problems are represented by Problem of Communication (CP), Problem of Design (DP), Problem of Maintenance(MP), Problem of Management(MaP), Problem of Rules and Procedures (RP) and the Problem of external and environmental factors (EP), therefore the regression of Potential Safety Index will be as the following:

$$PR = \beta_1. CP + \beta_2. DP + \beta_3. MP + \beta_4. MaP + \beta_5. RP + \beta_6. EP \quad (3.6)$$

To begin of the regression model, the data of each observed variables were tested to ensure the independence. The dependent variable is the Potential Safety Problem Index, giving the following results:

**Table 3.10** Model Summary for Potential Safety Problem Index

| Model | R     | R square | Adjusted R square | Std. Error | Change Statistics |          |     |     |               |
|-------|-------|----------|-------------------|------------|-------------------|----------|-----|-----|---------------|
|       |       |          |                   |            | R square          | F change | Df1 | Df2 | Sig. F change |
| 1     | 0.868 | 0.754    | 0.741             | 0.57459    | 0.754             | 57.629   | 6   | 113 | .000          |

Predictors: CP, DP, MP, MaP, RP, EP

Dependent Variables: PR

The table gives an  $R^2$  value of 0.754 which shows that this model is a relatively valuable representation of data, as almost 75% of variation can be explained by six variables. The Coefficients in the regression model for Current Safety Index are shown in the Table 3.11.

This table shows that all six independent variables affect the Current Safety Risks index because all the p-values are below 0.05. It is also shown that the linear equation of Current Safety Risks index is:

$$PR = 0.262 + 0.252CP - 0.024 DP + 0.290MP + 0.087 MaP + 0.132RP + 0.339EP \quad (3.7)$$

In which: CP – Communication Problem Index, DP – Design Problem Index, MP – Maintenance Problem Index, MaP – Management Problem Index, RP – Rule and Procedure Problem Index, EP – External and Environmental Problem Index.

**Table 3.11** Linear Regression Coefficients for Safety Risks Index

| Model      | Unstandardized Coefficients |            | Standardized Coefficients | t      | Sig.  | 95.0% Confidence Interval for B |       |
|------------|-----------------------------|------------|---------------------------|--------|-------|---------------------------------|-------|
|            | B                           | Std. Error | Beta                      |        |       | Lower                           | Upper |
| (Constant) | 0.262                       | 0.167      |                           | 1.571  | 0.019 | -0.069                          | 0.593 |
| CP         | 0.204                       | 0.055      | 0.252                     | 3.721  | 0.000 | 0.095                           | 0.312 |
| DP         | -0.021                      | 0.069      | -0.024                    | -0.306 | 0.046 | -0.159                          | 0.116 |



|     |       |       |       |       |       |        |       |
|-----|-------|-------|-------|-------|-------|--------|-------|
| MP  | 0.273 | 0.067 | 0.290 | 4.096 | 0.000 | 0.141  | 0.406 |
| MaP | 0.080 | 0.072 | 0.087 | 1.099 | 0.024 | -0.064 | 0.223 |
| RP  | 0.113 | 0.079 | 0.132 | 1.426 | 0.042 | -0.044 | 0.269 |
| EP  | 0.262 | 0.044 | 0.339 | 5.962 | 0.000 | 0.175  | 0.349 |

### ***Workers' perception of safety management procedure***

This part of research focused on several separated aspects in applying safety management system (SMS) and related problems such as Purpose of SMS, Profitability of SMS, safety training, workplace safety control. The primary purpose of these questions is finding the ideas or personal assessment. Therefore, the statistical methods in this part only concentrated on comparing attitudes of workers/experts, not establishing the regression model.

In the part of safety management procedure's purpose, most of the respondents (70%) thought that "The overall effect of safety management procedures is necessarily properly considered in detail", however, 65% public transport operation and 30% signalling-controlling respondents indicated the inconvenience of safety management procedures. Simultaneously, approximate 60% signalling-controlling workers, 32% rolling-stock staffs and 65% public transport operator complained about the deficient quality of safety procedure training. In the part of profitability of safety management procedures, 50/120 (42%) respondents seen safety as an optional expenditure, including 54% financial manager and 38% project managers. As a result, safety cost is depreciated and they deducted technical solutions for ensuring system safety level. Fortunately, 67% construction maintenance, 88% signalling-controlling staffs, 79% rolling-stock staffs and 77% financial managers remained the appreciation on maintenance role to prevent accidents. In the part of workforce interest in competency and safety training, 80% respondents indicated that they only "...attended the training which required by law..." and 34% respondents expressed that "compulsory training during work hours gives employees a pleasant break from work that they carry out in a harsh working environment". They also determined the purpose and methods of training is "...changing the employee's safety attitude rather than technique and procedure..." (62%). Finally, on the aspect of workplace safety control, the safety management controls are sufficiently applied at most companies (70% respondents agreed). However, 63% staffs assumed that "...little systematic use of the standard work-related safety management controls...", especially in construction maintenance (80%), controlling-signalling (82%), rolling-stock group (63%).

### **3.3.3 Key Findings**

After using statistical analysis for survey results, several findings were summarised as in the following:

- According to the regression equation (3.5), the main problem of current safety condition is the Problem of Violation and Problem of Stress and Fatigue. The problem of stress and fatigue is generally generated from external factors such as lack of employer and high working pressure. Whereas the problems of violation included many serious personal failures of staff such as using alcohol or drugs, spending working time for entertainment or taking risky short-cuts as a standard practice. The suggested solutions to deal with these problem are prepared and expressed in the following part.

- According to the regression equation (3.7), the main problems of Potential Safety Problem are the Problem of Communication, Problem of external factors and Problem of Maintenance. The main current safety problem which is concluded in equation (3.5) are presented

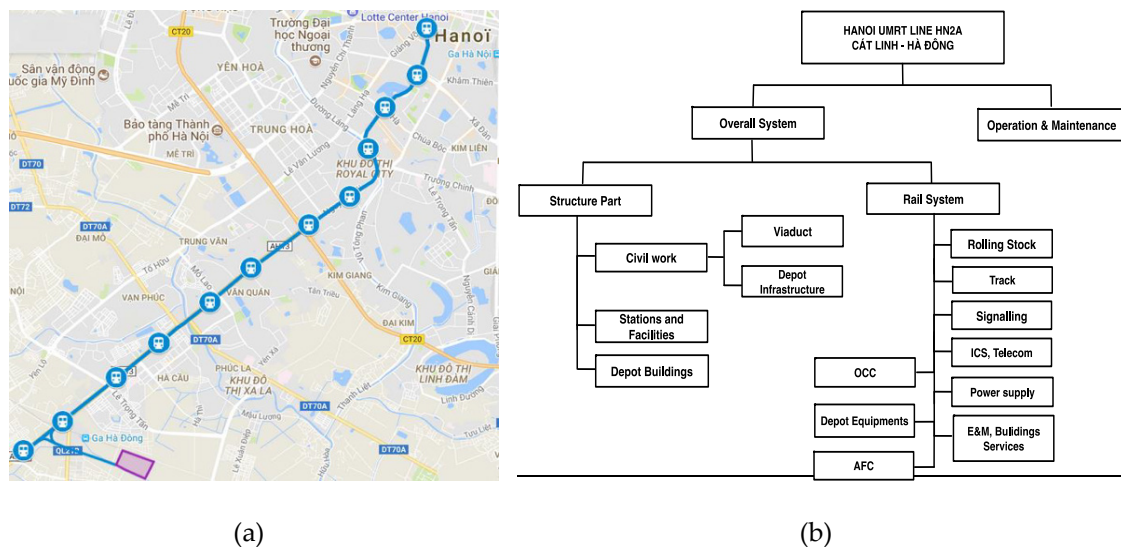
in the detailed aspects of the metro system. The Problem of Communication and Problem of external factors significantly related to safety culture in the working area and passenger consciousness. The Problem of Maintenance is more influenced by rule and procedure compliance than existing technical solutions. It can be summarised that the main solutions needed to be paid attention are providing technical solutions for warning and prevent human failures in every component of the metro system and upgrading the safety culture, to ensure the workers/passengers prevent high-risk actions themselves. For example, a comprehensible set of safety management guidelines might be an effective solution for standardising working procedure, reducing the misunderstand and communicating to wrong people in communication problem. It is also a hazard identification document to indicate all of possible failure in operating, therefore, the railway staff could recognize the potential incident for avoiding. It is possible to improve the safety level. Finally, the problem of stress and fatigue are limited by an effective working schedule which has the longest shift is under 10 working hour (according to the plan of operation scheme for Hanoi Metro Line HN2A). However, we also need to pay attention to recheck the working schedule and worker's condition to inhibit the unfavourable impacts of stress and fatigue.

- Based on conclusion of perception of safety management procedure, most of railway experts/staffs depreciated the role of safety management procedures/safety management system, had dubious motivation in competent and safety procedure training. Therefore, the quality of procedure application is really limited in both procedure preparation phase and applying phase.

### 3.4 System description of Hanoi Metro Line HN2A. Cat Linh – Ha dong Station

#### 3.4.1 Overview of metro lines

Hanoi Urban Railway Cat Linh - Ha Dong Line UMRT HN2A is a 13021.48 m long elevated light rail transit project with total 12 stations, the average distance between stations is 1151m and will be the main southwest traffic route in the urban transport network of Hanoi city (Figure 15a). One Rolling Stock Depot with integrated functional maintenance center and operation control center is deployed into this line and located at the southeast of Ha Dong station. All 13 trains will operate as 4-car trains, whose designed maximum speed reaches 80 km/h, and be run in the initial stage of HN2A project with a service speed of 35 km/h. This line HN2A is fully automatic operated and controlled under the signaling system Moving Block - Communications Based Train Control (CBTC). The trial operation of the project HN2A was divided into two phases: trial operation from October 2018 to December 2018 and full-scale test run from December 12, 2020 to December 31, 2020 in order to check its safety before it can be approved for commercial service. From November 6, 2021 Line HN2A is put in commercial operation. The equipment of the entire UMRT Line 2A Cat Linh - Ha Dong is designed for installation and use for typical environmental conditions of Hanoi city. Outdoor equipment must be suitable for usage in environmental conditions and in natural ventilation, and be able to resist water, moisture, rain and flushing..



**Figure 13** Overview of Hanoi Urban Railway Line HN2A (a)  
Structure of Line HN2A sub-system (b)

The information and features of the System specifications are collected and cited from Technical Designs and Feasibility Report from Beijing Urban Engineering Design and Research Institute Co., Ltd, the design contractor of Metro Line HN2A :

- Technical Design and Feasibility report statement (BUEDRI, 2010)
- Volume 1: Track, Station and Line (BUEDRI, 2009).
- Volume 3: Rolling stocks (BUEDRI, 2011).
- Volume 4: Signal system (BUEDRI,2014)
- Volume 8: Risk Assessments and Safety Management (BUEDRI,2015)

### 3.4.2 Infrastructure

Primary technical features of track and infrastructure of Line HN2A are:

All 13 trains will be train type B of 1435mm double lines, operate as 4-car trains, whose designed maximum speed reaches 80 km/h, and be run in the initial stage of HN2A project with a service speed of 35 km/h. Travel form is Right-side form, which includes right line from Cat Linh Station to Ha Dong Station and left line from Ha Dong Station to Cat Linh Station.

Minimum curve radius: (i) Main line section: Not less than 300 m normally and 250m under difficult conditions; (ii) Main line of station: Straight line normally and 800 m under difficult conditions; (iii) Auxiliary lines: 200 m normally and 150 m under difficult conditions; (iv) Yard line: 110 m. The minimum length of circular curve for main lines and auxiliary lines should not be less than 20 m and not less than the total wheel base of a vehicle under difficult conditions.

The maximum slope of main lines should not exceed 30‰, 35‰ can be adopted at difficult locations and the maximum slope of contacting line and release line should not exceed 40‰. The calculated line of station platform for viaduct should be set on flat slope or at difficult location with a slope of less than 3‰. The yard track should be set on flat slope and the outside line can be set on the road with a slope of less than 1.5‰. The turnout branch line should be set on the road with a slope of less than 5‰ and 10‰ at difficult locations.

The gauge of the project was designed based on a maximum velocity of 80km/h for trains on the section and a maximum velocity of 55km/h for the station; an overspeed of 5km/h is allowed for temporary.

Track: (i) Viaduct section and stations: The structural height of the track is 500 mm; (ii) The switch of main line adopts No.9 straight switch at 60kg/m and the depot adopts No.7 switch. (iii) Track superelevation: Positive line curve is the largest high value of 120 mm

Clearance: (i) Road clearance is 4.75m; (ii) Railway clearance is 5.3m.

### 3.4.3 Power supply characteristics

The electrical loop mode between stations and between rectifier substations is the recommended solution. However, electrical loops for High Voltage Lighting and Power network and Electrical Traction high voltage network have to be separated for safety reasons.

Electric Power is supplied by two 22kV High voltage stations. In case one of stations is error so all charge is supported for line by only one station so that high voltage cable which connect from each High voltage station to line cable must have double capacity as compared to normal operation. Because the impedance of the electrical circuit (cables, primary network, transformer), the voltage cannot be exactly the same in all the location of the high voltage feeder lines; therefore, standards allow the following variation for AC voltage of  $\pm 5\%$ .

The low voltage network will be supplied by electrical feeders coming from the High Voltage Lighting and Power network. High voltage electrical feeders will be laid, separately, in the cable trough along both tracks for safety reasons. This network consists of lighting and power substations installed in each passenger station and in the depot. Two types of lighting and power substations are to be considered including lighting and lower substation for underground stations and for elevated stations.

Lighting and power substations are symmetrical, and each of the two transformers (T1 and T2) has its own 22 kV independent High Voltage incoming cell. These transformers supply the low voltage equipment with 230/400 V AC, 3-phase + neutral; this electrical equipment can be divided into several groups:

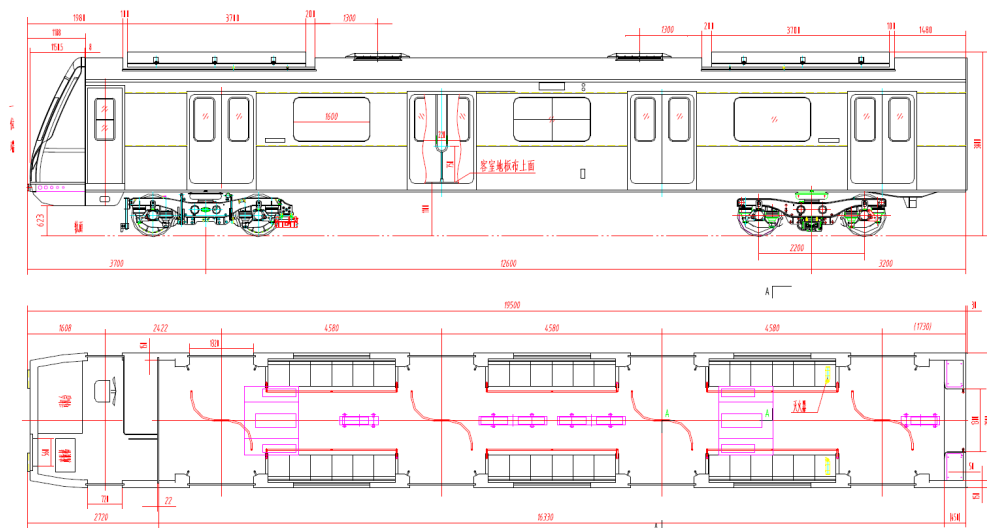
- Lighting and Power equipment in elevated and underground stations:
- Equipment required for proper operation of the Metro Line
- Equipment which do not affect proper operation of the Metro Line
- Equipment required for emergency situations of the Metro Line
- Comfort-related Equipment.
- Lighting and Power equipment in the Depot:

The low power supply of the depot is also symmetrical, fitted with 2 transformers connected to two independent High Voltage incoming cells. These transformers supply the 230/400 V AC 3-phase depot equipment.

The power collection of rolling stocks: The mode of power collection must be appropriate to the system requirements, avoid unsightly elements and allow optimising the capital cost (especially driven by the diameter of the tunnel). In this respect, it has been decided to use: (i) No overhead line equipment; (ii) Third rail-type system at track level with current collection from above. The maximum and minimum voltages of 750V traction supply system shall be as follows: Nominal voltage 750V; Minimum working voltage 600V; Maximum working voltage 900V; Minimum abnormal voltage 500V.

### 3.4.4 Rolling stocks

- Size and dimensions :



**Figure 14.** Main dimensions for rolling stocks of Metro Line HN2A

Car length over couplers and  $\frac{1}{2}$  gangway..... between 19.5-20m  
 Maximum train length over coupler .....~100m  
 Maximum height from top of rail to floor ..... 1,100 +20/-50mm  
 Nominal clear height inside the car .....2.10m  
 Distance between pivots of bogies .....between 11m and 13m  
 Maximum bogie wheelbase.....2 m

Car width .....between 2.75 – 2.85m  
 Maximum car height (rail top to roof top) with air-conditioning units .....3.80m  
 Assuming a steel wheel track system, track gauge is the standard gauge .....1,435 mm  
 Maximum axle load.....16T  
 According to this value, maximum wheel diameter could be about.....860mm

- Performances and Traction effort:

**Table 3.12.** Main features of train traction and performance

|  |                      |
|--|----------------------|
| Starting acceleration at least equal to  | 1m/s <sup>2</sup>    |
| Acceleration at least equal to from 0 to 35km/h                                | 0.85m/s <sup>2</sup> |
| Electric Service brake rate (maximum) at maximum load                          | 0.95m/s <sup>2</sup> |
| Emergency brake rate (maximum) without taking into account any jerk limitation | 1.25m/s <sup>2</sup> |
| Maximum speed  | 80km/h               |
| Design speed   | 90km/h               |

Usual performances shall take into account the line profile and operation requirements as average commercial speed, dwell time and maximum speed. On dry, tangent and level track under 750 VDC electrical supply, with 6 passengers/m<sup>2</sup> car weight, values are as in Table 3.12.

- Weight and axle load: The average passenger weight considered is 65kg. The ratio of weight to surface (overall length x max width) of an empty vehicle shall not exceed 600kg/m<sup>2</sup>. The maximum track axle load shall not exceed 16 tons/axle.
- Braking system: Braking system shall be of a computer-controlled electro-pneumatic type and shall consist of:
  - + Service brake: electrical regenerative brake combined with pneumatic brake; electrical brake has priority and blending with the pneumatic one is computer-controlled in order to achieve the requested deceleration level; the service brake shall have to stop the train within the defined braking distance, irrespective of the load condition; should the power line be nonreceptive during electrical braking, energy would be consumed in resistances;
  - + Emergency brake: as the service braking, automatically applied under emergency conditions, and shall have to stop the train in AW4 load condition running on a straight and on level track from the maximum speed within the defined braking distance,
  - + Parking brake: fitted with springs, able to fix the train in depot or in line,
  - + Safety brake: it shall be a pneumatic brake and shall have to stop the train in strict conditions,
  - + Holding brake: during train stops in stations the train holds by mean of the pneumatic brake, controlled by the train computer.

### 3.4.5 Signalling and Controlling system

Line HN2A is operated under a continuous communication-based system with 3 operating levels and 4 driving modes. Three levels of operation are in the priority of CBTC, ITC, Interlocking. CBTC mode is normal mode, ITC and Interlocking are degraded in modes 1 and 2 respectively. Four driving modes including operation are

- (i) AM- Automation driving under ATP supervision, train operation is granted through the radio system and track-side signals “off” in AM mode;
- (ii) CM - Manual train driving mode under the supervision of ATP and the track side signals;
- (iii) RM - Restricted manual train driving mode. Safety of train operation is ensured together by interlocking equipment, on board ATP, dispatching staff, train drivers; and
- (iv) NRM - Non Restricted Manual Mode: on-board signalling system is in the non-available state, the train driver drives with the dispatch command and displays of the trackside signals.

The CBTC system of the Line HN2A schematically sketched in (PMU,2019) and shown on Fig 3.6. The entire main line is divided into four interlocking zones, each equipped with a central interlocking (CI) and local Automatic Train Supervision ATS equipment, who is located in Cat Linh, Thuong Dinh, Phung Khoang and Van Khe stations. Line HN2A adopts the system CBTC LCF-500 from TCT which consists ATP/ATO, CI, DCS, ATS and MSS sub-system. Distributed monitoring system ATS and train protection system ATP provide train headway control and over speed protection. Train auxiliary operation system ATO is to realize automatically operation base on ATS command, TSR/PSR conditions which under ATP protection. Four station control area CIs are failure-safe mode system, which is to realize basic interlocking function normally. In CBTC control level, CIs provide related route information in accordance with moving block requirement and control area ZCs, whose equipment was installed in the Cat Linh and Van Khe stations, send the movement authority to train. In ITC control level CIs provide related route information in accordance with fixed block requirement and send movement authority via Balise. Data communication system DCS realizes data transmission between wayside an on-board system. MSS maintenance supports system offers equipment work status monitoring and maintenance support function for CBTC system. Wayside signalling equipment are signal, switch point, axle counter, LEU, variable Balise, loop and fixed Balise. The function of Automatic Train Supervision - ATS is clarified as in the following (as seen in Figure 17 and 18):

**Line and depot supervision:** This function shall present the Hanoi Pilot Light Metro Line transportation network including the depot. This function shall provide supervision and control of all the track, wayside, stations and depot equipment related to traffic operations.

Those equipment related to traffic operations shall be: (i) equipment of the signalling system (including track-circuits, signals, track-switches, interlocking, ATC controllers); and (ii) traction power facilities.

This function shall be coupled with the traction management functions. Information shall be made available on Man Machine Interface. Locally, an authorised traffic operator such as a main station’s supervisor shall be able to supervise and control local traffic on a section of the line such as terminal station.

**Train supervision:** This function shall monitor train equipment and component status by detecting and reporting all events and alarms transmitted by the rolling stock system through the radio network.

Events and alarms monitoring is necessary to ensure train availability for line operation service. The ATS shall report all available alarms and events concerning: (i) ATC on-board components and (ii) Rolling stock.

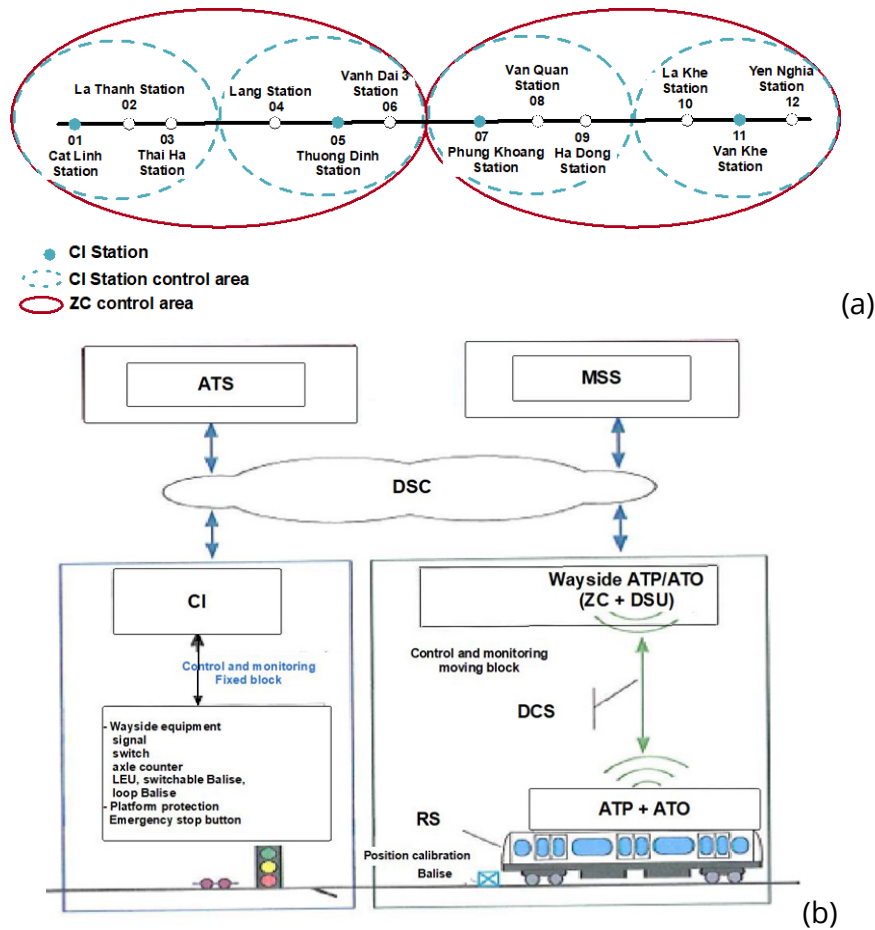
**Train Tracking:**

- Detecting any train movement and determining accurately the position of all trains on mainline and depot.

- Ensuring the consistency between train location and train identification.
- Reporting failures or alarms
- Several trains situated on the same single track section.
- Communications loss with CBTC-equipped trains.

The “Train Tracking” function must rely on two detection mechanisms:

- Primary detection: uses the information transmitted periodically by the ATC subsystem. Each CBTC-equipped train communicates its position and its rolling stock's identity to the ATS sub-system.
- Secondary detection: uses the information received from the signalling system. The ATS sub-system shall determine the train's localization thanks to the status acquisition of wayside equipment such as track circuits, axel counters and points.



**Figure 15** (a) Zone of interlocking control for UMRT Line HN2A sub-system

(b) CBTC Structure of Metro Line HN2A

Thanks to the primary detection, the ATS sub-system is able to track movement of the CBTC equipped trains which are passing through faulty track-circuits. The secondary detection represents a backup solution which allows to track the train movements in case of failure or unavailability of the primary detection (e.g.: non-CBTC trains, communication loss with CBTC-equipped trains).

**Identification.** The following attributes are allocated to each train:



- Rolling stock ID: Unique number which identifies a physical train. In nominal mode, such data is automatically provided by the on-board ATC equipment. In case of degraded mode (i.e.: non-CBTC train, communications failure with CBTC-equipped train), the ATS sub-system shall enable the traffic operator to assign a Rolling Stock ID to a given train, according to the information provided by the driver.
- Exploitation ID: Number which identifies a train from an operational point of view. Based on the timetable and the trains localisation, the ATS system shall automatically assign an exploitation number to each train ready to start a commercial service. Moreover, the ATS sub-system shall reset the exploitation number of a train parked in terminus or depot after having accomplished its last trip. Regarding the provisional services, the traffic operator is in charge of assigning an Exploitation ID to each train.

Such attributes are displayed on the VCP and on the traffic console at the same time as the status of signalling equipment (e.g.: track circuit occupancy, track-switch position). There should exist a special mark to distinguish trains which have been assigned a Rolling Stock ID by the traffic operator. When the ATS sub-system detects the presence of a train without Rolling Stock ID assignment, it shall alarm the traffic operator.

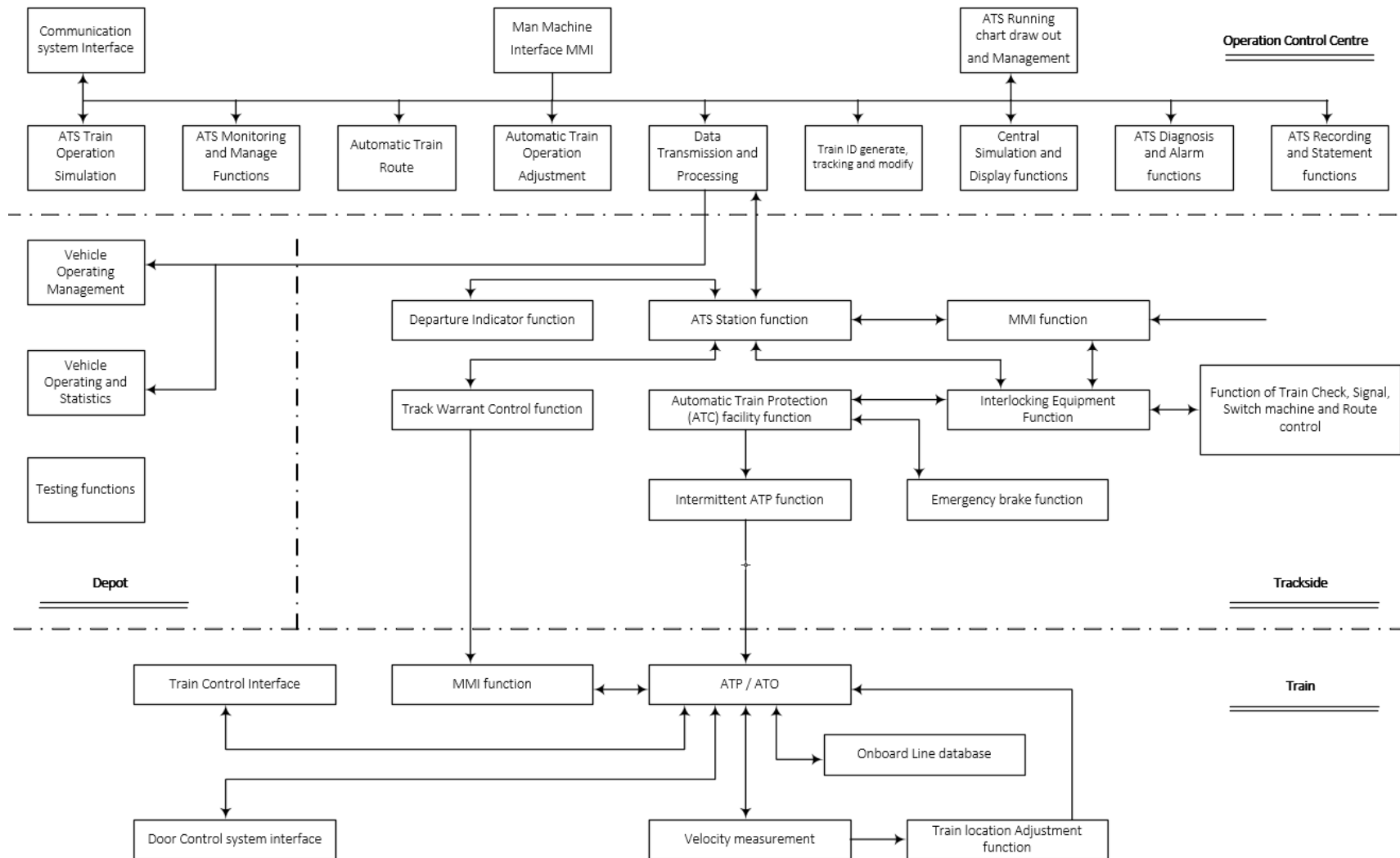
**Traffic management.** The ATS will control the following

- Timetable management: Timetables shall define, according to the operation program, the schedule (or headway) and type of service for each train during peak and off-peak hours.
- Train Dispatch: Line Insertion & withdrawal. Insertion-withdrawal of trains on line shall be manual or automatic. In automatic mode, the system shall analyse the operating conditions and send to the operator the results on the opportunity concerning insertion or withdrawal of a train. This function shall automatically manage train dispatching from or to depot's transfer tracks in order to adjust the train number on line necessary to follow the peak and off-peak hour needs defined in the operational timetable. This function shall manage the terminus route control.

**Traffic regulation:** Traffic regulation consists in the following operations:

- Adapting car passage frequency to the daily request,
- Absorbing any possible disturbance by all cars on the line at a moment and enabling the delayed train set(s) to make up time to provide a constant inter-car interval.

The traffic regulation functions shall maintain regularity of service according to the operation plan defined by the selected timetable and operating mode.



**Figure 16** Function of Signal System of Line HN2A

### **3.5 Safety-related issues in System Acceptance phase of Hanoi Metro Line HN2A projects**

The planning and construction of the Metro Line HN2A project began in 2009 and is anticipated to be finished in 2015 under the design and manufacture of Chinese contractors. The actual completion date has been pushed back to 2018. Hanoi Metro Company was founded in 2014 with the purpose of training railway staffs and prepare operating procedures and conditions for Line HN2A and following lines.

There are 03 testing operation phase of metro line HN2A as in the following:

- Phase 01 from 01.10.2018 to 10.12.2018 in China: including tested operating and system safety checking, operated as around 35% operation schedule. Total operation length in this phase is 85.455 train-operation-kilometres.
- Phase 02 from 11.12.2018 to 31.12.2018 in China: including tested operating at 100% system capacity with 272 trains/day. The total operation length in this phase is 70.747 train-operating-kilometres.
- Phase 03 from 06.12.2020 to 30.12.2020 in Vietnam: Testing and acceptance phase. Tested operating as 100% system capacity with 272 trains/day. Total operation length in this phase is 84.966 train-operation-kilometres.

After 02 testing phase in China, the project are progressed to the System Acceptance and Safety Certificate phase. This process takes 2.5 years from March 2019 to June 2021 to obtain the Safety Certificate and start commercial operation in November 2021. However, while analysing and certifying system safety, the Apave - Certifer - Tricc safety consultancy consortium (ATC) identified numerous manufacturing and risk assessment issues. The following are the key issues with the metro line HN2A's system safety. (ATC, 2019).

#### **3.5.1 Safety-related key issues founding in System Acceptance phase of metro line HN2A**

##### **1. The Safety Management System and Risk Assessment documents**

These documents were not provided or proven during the design and production of the Rolling Stocks sub-system.

Both the investor and the design-manufacturing contractor are to responsible for this problem. The contractor BSR (Beijing Subway Rolling Stock Equipment) stated that there was no requirement for Safety Integrity Level (SIL) in the project contract. The contractor also stated that there were no SMS and risk assessment method standards in China at the time of contract signing for the HN2A project in 2008.

The contractor furnished RAMS-related documentation for the braking subsystem. However, according to the safety assessment warning, there is no proof that the safety and security measures have been implemented. Moreover, SIL certificates are only legitimate when supported by technical evidence. SIL certifications (which must be confirmed) are required for train/metro safety. The ATC consultancy verifies that system safety cannot be ensured if only a fraction of safety functionality meets SIL safety integrity standards (software). To assure the safety level of a safety function, all other components must be demonstrated to have the same level of security (see in § 5.3.2.6, § 6.3.2 and § 6.4.3 in EN 50126, 2018).

Therefore, Hanoi Metro Company must conduct on-site testing, design a Safety Management System strategy, and conduct extra risk assessments.

## 2. Testing and validation procedure

The ATC consultancy suggested 03 types of assessments for system acceptance:

- Assessed by related standards: If sufficient proof is provided that the relevant safety and design standards are met, the sub-system is accepted.
- Assessed by similar system: If the equipment, sub-system has been safely manufactured, installed and operated in similar systems, then the sub-system is safely accepted. The similar systems are referenced as Line Northeast of Singapore, Line 3 of Shanghai, Line 1 extension and Line 2 extension of Shanghai, Line 1 and Line 2 of Nanjing.
- Assessed by on-site testing: If the system cannot be proved secure by the above two methods, then perform on-site testing with the assessment of ATC consultancy.

During on-site testing, the ATC consultant pointed out the following errors:

- Errors of door indicator lights and emergency exit buttons.
- The ventilation system does not operate safely in the event of a fire and does not prevent smoke and fire entering the metro train.
- There is no automatic fire alarm system in the train.
- Inadequate, ineffective, and unsafe passenger information instructions at the station in case of needing to evacuate passengers

## 3. Errors in signalling system in CM- Manual train driving mode

Trackside signal is out of sight in curves.

### 3.5.2 Outline the solutions for System Safety of Metro Line HN2A

The safety issues pointed out by the ATC advisory show two major problems.

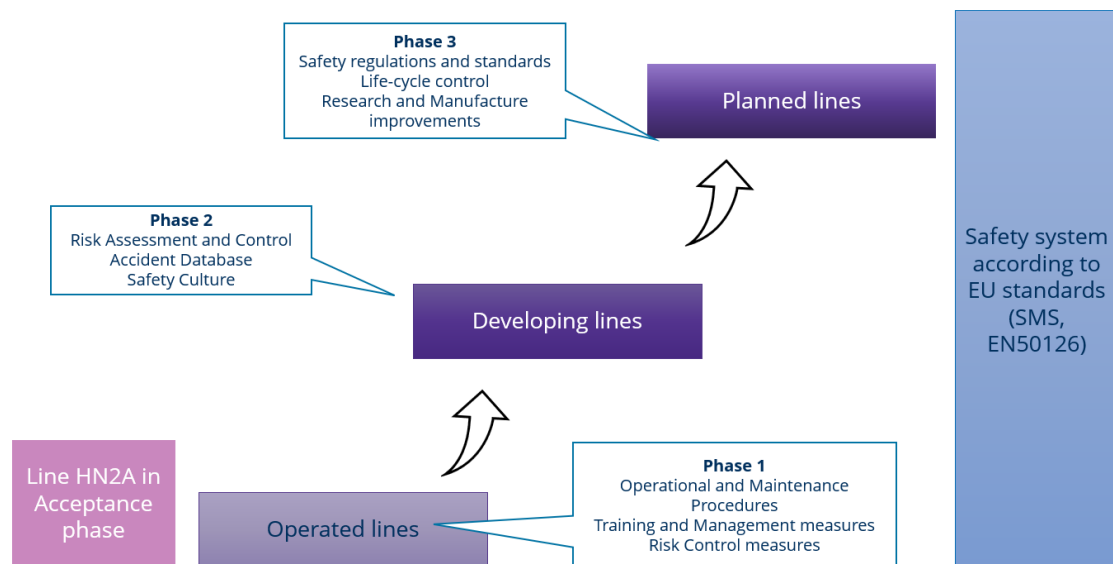
**Firstly**, these faults and hazards have developed during the manufacturing and execution of the project; it is impossible to go back in time to correct them, and it is also impossible to ignore the project without assuming responsibility for its management. At the time of completion, the HN2A metro line will have required an expenditure of up to \$868 million, thus it is vital to create measures to prevent system failure and assure passenger safety. The measures provided are

- Errors of door indicator lights and emergency exit buttons: Adjust control software, check safety acceptance.
- Errors of ventilation system: Due to the overhead route, both the chance and the risk are extremely low. Typically, this ventilation system failure is reported for subway lines under tunnels. When a train passes through a fire, the driver can still turn off the air conditioner, although he may forget due to panic, especially if the train loses power and must stop at the location of the fire. Therefore, Hanoi Metro Company should supply one additional safety employee per train to manage safety-related train operation issues.
- Automatic fire alarm system: Cost- and time-wise, the further installation of automatic fire alarms or surveillance cameras is not viable. However, it is possible to attach additional portable fire extinguishers in the passenger seats. The addition of a safety employee also helps to ensure safety in this case. In addition, it is necessary

to strengthen the implementation of accident treatment scenarios and clarify the passenger rescue process.

- Passenger information in station: Install more signboards for passengers, install tactile for disable, sign Mind the gaps and the other communication equipments in the station.
- Trackside signal problems: Trackside signals are only employed in the event of manual train driving (when there is a problem), while the system operates properly in CBTC automatic mode; hence, the failure of a signal along the route does not significantly impact system safety. The out-of-sight trackside signals have been solved by the solution of limiting the speed through the curve (reduced by 2 km/h compared to the original) and installing additional warning signs to increase the driver's attention.

**Secondly**, the capacity and experience of metro line project management are still very limited, so contracts are insufficient and missing system specifications and requirements. This results in discrepancies and errors throughout the design verification, approval, and product acceptance phases of later project phases.



**Figure 17** Outline of Safety Management System implementing process in Vietnam Metro projects

The operational phase of the Metro Line HN2A project must include the consideration of issues pertaining to risk assessment and the SMS plan. On this basis, establishing a standard framework and a system safety management methodology for future metro construction and planning projects.

As a system safety consultant, the author contributed to the writing of the Safety Management System plan for Hanoi Metro Company in order to achieve this objective. The subsequent chapters of the dissertation provide the results of the risk assessment and the suggested metro system inspection and maintenance methods. In addition, as previously discussed, the technical and production faults of the HN2A line cannot be remanufactured or modified, thus the present concentration are on the management process and enhancing human performance. Consequently assuring the monitoring of personnel for the technological systems, good technical condition and high operation efficiency, and the competence of personnel to respond to incidents.

ATC Consultants validated the safety of the following risk assessments, engineering management, and accident response processes in Chapters 4, 5, 6, and 7 during the finalisation of the Safety Certificate, and Hanoi Metro Company is now applying them in commercial operation.

Figure 19 clarifies the third step of enhancing the safety of Metro Line HN2A's system from its current level to that of a European-standard railway system:

- Phase 1: applicable for lines that are currently in operation, such as Metro Line HN2A. Focused on operational and maintenance procedures, as well as a training plan for railway personnel, in order to enhance human performance. Complete and update the risk assessment framework for Metro Line HN2A. The dissertation's findings are described in these applications.
- Phase 2: applicable for lines that are currently in construction and manufacturing, such as Metro Line HN3, Line HN2, HCMC Line 1 and Line 2. Continue refining and enhancing engineering management methods introduced during Phase 1. On the basis of the risk assessment by manufacturers (Line HN3, HCMC Line 2 with European manufacturers) and the risk assessment framework described in Chapter 4, a risk management plan for each line will be developed. Building Accident database for risk assessment research and development.
- Phase 3: applicable for lines that are currently in planning. Enhance safety requirements and life-cycle management. Building a proactive Safety Culture step by step for the railway industry. This material is implemented gradually throughout all three phases, beginning with the creation of the concept and concluding with an improvement in the attitude of railway personnel on the HN2A line.

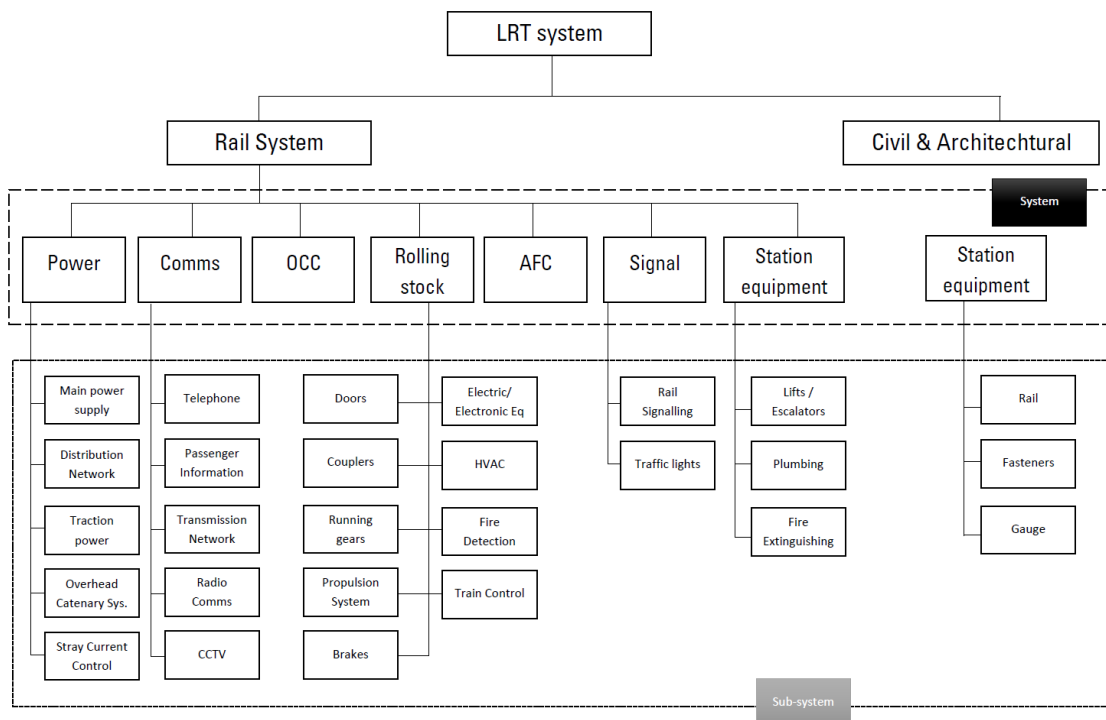
Solutions for phase 2 and phase 3 are introduced in Chapter 8 and Chapter 9 - Solutions for long-term developments.

## 4. SAFETY SOLUTIONS FOR OPERATED LINE – RISK ASSESSMENT

### 4.1 Purpose and scope of Risk assessment in HanoiMetro

This procedure has been established to standardise risk identification methods and procedures, from which a systematic and complete risk assessment can be established. These assessments are the scientific basis for determining risk control measures during urban railway operation of Hanoi Metro Company.

The urban railway project's activities are defined and categorised using a System Breakdown Structure (SBS). The project has been arranged in a tree structure to allow for execution phases and well defined work packages to avoid overlaps, ambiguities, and redundancies (Reales, 2014).



**Figure 18** System Breakdown Structure (Reales, 2014).

Based on the analysis of the advantages and disadvantages and the scope of application of risk assessment methods in Chapter 2: Literature review, the procedure recommends using three risk analysis methods appropriate for each management level and project phase.

- The Preliminary Hazard Analysis (PHA): It is a deductive risk analysis. The purpose is to identify, characterize and classify the risks. The hazards are identified, and each identified Hazard is assessed by combining its possible consequences for persons (hazard severity) and the occurrence of the situation (hazard frequency). The PHA identifies mitigations (provisions) to be implemented to gain an acceptable risk level.

The PHA is used for top-level management or at the beginning phase of projects to overview hazard and risk mitigation, logical thinking of risk identification.

- The Fault Tree Analysis (FTA) is based on top-down logic, starting from the hazard, called the Top Event, and looking downwards at all possible combinations of causes of that hazard. The FTA is established in technical management process. This technique is well-suited for assessing complicated systems with numerous components and variable hazard occurrences under various operating situations. This technology enables the creation of an open database for the study and update of discrete components.
- Bayesian networks facilitate the presentation of causal linkages and allow for probabilistic inference among a set of variables. The methodology is used to assess dangers resulting from interactions between technical systems and human factors. This analysis is used in analysing specific hazard scenarios to assess the impact of each factor in the probability of occurrence, thereby proposing appropriate risk control measures.

The results of the PHA analysis will be used as inputs to the FTA in order to evaluate situations that have the potential to cause significant harm and thereby disrupt the company's operations such as derailment, train collisions, collisions to people or objects, fire and explosion, etc. Bayesian network (BN) analysis is continuously researched and developed during the operation of the metro line to improve and enhance the accuracy of the FTA evaluation results. In the scope of this procedure, BN is presented general method and example of building a BN.

The greatly highlights that up to the current date, the Hanoi Metro line HN2A is the first and only urban rail line in Vietnam. It has been put into revenue service since November 2021 with an operational safety assessment launched for the first time, and long-term remains for the whole life cycle. Meanwhile, all the national main lines with narrow gauge 1000mm are too old and outdated in terms of infrastructure and technical standards that need to be renovated. Additionally, all of them have not been evaluated for safety and properly complied with any standardised method. As the fact-findings up to our best knowledge, this is the first report of the chosen safety assessment method for the Line HN2A, and testing this method with actual data that the author and Hanoi Metro Company have collected during the test & commissioning to the date of this article. The evaluation results published in the dissertation show that up to now, this first completely new safety assessment method is properly applicable for Line 2A. The research is still continuing to observe up-to-date operational data to perform hazards updates and evaluations of Line HN2A. These findings significantly highlight a straightforward method for safety assessment suitable and started to be applied for the first time in Vietnam, approved through application to the Line HN2A, despite that these methods are being applied commonly in some developed railways countries. To conclude, there are basic calculations, are easily applicable, and could be standardised for technical management of other railway lines in Vietnam.

## **4.2 The Preliminary Hazard Analysis of metro operation**

### **4.2.1 General method requirements**

This analysis is performed in two major steps:

- Identification of the hazardous situations applicable to the metro line HN2A: Hadong Station – Cat Linh.
- Analysis of these hazards and preliminary identification of the mitigation measures resulting in a set of PHA tables provided for each high level risk in Appendix 2.



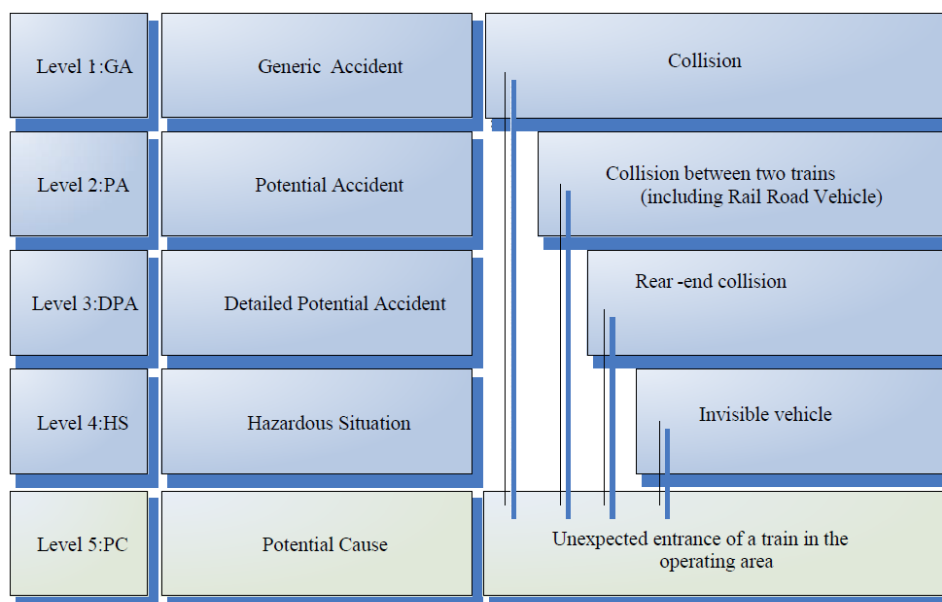
A top-down approach is applied for the hazard identification step. Its result is a hazard breakdown structure or hazard identification table as presented in the following sections. Each hazard is then analysed through an ‘hazard analysis like’ format in order to identify a first set of mitigation measures.

Requirements for risk analysis by the PHA method:

- Technical design and Feasibility report of Metro Line HN2A for civil work
- Requirements and Technical design for rolling stock, signal system, ATC functions, AFC system, maintenance guidelines, etc.
- Safety Management System reports, part of Potential risk controls.
- Operating plan and schedule of Metro Line HN2A.
- Related standards to railway system equipment which clarified in Chapter 3.
- Fire and Explosion Safety regulation in Vietnam.
- Risk analysis of Metro line 3: Nhon – Hanoi Station by Systra and Alstom.

#### 4.2.2 Identification of hazards

The identification of hazards is done in a deductive way. The purpose is to build up a breakdown of the hazards starting from generic accidents and getting into more detailed situations. This breakdown is performed on 4 different levels of depth. These 4 levels are deemed sufficient to be able to identify adequately detailed scenarios in front of which elementary causes can be identified. A five-level is used to describe the main potential causes inducing each scenario. The Figure 21 below illustrates this approach.



**Figure 19** Identification of the breakdown of hazards

There are 5 generic accident listed here below are identified: (i) Collision including Train collisions and Train to people / objects collisions; (ii) Derailment / Overturn; (iii) Gas emission – Toxic smoke – Air ventilation; (iv) Falls – inside a vehicle and from the train on to the track; (v) Fire and Explosion.

### 4.2.3 Hazard analysis and mitigation measures identification

Hazard identification is the combination of a top-down and a bottom-up process to provide higher confidence in its completeness:

- The top-down process is initiated by the System Preliminary Hazard Analysis and the Safety Analysis in manufacture company in the phase of project developing. The Safety Department is responsible to establish and review the System Preliminary Hazard Analysis of HanoiMetro in operation.
- The bottom-up process is developed by Maintenance Centres to analyse every potential failure for their equipment and evaluate their consequence on the regular operation. These suggestions are reported to Manager Responsible for Vehicle and Equipment for approval and submitted to the Safety Department for archives. The Dispatching Centre might participate in this process to analysis the operating conditons in necessary situations.

The functional and hardware requirements for the subsystems will be utilised as inputs for all safety assessments and processes, including top-down and bottom-up. Each detected hazard will be evaluated in terms of its potential consequences and the likelihood of the scenario occurring. The assessment may be based on logic, expert judgement, or historical evidence. The table 4.1 in the following defines the risk classification system based on severity and frequency of Metron Line HN2A.

The severity of hazards is classified into 6 levels from minor to castatrophic damage compliance to the procedures in incident management in Chapter 7. The estimation of the likelihood of occurrence of a hazard will be estimated on the basis of expert judgement, on field data from similar applications or failure data provided by international standards. Where relevant, the occurrence of a hazard will also take into account the occurrence of external events (triggers) when those ones largely contribute to the likelihood of the related potential accident.

The Preliminary Hazard Analysis of Metro Line HN2A is provided in Appendix 2.

### 4.2.4 Risk resolution measures

The objective is to define and specify the safety provisions (or mitigation measures or safety requirements) to be implemented to mitigate the risks in order to reach an acceptable level (i.e. such that the risk acceptance criteria is fulfilled). A safety provision is an item that is characterized with safety requirements. An item can be a function performed by a product, an operating procedure or process or a maintenance procedure or process.

The order of precedence for resolving identified risks is: (i) Hazard elimination (by design); (ii) Risk reduction (by reducing either the hazard severity or frequency of occurrence); (iii) Implementation of operation procedures.

As a result a safety provision can be of one of the following type: (i) Application of a safe design criteria; (ii) Definition of a protection function; (iii) Compliance with relevant rules and standard; (iv) Operation and Maintenance rules and procedures.

Prior to revenue service it is necessary to provide the assurance that these provisions are either effectively implemented in the design or adequately considered by operation and maintenance. Once in revenue service, the operator and maintainer will perform the necessary activities to maintain the level of safety provided by these provisions. The Hazard Logs are completed with the description of the safety provisions.

**Table 4.1** Risk classification based on severity and frequency of Metro Line 2A

|           |                    |                             | Severity                                     |                |                   |                |                    |                        |
|-----------|--------------------|-----------------------------|--|----------------|-------------------|----------------|--------------------|------------------------|
|           |                    |                             | 6  | 5              | 4                 | 3              | 2                  | 1                      |
|           |                    |                             | Minor  | Insignificant  | Normal            | Critical       | Extremely Critical | Castatrophic           |
|           | Safety for people  | Deaths                      | ---  | ---            | ---               | 1-3            | 3 -10              | From 10 deaths         |
|           |                    | Major injuries              | ---  | ---            | 1                 | 2-3            | 10 – 20            | Over 20 injuries       |
|           |                    | Minor injuries              | ---  | 1-5            | 5-10              | 10-20          | 20-50              | Over 50 minor injuries |
|           | Property damage    | Direct loss to economy      | ---  | ---            | 500 mil. – 1 bil. | 1-3 bil.VND    | 3 – 10 bil.VND     | over 10 bil. VND       |
|           | Operational safety | Interruption of network     | ---  | ---            | <15 min           | 30min – 1 hour | 1 hour – 1 day     | 1 day – 1 weeks        |
|           |                    | Interruption of single line | ---  | 15-30 min      | 30 min – 1 day    | 1 hour – 1 day | 1 day – 1 week     | Over 1 weeks           |
|           |                    | Interruption of station     | 15-30 min                                    | 1 hour – 1 day | Under 1 week      | 1 week         | 1 month            | ---                    |
|           |                    | Train delayed               | <15 min                                      | ---            | ---               | ---            | ---                | ---                    |
| Frequency | A                  | Frequent                    | $\lambda \geq 10^{-5}/\text{hour}$           | R3             | R2                | R1             | R1                 | R1                     |
|           | B                  | Probable                    | $10^{-6} > \lambda \geq 10^{-5}/\text{hour}$ | R3             | R3                | R2             | R2                 | R1                     |
|           | C                  | Occasional                  | $10^{-7} > \lambda \geq 10^{-6}/\text{hour}$ | R4             | R3                | R3             | R2                 | R2                     |
|           | D                  | Remote                      | $10^{-8} > \lambda \geq 10^{-7}/\text{hour}$ | R4             | R4                | R3             | R3                 | R2                     |
|           | E                  | Improbable                  | $10^{-9} > \lambda \geq 10^{-8}/\text{hour}$ | R4             | R4                | R4             | R3                 | R3                     |
|           | F                  | Incredible                  | $\lambda < 10^{-9}/\text{hour}$              | R4             | R4                | R4             | R4                 | R3                     |

## **4.3 The Fault Tree Analysis of Metro Line HN2A**

### **4.3.1 Overview of Fault Tree Analysis method**

Fault Tree Analysis (FTA) is a top-down deductive analysis to translate a physical system into a logical diagram. A fault tree analysis may be qualitative, quantitative, or both, depending on the scope of the analysis (Galante et al. 2014; Rausand et al. 2020). The main objectives of a fault tree analysis are: (a) To identify all possible combinations of basic events that may result in a critical event in the system; (b) To find the probability that the critical event will occur during a specified time interval or at a specified time  $t$ , or the frequency of the critical event; (c) To identify aspects of the system that need to be improved to reduce the probability of the critical event. All the events in a fault tree are connected by logic gates (Haimes 2009; Rausand et al. 2020). Logic gates represent the logical relationship between output and input events. In a particular analysis of a system, these logic gates explain how failures of component or subsystem combine and lead to an unexpected consequence. According to (IEC 2006), five main logic gates in FTA are: AND gate - The output event only occurs if all input events occur; OR gate - The output event occurs if any input events occur; PRIORITY AND gate - The output event only occurs if all the input events occur in a specified sequence, which is usually from left to right; EXCLUSIVE OR gate - The output event only occurs if exactly one input events occur, while any other input event does not occur; INHIBIT gate - The output event occurs if one input event occurs and the condition allows at the same time.

Besides using Fault Tree Analysis, risk analysts often use a combination of FTA and Event Tree Analysis as a stand-alone or supporting tool to complete FTA analysis. Event tree analysis is a probabilistic and graphical approach to modelling and analysing accident situations (Rausand et al. 2020). The technique is inductive and logical methods with a tree-like graphical representation of sequential events. The generated figure depicts several accident scenarios (i.e., event sequences) that might occur in the aftermath of a specified hazardous event. The event tree illustrates the system's/response plant's to the dangerous occurrence. External events that have an effect on the accident scenario may be included in the event tree as well (Hong E.-S 2009; Ayyub 2003) .

### **4.3.2 Method and procedure of a Fault Tree Analysis**

#### **Step 01. Overview and operational assessment of UMRT Line HN2A**

The research provides an overview of the UMRT Line HN2A and its fundamental technical features based on its technical design and operational environment circumstances. Introduction to the infrastructure, the subsystems that comprise the system, most notably the signal and control system. From there, undertake a risk analysis on a severe hazard in the railway operation.

According to railway accident classification of EU, railway accident is classified into 6 types such as Collisions of Train, Derailments, Level crossing accidents, Accident to persons, Fires

in rolling stocks and Other accidents. (ERA, 2020, Evans 2011b; Evans 2021). Japan railway accident classification for tramway also included 6 types of accident which are Train collisions, Train Derailments, Level crossing accidents, Accident against road traffics and other accidents with casualties (JTSB, 2022). Such classification is also completely similar to the studies of International Union of Railway (UIC, 2021). In the UMRT line HN2A, based on the technical design and above international practice of classification, risks related to collision (including Train-to-Train Collisions and Collisions with an obstacle), derailment, and fire hazards are generic operation risks.

Based on the The Preliminary Hazard Analysis of Metro Line HN2A and the general knowledge of railway accident (which clarified in section 2.2.2, section 2.3.4 and Chapter 3 on actual conditions in Vietnam), the dissertation concentrated on 04 types of generic and significant accident such as Train Collisions, Train Derailment, and Incidents leading to people injured in urban railway operation. These types of accidents are similar in low frequency but serious severity and complex interactive failures. Therefore, it is necessary to analyse the root reasons leading to accidents. The other types of high frequency and low severity could be controlled by regulations and accident training.

As there have not been any accident reports in the early stages of operation of the Line HN2A, so the risk frequency estimates are inherited and referenced from technical design of the Line HN2A and similar European systems, and the accident data are published (which lists in section 2.2.2, section 2.3.4, and above paragraph).

**Step 02.** Establishing Fault Tree Analysis to assess the basic error and failure frequency leading to main accidents.

The reason of a accident is classified into several major categories of failure, each of which is further subdivided into particular sub-failures. Following that, the research uses the Fault Tree Analysis approach to determine the probability of each sub-failure and to compute the hazard rate for the hazard occurrence.

Fault tree with a single AND-gate: Let  $E_i(t)$  denote that the event  $E_i$  (human error or component failure) is occurring at time  $t$ ,  $i = 1, 2, \dots, n$ . Since the TOP event will occur if and only if all the basic events occur, the Boolean representation of the fault tree is

$$TOP(t) = E_1(t) \cap E_2(t) \cap \dots \cap E_n(t) \quad (4.1)$$

The probability that the event is occurring at time  $t$  is denoted  $Q_i(t) = \Pr(E_i(t))$ . Assumed that all of events  $E_i(t)$  are independent, the probability of TOP event at time  $t$ ,  $Q(t)$ , is expressed

$$\begin{aligned} Q(t) &= \Pr(E_1(t) \cap E_2(t) \cap \dots \cap E_n(t)) = \Pr(E_1(t)) \cap \Pr(E_2(t)) \cap \dots \cap \Pr(E_n(t)) \\ Q(t) &= q_1(t) \cdot q_2(t) \dots q_n(t) = \prod_{i=1}^n q_i(t) \end{aligned} \quad (4.2)$$

Fault tree with a single OR-gate: In the case of Fault tree with a single OR-gate, any of the basic events will cause the TOP event to occur, and the Boolean representation is

$$TOP(t) = E_1(t) \cup E_2(t) \cup \dots \cup E_n(t) \quad (4.3)$$

Assumed that all of events  $E_i(t)$  are independent, the probability of TOP event at time  $t$ ,  $Q(t)$ , is expressed

$$\begin{aligned} Q(t) &= \Pr(E_1(t) \cup E_2(t) \cup \dots \cup E_n(t)) = 1 - \Pr(\bar{E}_1(t) \cap \bar{E}_2(t) \cap \dots \cap \bar{E}_n(t)) \\ Q(t) &= 1 - (1 - q_1(t)) \cdot (1 - q_2(t)) \dots (1 - q_n(t)) = 1 - \prod_{i=1}^n (1 - q_i(t)) \end{aligned} \quad (4.4)$$

Any fault tree diagram can be represented as an alternative fault tree diagram with a single OR-gate with all the minimal cut set failures as input events, therefore, the probability  $Q_0(t)$  of the top event at time  $t$ , is expressed

$$Q_0(t) = Pr (C_1(t) \cup C_2(t) \cup \dots \cup C_k(t)) \quad (4.5)$$

In which,  $C_j(t)$  is the probability that minimal cut set  $j$  is failed at time  $t$ , for  $j = 1, \dots, k$ . Minimal cut set  $j$  will fail at time  $t$  when all the basic events  $E_{j,i}(t)$  in  $C_j$  occur at time  $t$ . The minimal cut set failure,  $C_i(t)$ , can therefore be represented as a fault tree with a single AND-gate. Using  $m$  to denote the number of basic events in minimal cut set  $C_j$ , the probability that minimal cut set  $C_j$  fail at time  $t$  can be expressed

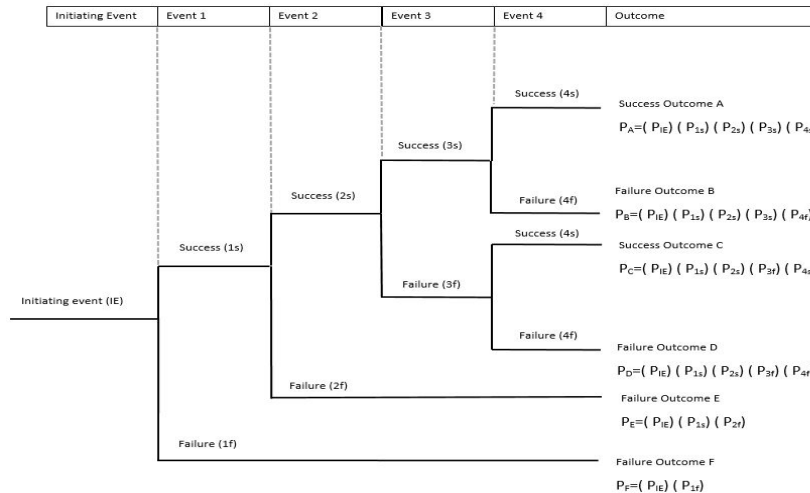
$$Pr (C_j(t) = Pr (E_{j,1}(t) \cap E_{j,2}(t) \cap \dots \cap E_{j,m}(t)) \quad (4.6)$$

$$\text{We get } Q_0(t) = \sum_{j=1}^k Pr (C_j(t)) - \sum_{i < j} Pr (C_i(t) \cap C_j(t)) + \sum_{i < j < l} Pr (C_i(t) \cap C_j(t) \cap C_l(t)) - \dots + (-1)^{k+1} \cdot Pr (C_1(t) \cap C_2(t) \cap \dots \cap C_n(t)) \quad (4.7)$$

In this part, the research examines three scenarios in which hazards are dangerous and incur damage ranging from critical to catastrophic: train collisions, train derailments, and collisions with people/external objects on the track. These hazard situations typically share the same characteristics of a complex, concurrent influence of numerous components during operation. For instance, danger can exist only when a breakdown in the ATC system happens concurrently with a failure in the driver's evaluation and a trigger event indicating the presence of people on track. Additionally, the analysis identified several risk scenarios that could interrupt the metro line, including power supplies, signalling, monitoring, communication system failures, and fire and explosion events.

The FTA analysis identifies possible subsystem failures and components with a high chance of occurrence of a critical incident event, allowing for rational engineering management solutions such as inspection and maintenance, which are discussed in Chapter 5 and Chapter 6. The scope of this dissertation does not include detailed and particular examinations of mechanical, electrical, and electronic operations. These issues should be investigated in specialised device studies and updated in the company's opened system database on the basis of this FTA research.

### Step 03. Validating the theoretical results



**Figure 20** Theoretical calculation of Event Tree Analysis

The research compares theoretical calculations to error data collected during the Test and Commissioning of UMRT Line HN2A in order to determine if the theoretical calculations are congruent with reality. Sub-failures that deviate significantly from reality and theory must be explicated and studied for causes. Event Tree Analysis is utilised in this stage to determine

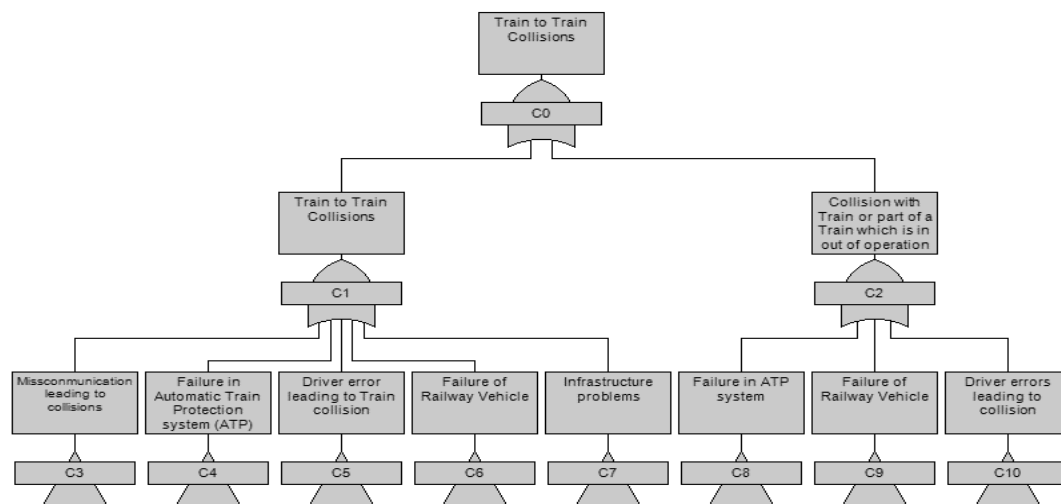
the probability of Train Collisions based on the error rate of the sub-failure documented in the operation report.

The primary goals of an event tree analysis are to: (a) Identify potential accident scenarios that might occur in the aftermath of a hazardous occurrence; (b) Identify the obstacles that are now in place (or that are intended to be in place) to prevent or reduce the adverse impacts of the accident scenarios; (c) Evaluate the barriers' applicability and reliability in relevant accident situations; (d) Identify internal and external occurrences that may have an effect on the scenario's event sequences—or their implications; (e) Calculate the likelihood of each accident scenario; (f) Identify and evaluate the potential effects of each accident scenario. The probability of success or failure scenarios from initiating event is describes as in the Figure 22.

Due to the fact that the contents of Chapters 4 to 7 are implemented as the Hanoi Metro Company's Safety Management Plan, this chapter will principally construct the urban railway operation's fault tree and evaluate the probability of hazard. Chapter 8 Discussion and Conclusion will include validation of these calculations as a recommendation on data accuracy.

### 4.3.3 Risk analysis for Train-to-train Collisions hazards

The Train Collisions are usually separated into 02 incident groups: Train to Train Collisions and Train collided with train/or a part of Train which is out of operation. Train-to-Train Collisions might have resulted from C3-Miscommunication, C4-Failure in Automatic Train Protection system (ATP), C5-Driver error, C6-Failure of Railway Vehicle or C7-Infrastructure problems. Collision with Train or a part of Train that is out of operation might have resulted from C8-Failure in ATP system, C9-Failure of Railway Vehicle or C10- Driver errors.

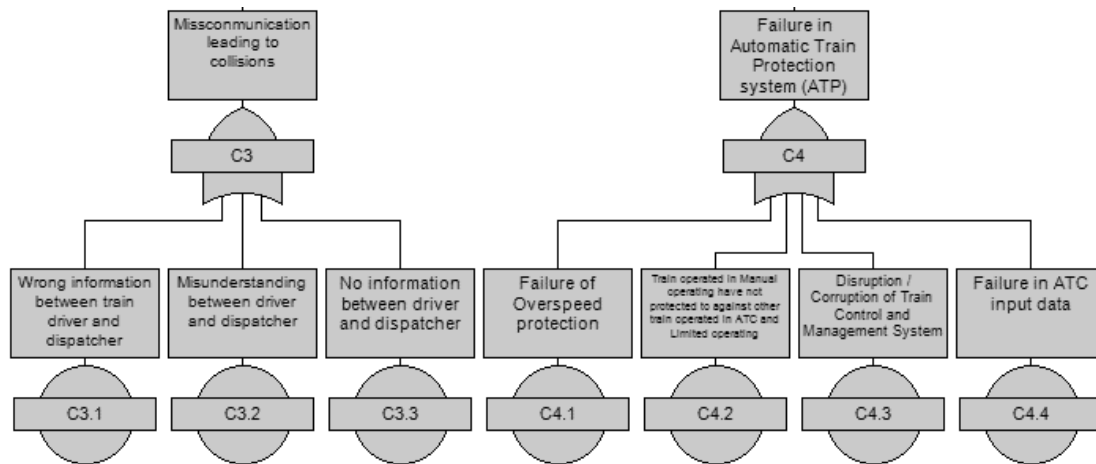


**Figure 21** Fault Tree Analysis of Train Collisions

#### ***Miscommunication and Failure of ATP system***

Using modern monitoring and controlling systems, railway operators in Operation Control Centre (OCC) can remotely control a large area and complex system. Existing signalling systems give us all the information (status) about the signalling elements (points, signals, routes, level crossings, etc.) and ensure that all train movements are

coordinated and comply with timetable-based dis-patching. The subfailure and hazard rate are collected and calculated from (BUEDRI 2012; BUEDRI 2015).



**Figure 22** FTA of Top Events Misscommunication and Failure in ATP

**Table 4.2** Probability of Top Events Misscommunication and Failure in ATP

| No        | Top Event  | Sub-failure | Hazard rates<br>(10 <sup>5</sup> km-op-<br>eration) |
|-----------|--|-------------|---|
| <i>C3</i> | <i>Misscommunication leading to collisions</i>   |             | <i>2.92E-03</i>                                     |
| C3.1      | Wrong information between train driver and dispatcher  |             | 1.38E-03  |
| C3.2      | Misunderstanding between driver and dispatcher   |             | 1.04E-03  |
| C3.3      | No information between driver and dispatcher   |             | 5.00E-04  |
| <i>C4</i> | <i>Failure in Automatic Train Protection system (ATP)</i>  |             | <i>6.48E-05</i>                                     |
| C4.1      | Train operated in Manual operating method and have not protected to against other train operated in ATC and Limited operating method |             | 3.19E-05  |
| C4.2      | Disruption / Corruption of Train Control and Management System   |             | 1.02E-06  |
| C4.3      | Failure in ATC input data  |             | 3.19E-05  |

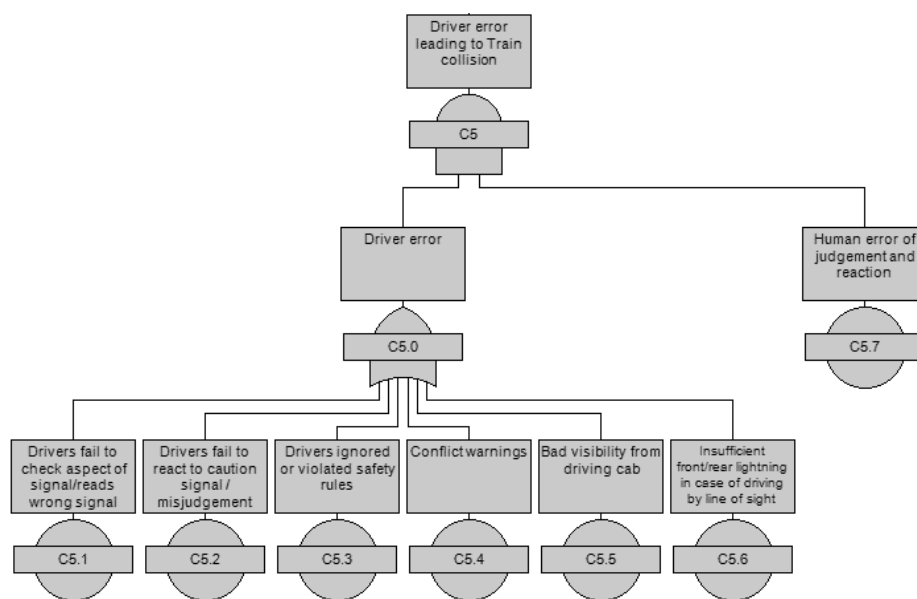
Besides, thanks to modern safety communication systems, other responsibilities include operating passenger information systems, monitoring the catenary system, and controlling alarm systems, which are a significant portion of the operator's workload. According to (BEU 2020; Lin et al. 2012), the following are the most common types of operator and Automatic Train Protection system (ATP) errors:

- Human errors comprise the following types of errors: (i) diagnostic and decision-making errors, which are caused by a misunderstanding by the operators, (ii) errors of commission, which occur when an operator performs an action that is both erroneous and unrequired by the system; (iii) misunderstanding between the operator and the driver as a result of the omission of critical information
- ATP technological failures include: (i) problems in software programming or processing; (ii) Failure or corruption of the Train Control and Management System; (iii) Disconnection or failure of the data input.

### **Driver's errors**



Driver error and faulty action are frequently combined in a railway accident, leading to the driver's failure to prevent the accident. In an accident, the driver's concentration and assessment are compromised, resulting in judgement errors of approximately 2% to 6% (Dingus et al. 2016). Based on the support of modern technology in railway controlling and monitoring, our calculation assumed this error is around 2.5%. A fatigue problem, attention, violation of regulations, or environmental conditions could all be factors that contribute to the errors in judgement. The error actions of the driver might be (i) failing to check aspect of signals, (ii) errors in reaction to caution signal, (iii) ignored or violating the safety rules or (iv) insufficient information from ATC, signal light. The violating rules in the Vietnam railway industry is a significant problem, as in the safety perception survey (Luong, 2020), with a high proportion of answers in the influence of alcohol or illicit drugs compromising rail safety or using entertainment form in duty.



**Figure 23** FTA of Top Events: Driver errors leading to Collisions

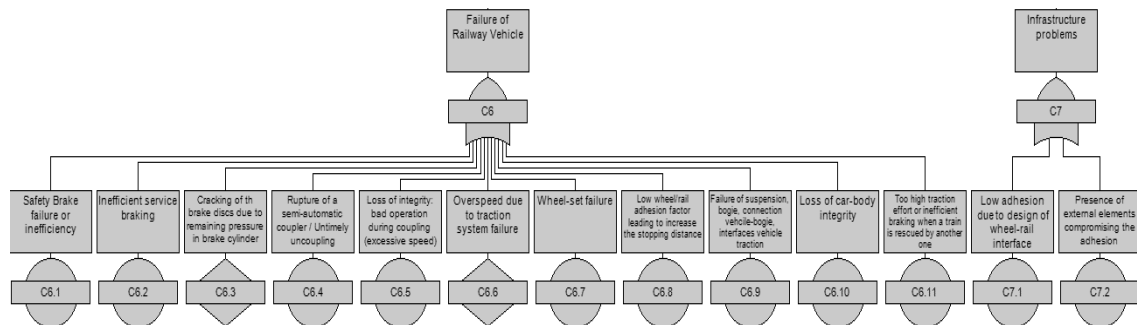
**Table 4.3** Probability of Top Events: Driver errors leading to Collisions

| No   | Top Event                               | Sub-failure   | Hazard rates<br>(10 <sup>5</sup> km-operation) |
|------|---|---|--|
| C5   | Driver error leading to Train collision |   | 5.12E-03                                       |
| C5.0 | Driver errors                           |   | 2.56E-01                                       |
| C5.1 |   | Drivers fail to check aspect of signal/reads wrong signal     | 3.75E-02                                       |
| C5.2 |   | Drivers fail to react to caution signal / misjudgement        | 3.75E-02                                       |
| C5.3 |   | Drivers ignored or violated safety rules                      | 5.00E-02                                       |
| C5.4 |   | Conflict warnings   | 5.00E-02                                       |
| C5.5 |   | Bad visibility from driving cab                               | 6.75E-02                                       |
| C5.6 |   | Insufficient front/rear lightning in driving by line of sight | 1.35E-02                                       |
| C5.7 | Human error of Judgement /reaction      |   | 2.00E-02                                       |

### Failure of Vehicle and Infrastructure

The category of technical equipment factors contains potential failures on the rolling stock or on technical facilities. Rolling stock failures mainly include:

- Locomotive: running gear failure, traction motor failure, crank case, oil or fuel fire, electrically caused fire, third rail/pantograph defect, onboard computer failure to respond;
- Bogie: broken bogie frame, defect on suspension (primary or secondary), failure of the damper;



**Figure 24** FTA Top Events: Failure of Vehicle and Failure of Infrastructure

- Wheels: broken or damaged flange, broken wheel plate, broken or loose wheel rim, thermal crack;
- Coupler: broken knuckle, coupler mismatched, broken coupler carrier or shrank, failure of articulated connectors;
- Axle set: broken or defective wheel shaft, roller bearing defect, hot box;
- Vehicle body: broken or defective bolster, broken or defective traction beam, broken or defective centre plate, broken draft or centre sill, loss of integrity;
- Brake system: detrition of brake shoe, broken or defective brake disc, blockage of brake line, uncoupled air or hydraulic hose, obstructed brake pipe (Wang 2014);
- Improper structure design of rolling stock (VR 2021; BUEDRI 2012 - BUEDRI 2015; Wang 2014).

**Table 4.4** Probability of Failure of Vehicle and Failure of Infrastructure

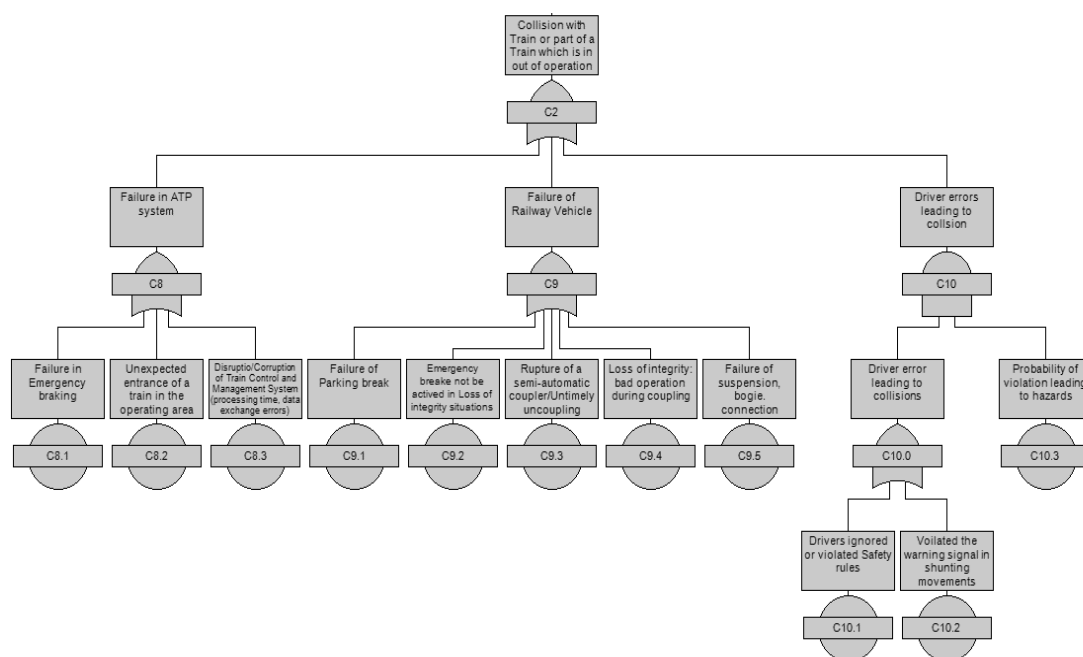
| No   | Top Event                         | Sub-failure  | Hazard rates<br>(10 <sup>5</sup> km-operation) |
|------|-----------------------------------|--|--|
| C6   | <i>Failure of Railway Vehicle</i> |  | <i>4.49E-03</i>                                |
| C6.1 |                                   | Safety Brake failure or inefficiency   | 1.32E-04                                       |
| C6.2 |                                   | Inefficient service braking  | 1.32E-04                                       |
| C6.3 |                                   | Deterioration / Cracking of the brake discs due to a parking brake remaining applied or remaining pressure in brake cylinder | 6.08E-04                                       |
| C6.4 |                                   | Rupture of a semi-automatic coupler / Untimely uncoupling  | 3.02E-04                                       |
| C6.5 |                                   | Loss of integrity: bad operated during coupling (excessive speed)  | 5.08E-04                                       |
| C6.6 |                                   | Overspeed due to traction system failure   | 2.43E-04                                       |
| C6.7 |                                   | Wheel-set failure  | 6.08E-04                                       |

|           |  |                 |
|-----------|--|-----------------|
| C6.8      | Low wheel/rail adhesion factor leading to increase the stopping distance (weather condition included)                    | 3.04E-04        |
| C6.9      | Failure of suspension, bogie, connection vehicle-bogie, gauge dynamics, not respected gauge, interfaces vehicle traction | 9.13E-04        |
| C6.10     | Loss of car-body integrity   | 6.08E-04        |
| C6.11     | Too high traction effort or inefficient braking when a train is rescued by another one                                   | 1.32E-04        |
| <b>C7</b> | <b>Infrastructure problems</b>   | <b>1.04E-03</b> |
| C7.1      | Adhesion problem: design of the wheel-rail interface not taking into account   | 3.02E-04        |
| C7.2      | Adhesion problem: presence of external elements compromising the adhesion  | 7.39E-04        |

As a result of the problem with the railway infrastructure in collision accidents, adhesion has been diminished. Hence, the ability to stop trains has been inhibited, potentially resulting in SPADs, station platform overruns, and crashes. Furthermore, it has the potential to cause damage to rails, requiring regrounding and premature replacement, as well as failure to activate track circuits, which might have possibly serious implications.

### Analysis of Collisions with Train or part of Train which out of operation

**Figure 25** FTA Top Events Train collision with inactivated/or a part of train



| No        | Top Event  | Sub-failure | Hazard rates<br>(10 <sup>5</sup> km-operation) |
|-----------|--|-------------|--|
| <b>C8</b> | <b>Failure in ATP system</b>                                   |             | <b>4.35E-04</b>                                |
| C8.1      | Failure in Emergency braking                                   |             | 4.35E-04                                       |
| C8.2      | Unexpected entrance of a train in the operating area           |             | 1.32E-04                                       |
| C8.3      | Disruption / Corruption of Train Control and Management System |             | 3.02E-04                                       |
| <b>C9</b> | <b>Failure of Railway Vehicle</b>                              |             | <b>1.95E-03</b>                                |
| C9.1      | Failure of Parking break                                       |             | 1.32E-04                                       |

|              |  |                 |
|--------------|--|-----------------|
| C9.2         | Emergency break not be activated in Loss of integrity situations | 9.50E-05        |
| C9.3         | Rupture of a semi-automatic coupler / Untimely uncoupling        | 3.02E-04        |
| C9.4         | Loss of integrity: bad operation during coupling                 | 5.08E-04        |
| C9.5         | Failure of suspension, bogie, connection                         | 9.13E-04        |
| <i>C10</i>   | <i>Driver error leading to collision</i>                         | <i>3.50E-03</i> |
| <i>C10.0</i> | <i>Driver error</i>  | <i>7.00E-02</i> |
| C10.1        | Driver ignored or violated Safety rules                          | 5.00E-02        |
| C10.2        | Violated the warning signal in shunting movements                | 2.00E-02        |
| <i>C10.3</i> | <i>Probability of violation leading to hazards</i>               | <i>5.00E-02</i> |

**Table 4.5** Probability of Train collision with inactivated/or a part of train

### **Calculation the Probability of Train Collisions for Line HN2A**

Based on the structure function of Train Collisions and theoretical formula (4.1) to (4.7), the quantitative assessment of Collisions failure can be calculated. The result would be in probability of incident per 100.000 km-operation or number of incident per year. The Probability of Train Collisions is calculated by the following Boolean algorithm

$$C0 = C1 \cup C2 = (C3 \cup C4 \cup C5 \cup C6 \cup C7) \cup (C8 \cup C9 \cup C10)$$

$$= (C3.1 \cup C3.2 \cup C3.3) \cup (C4.1 \cup C4.2 \cup C4.3 \cup C4.4) \cup [(C5.1 \cup C5.2 \cup C5.3 \cup C5.4 \cup C5.5 \cup C5.6) \cap C5.7] \cup (C6.1 \cup C6.2 \cup C6.3 \cup C6.4 \cup C6.5 \cup C6.6 \cup C6.7 \cup C6.8 \cup C6.9 \cup C6.10 \cup C6.11) \cup (C7.1 \cup C7.2) \cup (C8.1 \cup C8.2 \cup C8.3) \cup (C9.1 \cup C9.2 \cup C9.3 \cup C9.4 \cup C9.5) \cup [(C10.1 \cup C10.2) \cap C10.3]$$

$$= 1.95E-2 \text{ (accidents/100.000km-operation)}$$

Based on technical design and operational plan of the Line HN2A, the total length of this line is 13.02 km. The number of train operated per day in the first commercial operation phase (2021-2025) are 152 trains/days and in the second commercial operation phase (from 2026) are 252 train/days. Therefore, the probability of Train Collisions are:

From 2021-2025,  $C0 = 1.95E-2/100.000\text{km} * 13.02\text{km} * 152 \text{ trains/day} * 365 \text{ days} = 0.014 \text{ collisions/year}$

From 2025,  $C0 = 1.95E-2/100.000\text{km} * 13.02\text{km} * 272 \text{ trains/day} * 365 \text{ days} = 0.025 \text{ collisions/year}$ .

### **4.3.4 Risk analysis for Train derailments hazards**

Three high-priority antecedents are employed in this thesis as top-level intermediate events in the fault tree of derailment: derailments caused by Signal Passed at Danger (SPAD), signalling and dispatching errors, Wheel set and Track failure. This group of precursors is reported to be responsible for 85% of derailments in Germany and 62% of derailments in Japan, according to published investigative reports.

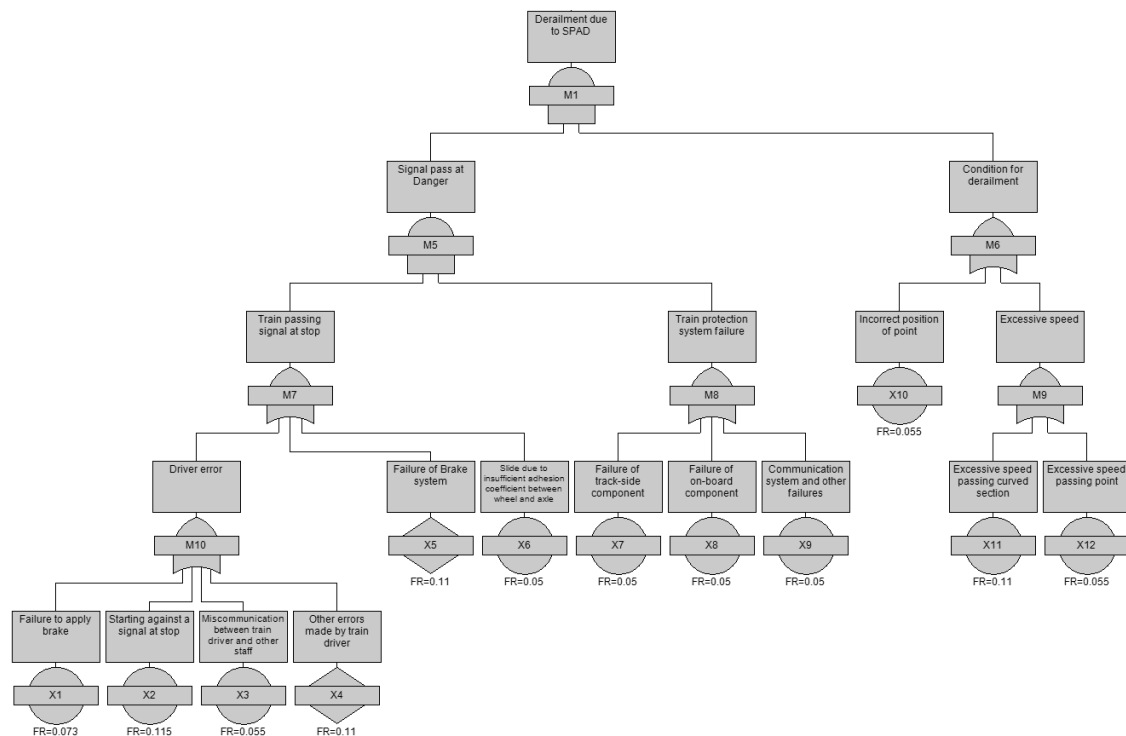
Due to the fact that urban railways operate at a relatively low speed (max. 80 km/h), the proportion of overspeed appears to be rather low, and it is typically associated with speed control device (SPAD) failure. However, train derailment is a complicated catastrophe that can occur for a variety of reasons owing to the interaction of several components, and the resulting damage will be catastrophic if it occurs.

As a result, the thesis established an FTA to investigate the reasons of derailments and to monitor the system's performance. Train derailment statistics are not often investigated in

detail for urban railways. Additionally, estimating data from main line railways is incompatible with the operation characteristics of urban railways. As a result, the thesis proposes to construct an FTA for Line HN2A and to continue monitoring for subfailures in order to ascertain the failure rate of Train Derailment in the first few years following commercial operation.

### **Signal pass at Danger (SPAD)**

Derailment due to SPAD can only occur if unsafe conditions leading to a derailment are met at the same time, such as incorrect position of a point. This event is the most common hazard for railway safety which could lead to a train derailment. The number of SPADs in Germany reported by BEU was 566 in 2019 (BEU, 2020) and only 3% resulted in accidents.



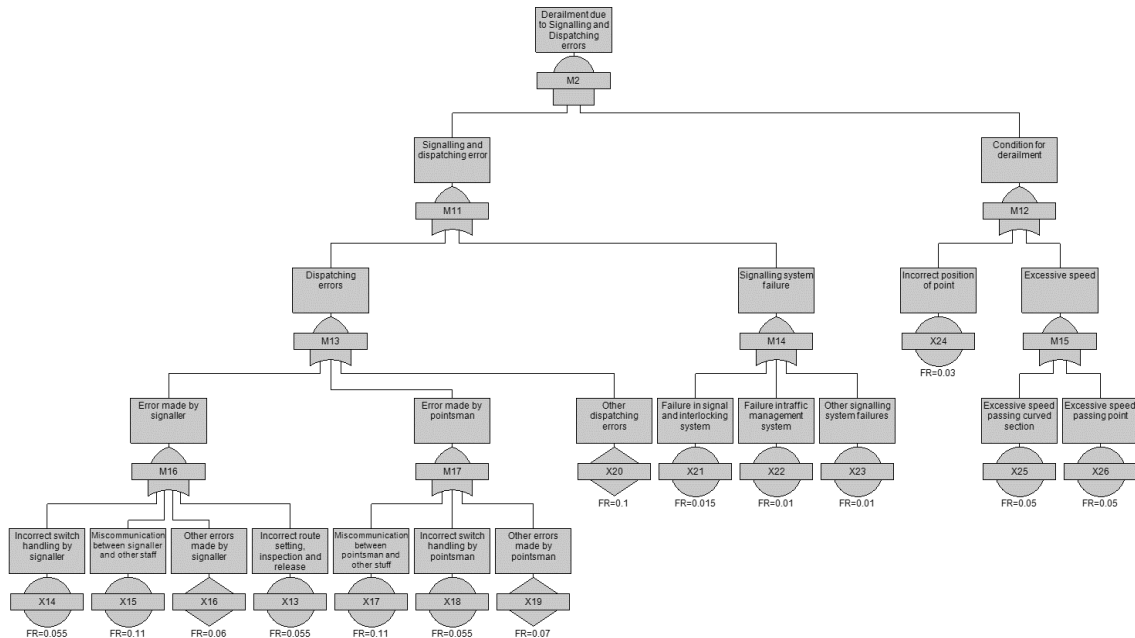
**Figure 26.** FTA of Top Event 1 – Derailment due to SPAD

For the train without train protection system, SPAD normally occurs as the result of train driver errors, where train driver may fail to observe red signal and react to red signal incorrectly, i.e. fail to apply the brake in time. Train driver may start the train against a signal at stop, causing SPAD in another situation. In addition, the existence of miscommunication between railway staff may also result in SPAD during shunting operation. Additionally, SPAD may also occur due to the failure of brake system or insufficient friction between wheel and track.

On the one hand, in order to prevent a train from passing a stop signal, A widely used type of train protection system is the inductive train protection device, where data is transmitted between trackside and on-board magnets. If a train passes a trackside magnet at a speed exceeding the braking curve, the emergency brake will be automatically applied unless the train driver presses intervention button. Similarly, Automatic Train Supervision (ATS) was developed in Japan to prevent the train from passing a red signal by using an in-cab alarm device as well as applying an emergency brake automatically.

### **Signalling and dispatching errors**

The most common causes are incorrect route setting and inspection and incorrect switch handling by signallers as well as incorrect switch handling by pointsmen. Similar to conditions of derailment listed in the case of SPAD, the derailment occurs if a train passes points or curves at an excessive speed or points in the improper position after a signalling or dispatching error has been made.



**Figure 27** FTA of Top Event 2 – Derailment by Signalling and Dispatching Errors

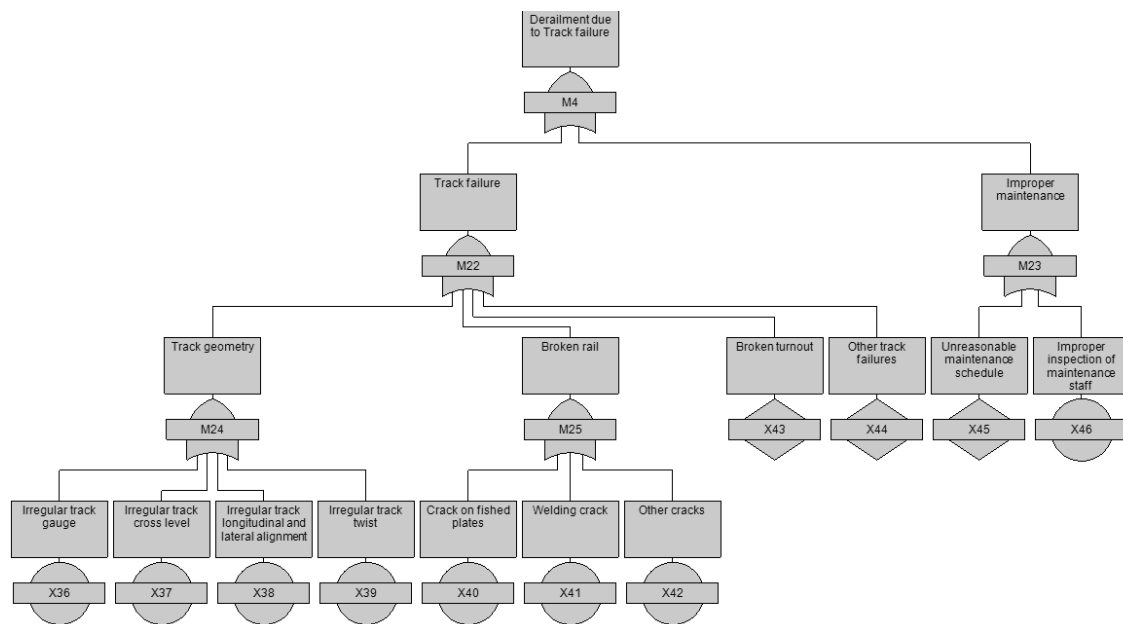
Interlocking routes can protect trains by clearing a lineside or cab signal and locking movable points when passing points. However, if the operator gives the train authority to enter the route where the point is not locked in the correct position or the point is damaged, or releases the route untimely, it is possible that the train derails when passing unsafe movable points. To reduce the risk of accidents caused by a signalling and dispatching error, mechanical, electro-mechanical and relay interlocking system are gradually replaced by computer-based system where railway signallers and pointsmen take less responsibilities for train dispatching and shunting operation.

### Track failure

Several common infrastructure factors are shown below:

- Roadbed: washout to substructure, subsidence.
- Rail, turnout: broken rail, breakage of turnout
- Track geometry: irregular track gauge, irregular track cross level, irregular track longitudinal and lateral alignment, irregular track twist
- Track fastening system: rotting sleeper, unscrewed screw spikes
- Derailer.

The most common defect of roadbed is the damage of washout to substructure due to flood, rainstorm or other extreme weather conditions. If a large quantity of water in the area of rail substructure exceeds the drainage ability, the ballast may be washed out and sleepers are hung into the air consequently, which could lead to the occurrence of derailment possibly.



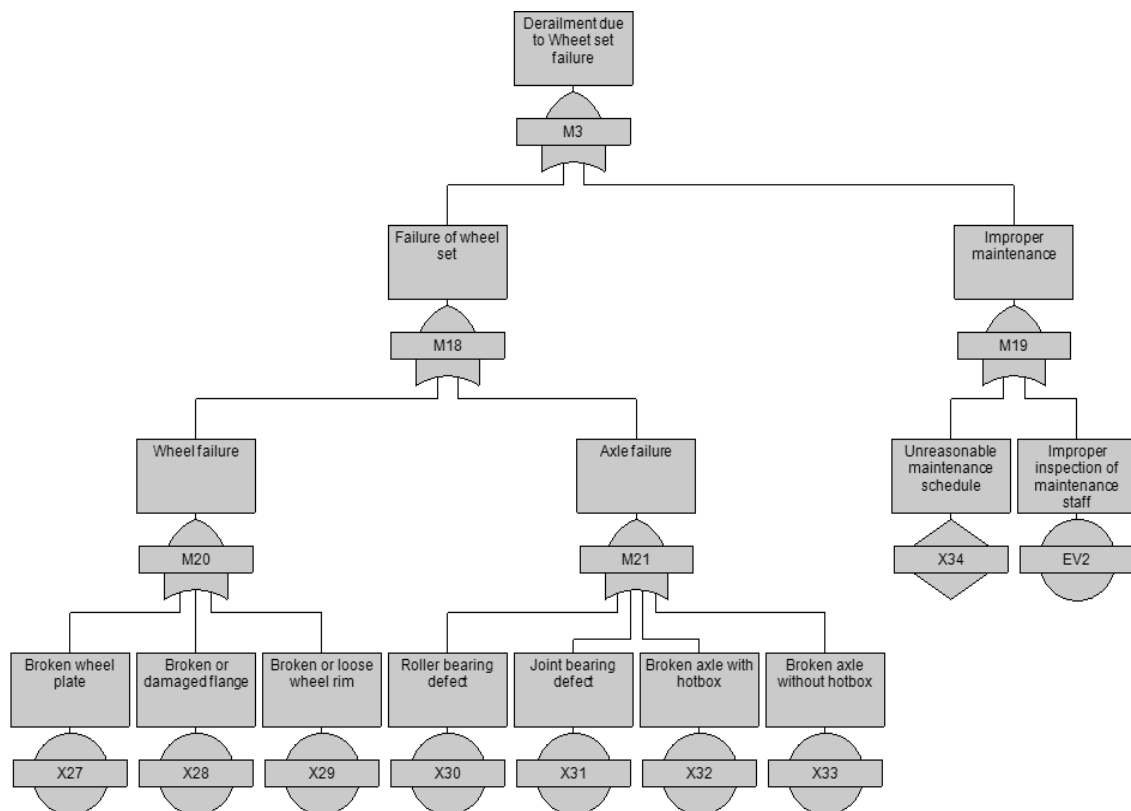
**Figure 28** FTA for Top Event – Derailment due to Track failure

Broken rails and turnouts could lead to discontinuous contact between wheels and tracks increasing the risk of derailment. Irregular track geometry may generate a resonance between the train and track, which contributes to the occurrence of a derailment. For the second category of infrastructure factors, the most important factor is the broken rail. For rails jointed with bolted fishplates, the cracks caused by huge shear force around the bolt hole occur and expand from the bolt hole. Similarly, for rails jointed by welding, the cracks may occur due to the poor welding quality. Once the contact stress between wheel and rail is too high, the spread of welding cracks or other fatigue cracks will be accelerated under wheel-rail interaction, which eventually causes broken rails (Liu et al., 2012)

The irregularity of track geometry can be divided into four classes, namely track gauge, track cross level, track alignment and track twist (Soleimanmeigouni et al., 2018)

- Track gauge: the distance between inner sides of two parallel rails at a given track location.
- Track cross level: the difference in elevation between the top surfaces of two adjacent rails, which is computed from the angle between the practical running surface of rail and a horizontal reference plane. The cross level in the curved track section is also called cant to measure the difference in height between the outer and the inner rail.
- Track longitudinal and lateral alignment: track geometry of the predefined centerline onto a longitudinal and a lateral plane.
- Track twist: the gradient of track cross level or cant in a given track section.

A periodic track irregularity can excite individual vibrations in the train when driving through the track section. If the excitation frequency coincides with the natural frequency of certain trains, the vertical force caused by resonances can become so great that the contact between wheel and rail is lost and the wheelset therefore derails. In addition, track irregularities can also result in different lateral forces acting on wheels, especially on the curved line, increasing the risk of derailment.

**Wheelset failure and technical equipment failure****Figure 29.** FTA for Top Event – Derailment due to Wheelset failure

The category of technical equipment factors contains potential failures on the rolling stock or on technical facilities. Rolling stock failures mainly include:

- Locomotive: running gear failure, traction motor failure, crank case, oil or fuel fire, electrically caused fire, third rail/pantograph defect, onboard computer failure to respond
- Bogie: broken bogie frame, defect on suspension (primary or secondary), failure of the damper
- Wheels: broken or damaged flange, broken wheel plate, broken or loose wheel rim, thermal crack
- Coupler: broken knuckle, coupler mismatched, broken coupler carrier or shrank, failure of articulated connectors
- Axle set: broken or defective wheel shaft, roller bearing defect, hot box
- Vehicle body: broken or defective bolster, broken or defective traction beam, broken or defective centre plate, broken draft or centre sill
- Brake system: detrition of brake shoe, broken or defective brake disc, blockage of brake line, uncoupled air or hydraulic hose, obstructed brake pipe
- Improper structure design of rolling stock



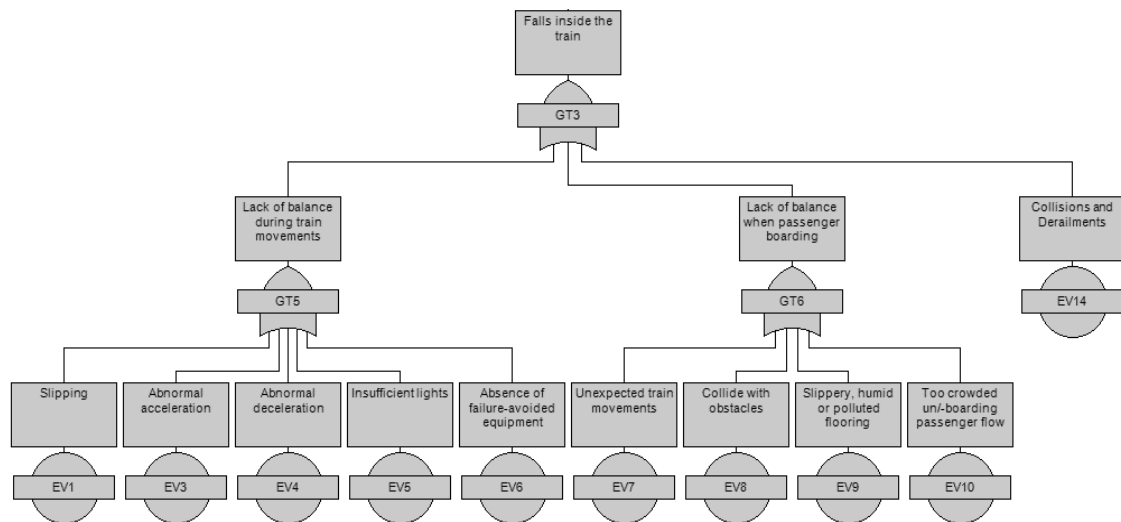
### 4.3.5 Incidents leading to people injured in urban railway operation

The incidents leading to people injured in urban railway operation is a type of incident with a high frequency because the density of urban railway users is very large, especially during peak hours.

This category of incidents can result in damage ranging from minor to catastrophic, depending on the location of the event and whether it was caused by a train collision or train derailment or natural disaster.

This accident could be divided into 4 hazard types: falling in the train, falling on the track, falling on the platform and gripped by train door.

#### ***People falls in the train***



**Figure 30** FTA for Top Event – People falls in the train

The main reason of the passenger falling inside the train is normally in lack of balance during train movement or passenger boarding:

- Slipping: can be a result of the floor material being chosen in a way that does not ensure friction, leads to passenger slipping as the train speeds. The other explanation is that the vehicle's floor surface is damp, tarnished, or was cleaned improperly, making the floor surface readily slippery.
- Obstacles: Passenger can accidentally collide with obstacles such as guide dog, person with reduced mobility, luggage, cycle transport of long or bulky objects leading to falling down
- Abnormal acceleration or deceleration: Excessive acceleration may be caused by traction failure, driver error, or any mechanical component of the roller bearing system failing. Estimating 10% abnormal acceleration/ deceleration damage to passenger.
- Insufficient lightings: This failure might be resulted from incorrect design of lightning system or failure of lightning based on insufficient or inadequate maintenance.
- Two crowded boarding/unboarding passenger flows.

The other reason is a consequence of Collisions or Derailment Accidents. These are catastrophic accidents that virtually surely result in passenger injury. Due to the lack of data

for the derailment accident, this part of the calculation will be performed using the collision accident calculation. It is estimated that 100% of collision accidents result in injury.

**Table 4.6** Probability of People falls in the train

| No   | Top Event  | Sub-failure                          | Hazard rates<br>(10 <sup>5</sup> km-operation) |
|------|--|--------------------------------------|--|
| GT5  | <i>Lack of balance during train movement</i>     |                                      | 1.1  |
|      |  | Slipping                             | 4E-01  |
|      |  | Abnormal acceleration                | 2E-01  |
|      |  | Abnormal deceleration                | 2E-01  |
|      |  | Insufficient lights                  | 1.5E-01  |
|      |  | Absence of failure-avoided equipment | 1.5E-01  |
| GT6  | <i>Lack of balance during passenger boarding</i> |                                      | 2.4  |
|      |  | Unexpected train movements           | 4.5E-03  |
|      |  | Collided with obstacles              | 0.7  |
|      |  | Slippery, humid or polluted flooring | 5E-01  |
|      |  | Too crowded boarding passenger flow  | 1.2  |
| EV14 | <i>Collision and Derailments</i>                 |                                      | 1.95E-02                                       |
| GT3  | <i>Falling inside the train</i>                  |                                      | 3.52   |

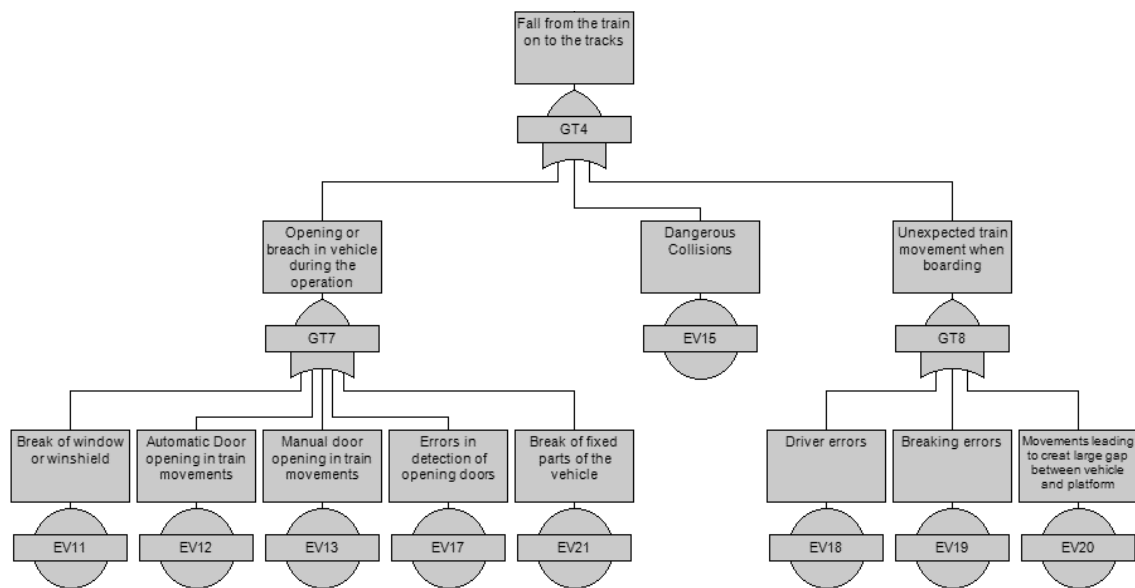
#### **People falls on the track**

The main reason of the passenger falling on the track is normally opening door or window during the movement or unexpectedly train moving as in the Figure 32.

- Opening or breach in vehicle during the operation: The critical risk in this case is breaking or window or opening of door (automatic opening or by manual). The additional failure is error in door opening detection and break of any part of the vehicle. This tolerate failure rate of automatic door according to technical design is  $2 \cdot 10^{-7}$  failure / operating hour and error of door detection is  $3 \cdot 10^{-8}$  failure / operating hour.
- Unexpected train movement when passenger boarding: This incident might be resulted from driver errors in controlling or breaking errors. The additional failure is creating a large gap between vehicle and platform.

**Table 4.7.** Probability of People falls on the track

| No   | Top Event  | Sub-failure  | Hazard rates<br>(10 <sup>5</sup> km-operation) |
|------|--|--|--|
| GT7  | <i>Opening or breach in vehicle during the operation</i> |  | 8.8E-03  |
|      |  | Break of window or windshield                                      | 1.87E-03                                       |
|      |  | Automatic Door opening in train movements                          | 1.04E-03                                       |
|      |  | Manual Door opening in train movements                             | 1.87E-03                                       |
|      |  | Errors in detection of opening doors                               | 2.08E-04                                       |
|      |  | Break of fixed parts of the vehicle                                | 3.82E-03                                       |
| GT8  | <i>Unexpected train movements when boarding</i>          |  | 6.73E-03                                       |
|      |  | Driver errors  | 3.5E-03  |
|      |  | Breaking errors  | 2.3E-04  |
|      |  | Movements leading to create large gap between vehicle and platform | 3E-03  |
| EV14 | <i>Collision and Derailments</i>                         |  | 1.95E-03                                       |
| GT4  | <i>Falling on the track</i>                              |  | 1.75E-02                                       |



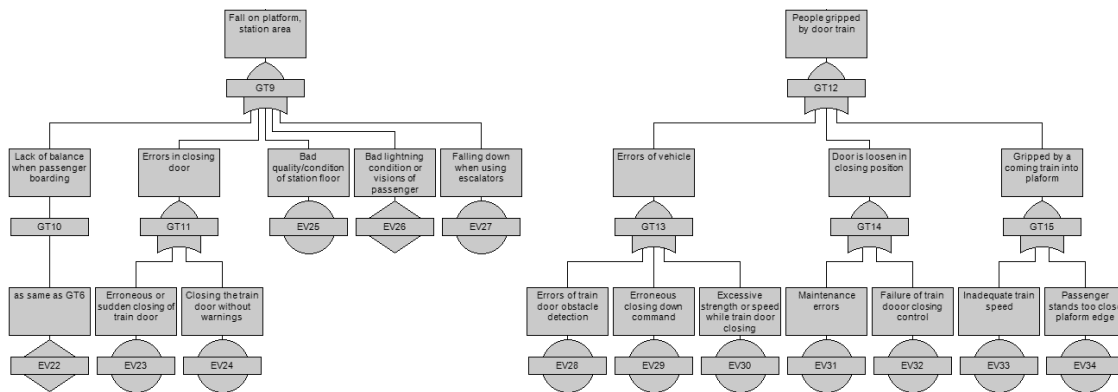
**Figure 31** FTA for Top Event – People falls on the track

- The other reason is a consequence of Collisions or Derailment Accidents. These are catastrophic accidents that virtually surely result in passenger injury. Due to the lack of data for the derailment accident, this part of the calculation will be performed using the collision accident calculation. It is estimated that 10% of collision accidents result in falling out of passenger to the track.

#### **People falls on platform and gripping by train door**

**Table 4.8.** Probability of People falls on platform and gripping by train door

| No   | Top Event                                      | Sub-failure   | Hazard rates<br>(10 <sup>5</sup> km-operation) |
|------|--|---|--|
| GT9  | <i>Fall on platform, station area</i>          |   | 4.75   |
|      |  | Lack of balance when passenger boarding             | 1.1  |
|      |  | Errors in closing door                              | 3.11E-03                                       |
|      |  | Bad lightning condition or vision                   | 3.5E-01  |
|      |  | Bad quality/condition of station floor              | 1.8  |
|      |  | Faling down when using escalators                   | 1.5  |
| GT13 | <i>Errors of vehicle</i>                       |   | 2.29E-03                                       |
|      |  | Errors of train door obstacle detection             | 2.08E-04                                       |
|      |  | Erroneous closing down command                      | 1.04E-03                                       |
|      |  | Excessive strenght or speed when train door closing | 1.04E-03                                       |
| GT14 | <i>Door is loosen in closing position</i>      |   | 6.04E-03                                       |
|      |  | Maintenance errors                                  | 5E-03  |
|      |  | Failure of train door closing control               | 1.04E-03                                       |
| GT15 | <i>Gripped by a coming train into platform</i> |   | 7.5E-03  |
|      |  | Inadequate train speed leading to accident          | 5E-03  |
|      |  | Passenger stand too close platform edge             | 1.5  |
| GT12 | <i>People gripped by door train</i>            |   | 1.58E-02                                       |



**Figure 32.** FTA for People falls on platform and gripping by train door

According to above calculation tables, the accident failure of TOP EVENT: Incident leading to people injured is 8.3 incidents per  $10^{-5}$  operating kilometres.

Based on technical design and operational plan of the Line HN2A, the total length of this line is 13.02 km. The number of train operated per day in the first commercial operation phase (2021-2025) are 152 trains/days and in the second commercial operation phase (from 2026) are 252 train/days. Therefore, the probability of Train Collisions are:

From 2021-2025,  $C0 = 8.3/100.000\text{km} * 13.02\text{km} * 152 \text{ trains/day} * 365 \text{ days} = 60$  incidents/year

From 2025,  $C0 = 17.76/100.000\text{km} * 13.02\text{km} * 272 \text{ trains/day} * 365 \text{ days} = 107$  incidents/year.

## 4.4 The Bayesian Network application for Metro Line HN2A

### 4.4.1 Methods and Procedure of establishing the Bayesian Network

A Bayesian network illustrates the causal probabilistic relationship between a set of random variables, their conditional dependencies, and a joint probability distribution in a compact manner. It consists of a directed acyclic graph and a collection of conditional probability distributions. The directed acyclic graph consists of nodes representing random variables. If there is a causal probabilistic dependence between two random variables in the graph, their nodes will be connected by a directed edge. And this edge demonstrates that random variable A causes random variable B. Cycles are not permitted in the graph because directed edges imply a static probabilistic causal dependence. For each node in the graph, a conditional probability distribution is defined for each conceivable outcome of the preceding causal node (Murphy, 1998, Rausand, 2011, Horny, 2014).

A Bayesian network analysis consists of the five steps listed below:

- **Step 1:** Plan and organise.

The contents of this phase are similar across numerous risk assessment approaches. In addition, BN is a quantitative evaluation approach, therefore the system description, system specifications, and data collection can be inherited from the PHA or FTA, as discussed in sections 4.2 and 4.3.

In chapter 2 - Literature review, the dissertation also highlighted that a fault tree could be further strengthened by transmitting into BN, which could offer significant advantages. For

instance, FTA is inappropriate for assessing the relationship between human factors and railway personnel errors.

Regarding practical metro operation in Hanoi, only one metro line (Line HN2A) has been commercially operated for seven months as of the submission date of the dissertation, and accident and error data are extremely restricted. In addition, the experience of the operator, the operator, the safety team is still limited, and risk assessment research in Vietnam has been at the basic concept level (which is relevant in Chapter 3). Consequently, the dissertation emphasises the FTA's strategy for constructing a simple, module-based assessment system that is easy to implement for Metro Line HN2A and applies to other lines currently under construction and planning. The BN technique is presented to the construction process and analytical foundation for analysing complex incidents involving many human and technological reactions. Instead of becoming the primary assessment method in the near future, the BN approach is employed by FTA to improve the accuracy of its evaluation system.

Section 4.4 provides a protocol and example for risk assessment by the BN approach in order to demonstrate the correctness and performance while assessing complicated systems. The BN technique is suggested in the Safety Management System to introduce a reasonable and effective analytical method and to encourage the technical personnel of HanoiMetro Company to study and develop risk assessment abilities.

- **Step 2:** Develop a Bayesian network.

Regarding fault tree analysis, it is essential to clearly and unambiguously describe the end node(s). The subsequent step is determining the causes (parents) that may impact the terminal node(s) and creating the arcs connecting the relevant nodes. It is comparable to building the top structure of a fault tree. This procedure is repeated until the required level of resolution has been attained.

There are several accessible computer applications for Bayesian networks. In the majority of practical analyses, an effective programme is required. The majority of these computer tools have a graphical interface that would be used to create and modify Bayesian networks. The next step is to specify the states of each node as discrete random variables with a predefined discrete value set. Create the tables of conditional probabilities.

- **Step 3:** Quantitatively examine the network.

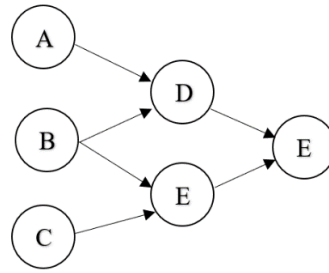
### **Conditional independence**

The probabilistic analysis methodology, including Bayes' formula, conditional probability and conditional independence is the fundamental concept of BN. The conditional probability formula  $P(A|B)=x$  refers to the statement, where the probability of event A is x if event B has already occurred. Assume that events  $B_1, B_2, B_3, \dots, B_n$  are mutually exclusive and the condition  $P(B_i) \geq 0, i=1,2,3,\dots,n$  is satisfied. According to the conditional probability theory, probability of the given event A can be expressed as:

$$P(A) = \sum_{i=1}^n P(B_i) P(A|B_i) \quad (4.8)$$

The posterior probability  $P(B_i|A)$  can be according to Bayes' formula:

$$P(B_i|A) = \frac{P(B_i)P(A|B_i)}{\sum_{j=1}^i P(B_j)P(A|B_j)} \quad (4.9)$$



**Figure 33.** Simple structure of Bayesian Network

Supposing that the nodes in Figure 33 are conditionally independent with respect to their parents. This indicates that nodes D and E are independent given the state of their parents, namely nodes A, B, and C. This indicates:

$$P(D \cap E | A \cap B \cap C) = P(D | A \cap B) \cdot P(E | B \cap C) \quad (4.10)$$

Let X be a node and let Parent(X) denote the set of parents to node X. In this case Parent (D) = A  $\cap$  B and Parent (E) = B  $\cap$  C. When nodes D and E are conditionally independent, then

$$P(D \cap E | \text{Parent}(D, E)) = P(D | \text{Parent}(D)) \cdot P(E | \text{Parent}(E)) \quad (4.11)$$

In a general case, we may then write

$$P(X_1 = x_1 \cap \dots \cap X_n = x_n) = \prod_{i=1}^n P(X_i = x_i | \text{Parent}(X_i)) \quad (4.12)$$

where we consider n nodes represented by the variables  $X_i$ . and  $X_i$  is a possible state of  $X_i$  for  $i = 1, 2, \dots, n$ .

#### **Conditional Probability Tables:**

Each node must be paired with a conditional probability table (CPT). Conditional probabilities indicate probabilities dependent on prior knowledge or experience. A CPT provides the variable distribution for each combination of parent states.

These values could come from expert judgment, some external sources, be estimated from data, or be a combination of the above. It should be noted that for Bayesian networks, the more complex the interactions, the more conditional probabilities there are to specify.

Example of CPT is given as in the following table.

**Table 4.9** Example of Conditional Probability Tables for BN in Figure 33

|             | A    |      | B   |     |
|-------------|------|------|-----|-----|
|             | 0    | 1    | 0   | 1   |
| Probability | 0.85 | 0.15 | 0.7 | 0.3 |

(a) CPT of Node A, Node B

| D | [A, B] |        |        |        |
|---|--------|--------|--------|--------|
|   | [0, 0] | [0, 1] | [1, 0] | [1, 1] |
| 0 | 0.95   | 0.85   | 0.7    | 0      |
| 1 | 0.05   | 0.15   | 0.3    | 1      |

(b) CPT of Node D

- **Step 4:** Quantitative analysis of Bayesian Network

Sensitivity analyses rank the significance of factors relative to the target variable (usually the endpoint). These variables highlight where better network quantification should be researched and identify the most influential model endpoint variables. These are the variables that should receive the most consideration. These variables may reflect critical management activities or knowledge gaps in a management situation.

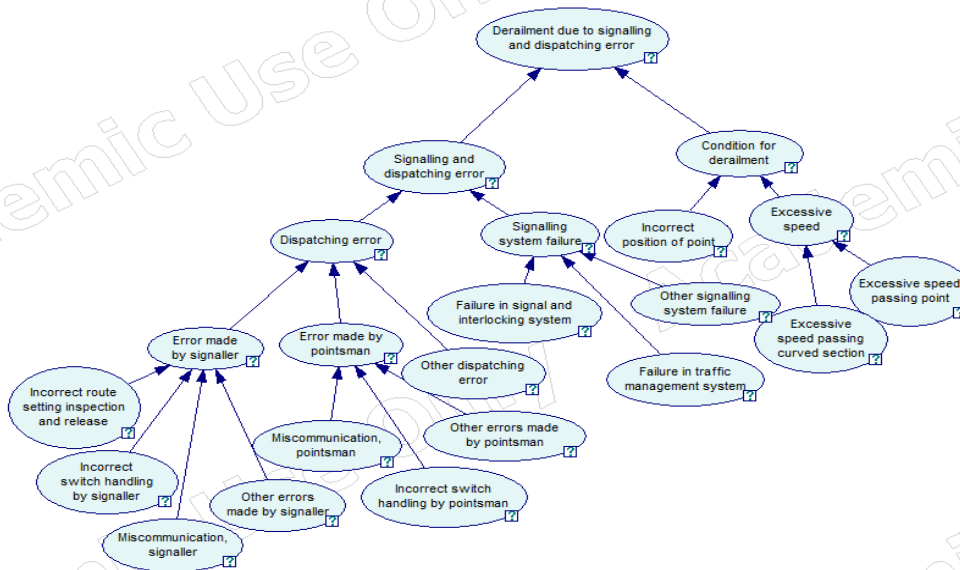
- **Step 5:** Document the analysis.

#### 4.4.2 Example of BN risk assessment - Derailment due to signalling and dispatching error

##### *Signalling and dispatching errors*

The failures in signalling and dispatching play important roles in precursors causing train derailments. This precursor is chosen as the first case to be developed in BN-analysis in order to explain how a fault tree can be transmitted into BN.

A diagram is built based on the sub-tree M2 - Derailment due to signalling and dispatching error (of which FTA are established in section 4.3.4) as presented in Figure 35. The root nodes at the bottom of network are basic events and the leaf node is the top event in the sub-tree.



**Figure 34.** BN of derailment due to signalling and dispatching error

The arcs in the BN-diagram are used to show the dependencies among root nodes, intermediate nodes and leaf nodes. However, the basic events in FTA resulting in an error made by signaller or pointsman are connected by OR-gates, which means the occurrence of any single subevent will lead to a signaller or pointsman's error. An advantage of BN is that the error probability is affected by the type of its subevent by considering conditional probabilities of each node state. For instance, as presented in the following tables, it is possible that miscommunication between signaller and other railway staff will not lead to a signaller's error if the operator does not violate safety rule. According to the hypothesis, the probability that a signaller makes an error is 40% if the miscommunication associated with a signaller exists. The probability increases to 75% if the miscommunication occurs accompanied by other kind of errors made by a signaller.

Given the probability of each root node in the network, the probabilities of intermediate events and the accidental outcome can be computed and the result is shown in the figures below by using Bayesian analysis software GeNIe. The occurrence probability of a derailment caused by signalling and dispatching error is 4.31%. Compared with the result of Fault Tree Analysis, the application of conditional probabilities can improve the degree of accuracy. Additionally, by taking risk reduction measures, probabilities of intermediate events and outcome decrease correspondingly, and the probability change is shown in the BN-diagram, which reveals effects of risk reduction measures clearly.

|  |  |        |               |                |               |                |               |                |               |            |
|--|--|--------|---------------|----------------|---------------|----------------|---------------|----------------|---------------|------------|
| Incorrect route setting inspection and release |  | normal |               |                |               |                |               |                |               | failure... |
| Incorrect switch handling by signaller         |  | normal |               |                |               | failure_occurs |               |                |               | ...        |
| Miscommunication, signaller                    |  | normal |               | failure_occurs |               | normal         |               | failure_occurs |               | ...        |
| Other errors made by signaller                 |  | normal | failure_oc... | normal         | failure_oc... | normal         | failure_oc... | normal         | failure_oc... | ...        |
| normal   |  | 1      | 0.85          | 0.6            | 0.25          | 0              | 0             | 0              | 0             | ...        |
| failure_occurs                                 |  | 0      | 0.15          | 0.4            | 0.75          | 1              | 1             | 1              | 1             | ...        |

|  |  |        |                |               |                |               |                |               |                |               |
|--|--|--------|----------------|---------------|----------------|---------------|----------------|---------------|----------------|---------------|
| Incorrect route setting inspection and release |  | normal | failure_occurs |               |                |               |                |               |                |               |
| Incorrect switch handling by signaller         |  | ...    | normal         |               |                |               | failure_occurs |               |                |               |
| Miscommunication, signaller                    |  | ...    | normal         |               | failure_occurs |               | normal         |               | failure_occurs |               |
| Other errors made by signaller                 |  | ...    | normal         | failure_oc... | normal         | failure_oc... | normal         | failure_oc... | normal         | failure_oc... |
| normal   |  | ...    | 0              | 0             | 0              | 0             | 0              | 0             | 0              | 0             |
| failure_occurs                                 |  | ...    | 1              | 1             | 1              | 1             | 1              | 1             | 1              | 1             |

Figure 35 CPT of error made by signaller

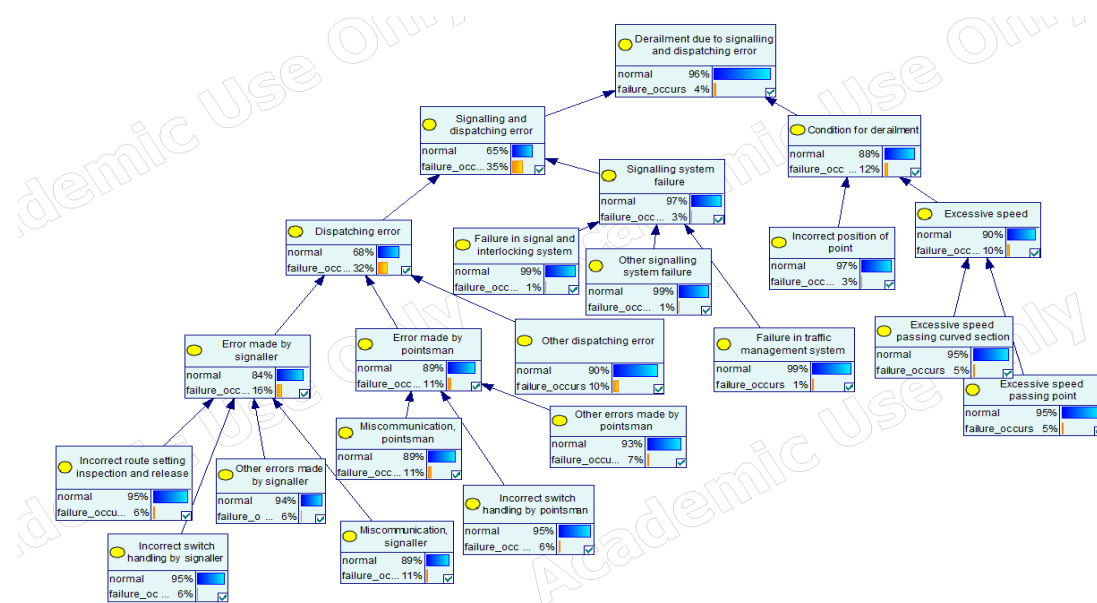


Figure 36 Probabilities of derailment due to signalling and dispatching error

The derailment is predicated on the simultaneous occurrence of an intermediate event caused by a fault or a human error, and an intermediate event related to objective conditions. Among the intermediate events leading to a signalling and dispatching error, the dispatching error with a failure probability of 32% plays a more important role than the signalling system failure. Furthermore, among intermediate events causing a dispatching error, the error made by signaller with a probability of 16% deserves the most attention. The detailed analysis of signaller errors will be clarified by Bayesian Network in the following section.

#### Detailed analysis of signaller errors

To analyse errors involving human behaviour and performance, FTA is insufficient due to its characteristics. On the one hand, FTA is not the best choice to solve the problem involving a



large quantity of common cause failures, because the complexity will increase significantly. On the other hand, the events in FTA are considered binary with only two states, normally the failure occurs or does not occurs. However, human factors shall be classified into several states to evaluate people's performance more effectively for risk analysis.

The application of BN has solved these problems. The BN-diagram presented below shows the relationship between performance-influencing factors and human errors during the signaller's operation. An error degree (ED) scale is used to classify the error behaviour, which provides the basis for multi-states classification in BN-diagram. Compared with the binary classification method, the error degree is able to describe human performance in railway operation more precisely. The state of a human factor with a higher risk of causing an accidental consequence has a higher value of error degree. For instance, the signaller's stress can be divided into four states, from ED0 to ED3, as introduced in the following:

- The state ED0 indicates that the signaller is mentally healthy in general.
- The state ED1 indicates that the signaller is in a psychological sub-healthy state with brief and mild symptoms, but his work is not therefore affected.
- The state ED2 indicates that the signaller has a psychological disorder caused by overload stress, which results in work-related problems.

The state ED3 indicates that the signaller suffers from psychological illness caused by overload stress, and the illness affects his working status greatly and he could not complete working tasks correctly consequently.

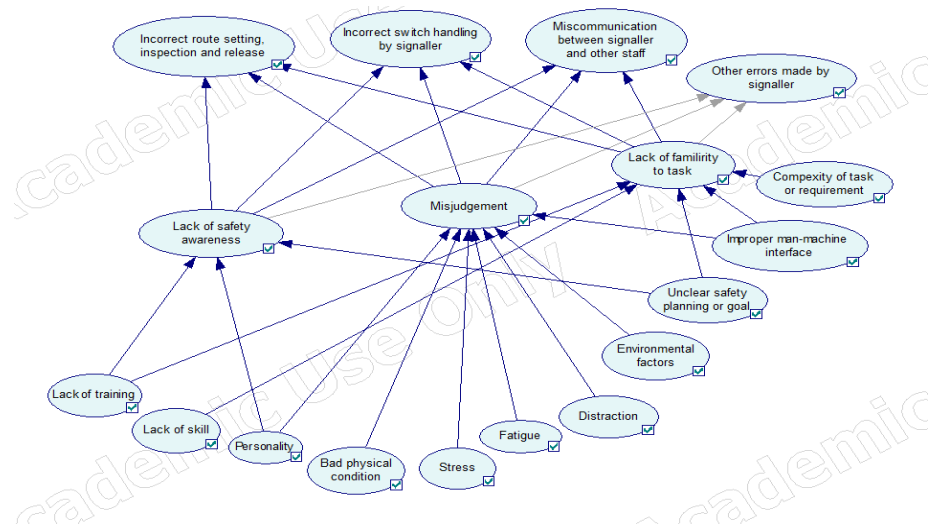
Based on the three groups of factors above, we can obtain intermediate events resulting from them:

- lack of safety awareness
- misjudgement
- lack of familiarity to tasks

The lack of safety awareness, this failure can appear as a result of individual and organisational factors. For instance, a signaller's personal carelessness and in-experience can contribute to weak awareness of safety. Alternatively, this failure can be attributed to inadequate safety management inside the organisation.

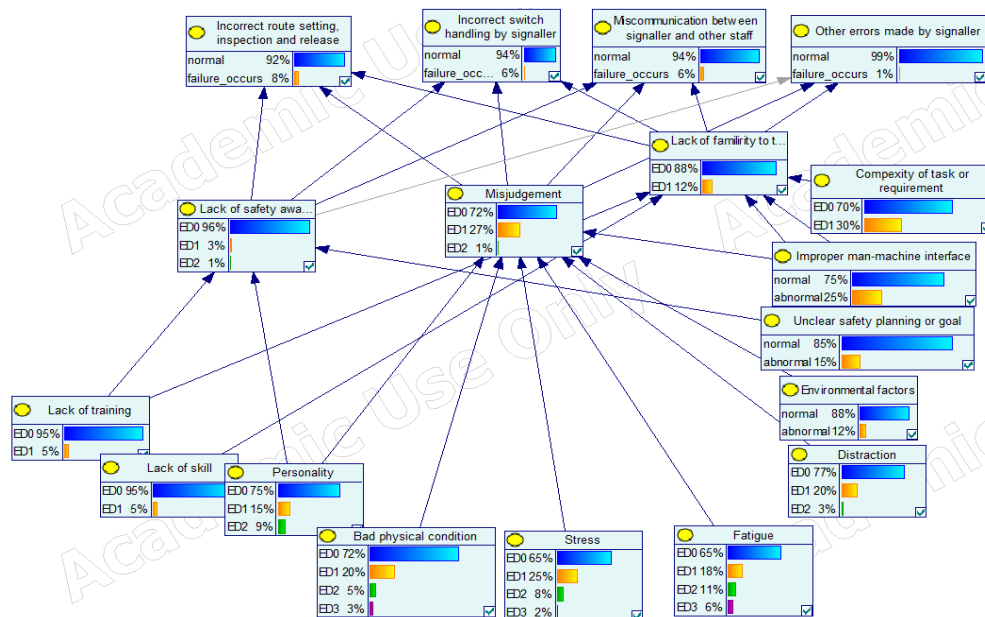
There are many factors leading to the misjudgement of a signaller. Signaller's misjudgement appears in the form of inadequate action timing and selection, such as untimely route release or switching command.

Generally, the lack of familiarity with tasks contributes to signaller's maloperation, which involves wrong timing and sequence of actions, such as wrong orders in a route setting operation. This failure occurs mostly due to improper training programs and staff management.



**Figure 37** Bayesian Network of error made by signaller

The probability of signaller mistakes are determined based on the assumption of fundamental performance-influencing variables and CPTs. Human error variables have variable ED levels, but other factors are binary.



**Figure 38** Node probabilities of error made by signaller

The analysis result indicates that the intermediate node misjudgement has a lower probability of ED0 than other two intermediate nodes in the diagram, which means it deserves more attention to prevent accidents due to signaller's error. Stress and fatigue with higher failure rates are main contributors to signaller's misjudgement. More data is required for the comparison of other factors because not only the error degree but also the contribution degree can affect the probability of consequence. The BN calculation in this chapter is only valid for demonstration purposes. In an actual analysis, a systematic set of evaluation criteria for each factor and CPTs needs to be established in order to achieve an accurate calculation result.

## **5. SAFETY SOLUTIONS FOR OPERATED LINE – RAILWAY VEHICLE MAINTENANCE AND OPERATIONS**

### **5.1 Railway Vehicle - Operating, Maintenance and Inspection**

#### **5.1.1 Purpose and Scope**

Rolling stock and other equipment are employed to carry out railway operations on a regular daily schedule. It is necessary to use, maintain, transport, and store in accordance with the manufacturer's recommendations to ensure that it remains safe in all situations.

The following procedures in this chapter aim to make sure that staff involved in the operation of rolling stock is aware of and compliant with the engineering and operational systems requirements. For detail, this procedure includes the following parts:

- Rolling Stock Operating.
- Vehicle Monitoring, Maintenance and Repair.
- Calculation of Maintenance and Repair Demand
- Vehicle Modification and Renovation.
- Rolling Stock Inspection.

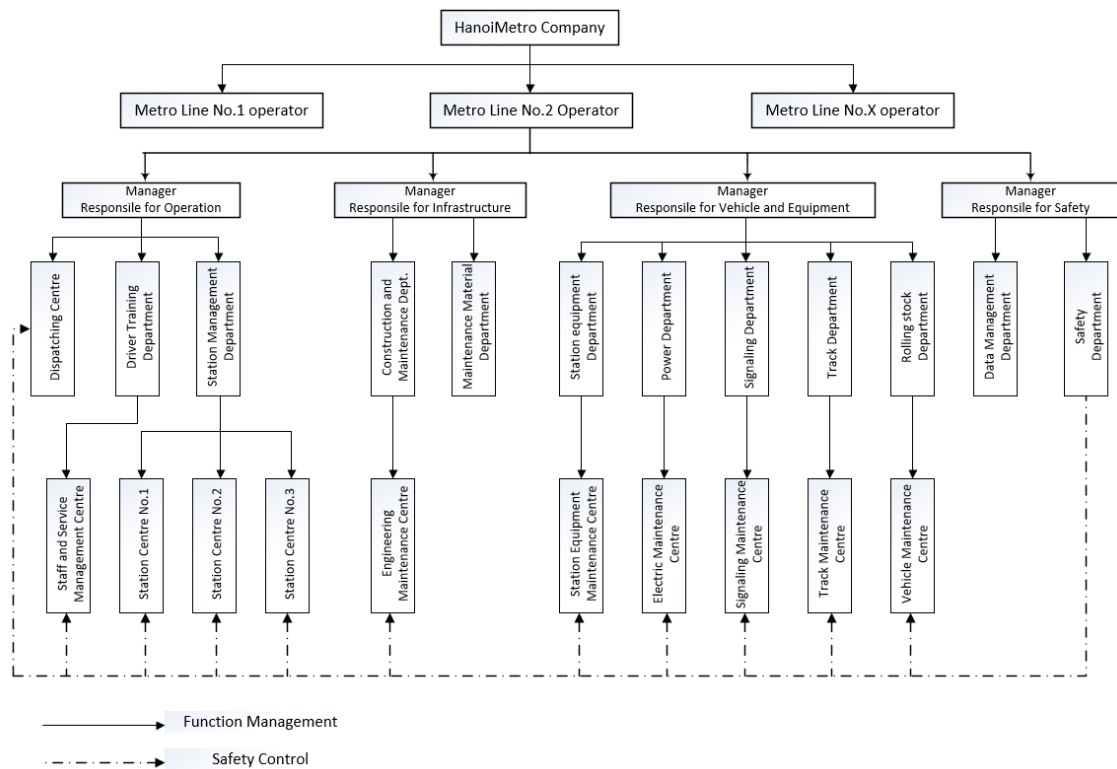
Dispatching Centre provided the real-time operation data and error identification of vehicles. Vehicle Maintenance Centre and Electric Maintenance Centre offered the maintenance service and provided empirical data and experience in vehicle inspection and maintenance. This data is transferred to the Maintenance database which is managed by the Rolling stock Department. The rolling stock Department coordinated with Power Department in developing and managing Codes of Practice, Guidelines and other supporting documents on the operation, maintenance and inspection of the vehicle.

These documents are technically completed by the Manager Responsible for Vehicle and Equipment, approved by the Manager Responsible for Safety, and finally annually reported to authority. The input data and manuals of rolling stocks and infrastructure which referred in Chapter 5 and Chapter 6 are cited from technical design as indicated in section 4.2.1. Furthermore, the specifications and maintenance manuals from JICA reports (JICA, 2015, JICA, 2016) are also taken into account.

#### **5.1.2 Management structure of Hanoi Metro Company.**

This section clarified the management structure of Hanoi Metro Company. Names and responsibilities of each centre or department referred to in Chapters 5 and 6 relating to maintenance and operation procedures are listed in this part.

The organised structure of the HanoiMetro was depicted in Figure 40. The Ha-noiMetro Company will be divided into several metro operators, each of which will control and operate a single metro line (for example, an operator for Line HN2A, an operator for Line HN3, etc.). Each Metro Line operator is headed by a Chief Manager, who is assisted by four Vice-Managers who are responsible for operational management.



**Figure 39.** HanoiMetro Company Structure

There are four division-manager which have responsibility for four main parts of maintenance and operation such as:

- **Operation:** including Dispatching Centre, Driver Training Department, Station Management Department and Station centres. These departments primarily manage operation procedures, emergency malfunction treatment operation procedures, and rescue plans.
- **Infrastructure:** including Construction and Maintenance Department and Material Department. These departments mainly prepare standards, technical staff and material for technical management of bridges, tunnels, stations, and other structures, as well as related rules and regulations.
- **Vehicle and Equipment:** responsible for Track, Vehicle and Signals maintenance to ensure the reliability and availability of system. These departments mainly control Depot and are the Task Force in accident treatment action.
- **Safety:** responsible in collecting and managing the safety reports from other departments and centres and take the internal assessments. This department also the primary and coordinating unit in accident treatment actions.

### 5.1.3 Procedures of Operating Rolling Stocks

This procedure is to prepare and to implement rolling stock engineering and operating procedures that meet applicable safety standards, rail regulatory requirements. The purpose of this Procedure is to arrange the normal operation of rolling stocks or manage any movement of any item of rolling stock on the network.

#### *Identification of Rolling Stock/Equipment*

All vehicles and equipment have to be identifiable by a unique asset number that is prominently displayed in a prominent location on the vehicle or equipment.

***Requirements for workers/staffs involved in operating:***

- Ensure physical and mental conditions to complete the required tasks. Be free of the effects of drugs, alcohol and fatigue.
- Possess a valid train driver's licence or other required certifications.
- Complete the Pre-Start Checklist (Appendix 3)
- Have participated in Pre-work briefings and workplace protection briefings in which provisions are made prior to the start of daily railway operating (Appendix 3 ).
- Establish and maintain effective communication in compliance with the network's appropriate rules and regulations.

***Preparation of rolling stock for travel***

Determine that danger lights or amber/orange flashing lights are operational and remain on during the operation.

Ensure that the vehicle carries (or the operator has immediate access to) the following when required to travel on the open network: (i) Two-way radio communication; (ii) Forms for tracking occupancy; (iii) Forms for tracking network conditions; (iv) Two red and two green flags; (v) Two multi-coloured hand lamps that have been approved

Assemble spare/backup Network Control and CB (Communication Barring) Radios as required for rolling stock movements.

Rolling stock must not enter service with a defective or isolated item of safety-critical equipment. Complete Vehicle Pre-mobilisation Checklist (Appendix 3).

The safe-working assessor of the Rolling Stock Department will contact the Dispatch Centre Department and Station Centre prior to rolling stock operations and check effective communication is established. The information needs to inform: (i) The number of track machines in the convoy; (ii) The identifying numbers of the machines in the order of travel; (iii) The authority required to travel.

The Dispatch Centre will check the schedule and inform the right of vehicle operation. The Station Centre will examine and confirm Train driving operation procedures.

***Travel Arrangements:***

While operating rolling stock on the track, operators have to ensure the following requirements.

- Only the operator shall ride on rollingstock unless a comparable level of protection, such as a cabin with seating, is provided for an extra person.
- Strict respect to stated and temporary speed limits is necessary.
- A safe braking distance is maintained between railway vehicles on track.
- The Station Centre must replay relevant messages from the Dispatch Centre to all Rolling Stock Operators. The Station Centre must effectively contact Engineering Maintenance for the tracking failure.

- The Rolling Stock Operator will communicate with the operators of other rolling stock associated with their duties and the Rolling Stock Department's safe-working assessor on an agreed-upon schedule.

In the event of a breakdown in communication with other track vehicles, the Rolling Stock Operator must:

- Degrade the automatic driving mode,
- Reduce of the vehicle's speed, and
- Prepare to stop within sighting distance.

The assigned staff of the Station Centre must inform the Dispatch Centre when the rearmost vehicle has:

- Departed a location.
- Entered or cleared a section.
- Cleared the Running Line.
- Arrived complete within a location.
- Cleared a location nominated by Dispatch Centre.
- Been removed from the line.

Authorisation, fitness for purpose, and compatibility with the running line and with approved coupling devices will be accomplished when authorised by the Manager Responsible for Operation.

### ***Security and Stabling of Vehicle***

After the working shift or when parked, all vehicles must be secured and/or stabled in such a way that no risk to the safety or health of any persons, railway infrastructure, or railway operators remains.

Methods by which this can be achieved are:

- Locked in a secure fenced compound in Depot.
- Electrically isolated.
- Stabled in an area with adequate lighting and having CCTV surveillance. Stabled in a secure mode with keys removed and doors locked.
- Have park brakes applied.
- Operating parts secured.

Always remove wheel chocks before attempting to move the equipment; otherwise, derailment may occur.

### ***Procedures if Rolling Stock breaks down***

- The Rolling Stock Operator must notify The Station Centre immediately. The Station Centre will inform to the Dispatch Centre. Protect the rolling stock in accordance with the network regulations.
- Make contact with Rolling Stock Department to arrange mechanic or electrician (or designated entity) to visit the worksite to repair machine and / or ensure it can be moved out of the section to clear the main line.

- If stuck on track attach the emergency tow bar and tow the machine back to the nearest siding using another track machine as soon as possible.

***Procedures if Rolling Stock is derailed or collided***

- Protect rolling stock in accordance with network rules and procedures
- The Rolling Stock Operator must notify The Station Centre immediately. The Station Centre will inform to the Dispatch Centre.
- Arrange first aid and emergency services as necessary.
- Implement the processes defined in Incident Management Procedure in relation to onsite examination of rolling stock involved in an incident by a qualified. Select representative or their agent, and where required arrange for the safe removal from site for further analysis, repair or disposal.
- Make contact with Rolling Stock Department to arrange mechanic or electrician (or designated entity) to visit the worksite to repair machine and / or ensure it can be moved out of the section to clear the main line.
- Inspect rolling stock for damage and carry out any urgent repairs required to make the item of rolling stock safe for traffic prior to departing the derailment site.
- The Dispatch Centre will inform to Engineering Maintenance Centre to assist in emergency response, to assess and repair the track damage.
- Undertake measures, including a risk assessment, prior to re-railing the item of rolling stock, with due regard to ensuring that neither machine nor the track infrastructure is further damaged.

**5.1.4 Vehicle Monitoring, Maintenance and Repair Requirements**

The purpose of this Procedure is to inform personnel responsible for the repair and maintenance of rolling stock of the procedures to be followed to ensure that, to the extent reasonably practicable, the item of rolling stock retains the same standards that enable the item of railway vehicle to continue to be safely operated.

This approach was designed to focus on the general requirements and considerations for each working phase. It is used in conjunction with specific Maintenance and Inspection Guidelines / Handbooks for each technical component/equipment.

***Security and Stabling of Vehicle***

After the working shift or when parked, all vehicles must be secured and/or stabled in such a way that no risk to the safety or health of any persons, railway infrastructure, or railway operators remains.

Methods by which this can be achieved are: (i) Locked in a secure fenced compound in Depot; (ii) Electrically isolated; (iii) Stabled in an area with adequate lighting and having CCTV surveillance; (iv) Stabled in a secure mode with keys removed and doors locked; (v) Have park brakes applied; (vi) Operating parts secured. Always remove wheel chocks before attempting to move the equipment; otherwise, derailment may occur.

***Monitoring and Inspection***

The Operator is responsible for routine daily maintenance and pre-start checks. The Vehicle Assessor or other equivalent who is in responsibility of the rolling stock on a day-to-day basis

shall ensure that weekly pre-start checklist forms are delivered to the Manager Responsible for Vehicles and Equipment.

- Inspection and testing in compliance with specified safety requirements and manufacturer's specifications, and as part of an Annual Maintenance Plan.
- Evaluation of service capability. Define the method for preventing damaged rolling stock from becoming operationally unable due to a change in operational capability.
- Identification of safety critical faults and abnormal deterioration rates.
- In service inspections included: (i) Pre-mobilisation checklists by qualified managers; (ii) Pre-Start Checklists by the vehicle engineers and dispatcher; (iii) Scheduled Maintenance documents; (iv) Braking systems; (v) Rail Wheel Inspection and (vi) Safety Critical Items.

The monitoring considers the seriousness and urgency of the situation, the importance of encouraging all employees to report incidents, and the importance of reports indicating if the pace of degradation of a defective item or system is significant.

### ***Maintenance and Repair***

Maintenance of rolling stock will only be conducted at Hadong Station Depot (for Line HN2A) and Nhon Depot (for Line HN3) which have adequate facilities for maintenance and repair.

The people assigned responsibility for the repair, maintenance and modification of rolling stock shall be assessed by Personnel qualification of Company.

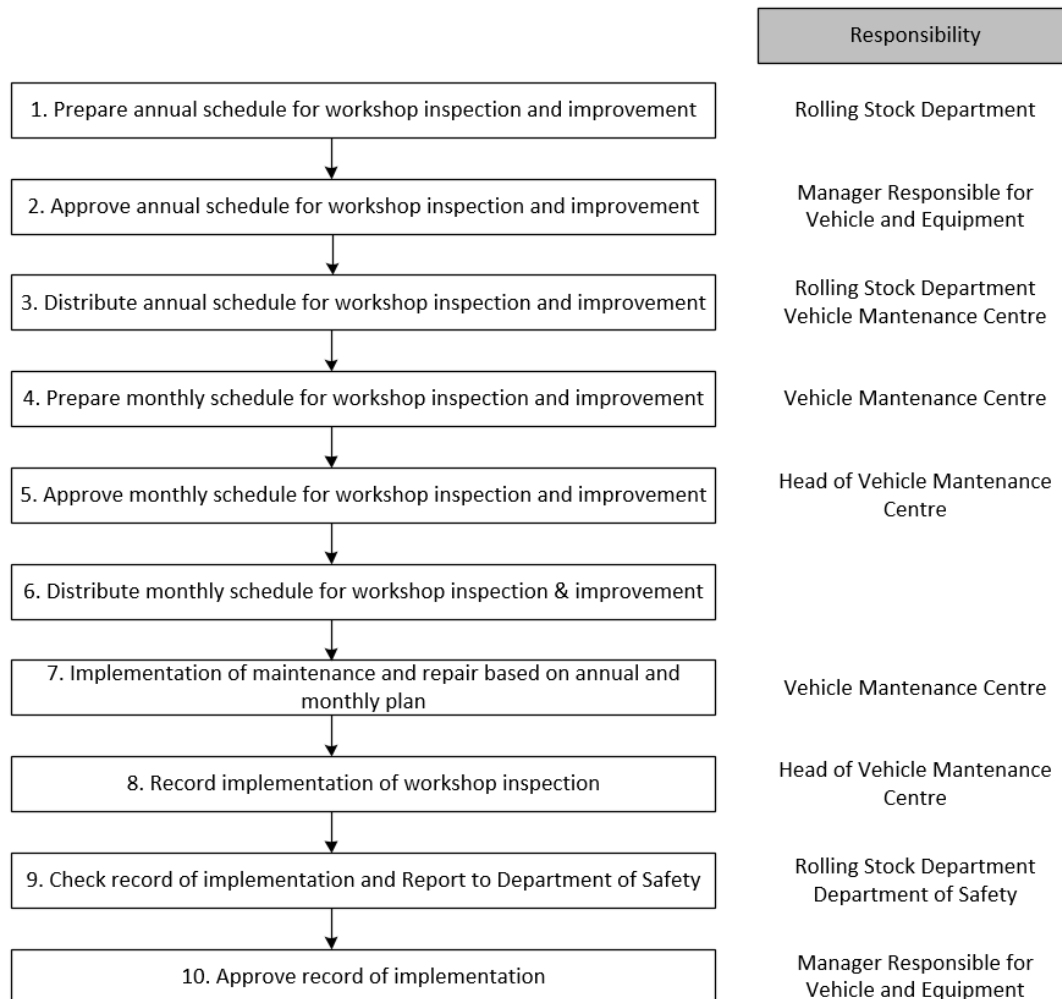
The operator records such daily maintenance for mobile rolling stock on a Pre-Mobilisation checklist. This form shall be sent to the Vehicle Maintenance Centre, which shall keep track of the maintenance working hour on a weekly basis.

The processes for the maintenance and repair need to incorporate the following:

- Any relevant preventative or corrective maintenance will be carried out in compliance with the applicable rolling stock regulations and according to annual maintenance plan.
- Operating, maintenance and spare parts manuals.
- The vehicle engineer/inspector is requested to complete a Pre- Mobilisation Checklist. The supervisor must be notified of any problems encountered during the inspection. These will be recorded in the Maintenance Management System, in part of Defects Register and Corrective Actions.
- Every situation involving rolling stock damage must be immediately reported to the Safety Department. Where damages has been assessed as a Notifiable Occurrence, must also be informed directly to the Manager Responsible for Safety.
- An annual maintenance plan will be developed for each item of rolling stock and be aligned to the manufacturer's specifications, legal criteria and relevant rail infrastructure and industry standards. Its content is for (i) planning maintenance work and ensuring that periodicities for attention are controlled by the implementation of the maintenance plan and (ii) for implementing an auditable maintenance management system that records last and/or next inspection.
- Additionally, a competent isolation system consisting of 'danger tagging' and 'out of service tagging' must be used to ensure that rolling stock or equipment is not used while it is in an unfit condition or is undergoing repair by a competent person.



Maintenance is scheduled on a calendar basis based on the manufacture's recommendation (daily, 10-day, monthly, 4-year medium scale repair and 8-year large scale repair), and notification of scheduled maintenance will be provided to operations that utilise the component of rolling stock. This timetable will be communicated 10 days in advance for monthly inspections and 60 days in advance for the medium and large scale repair. The planning process of maintenance and repair is described as in the following figure.



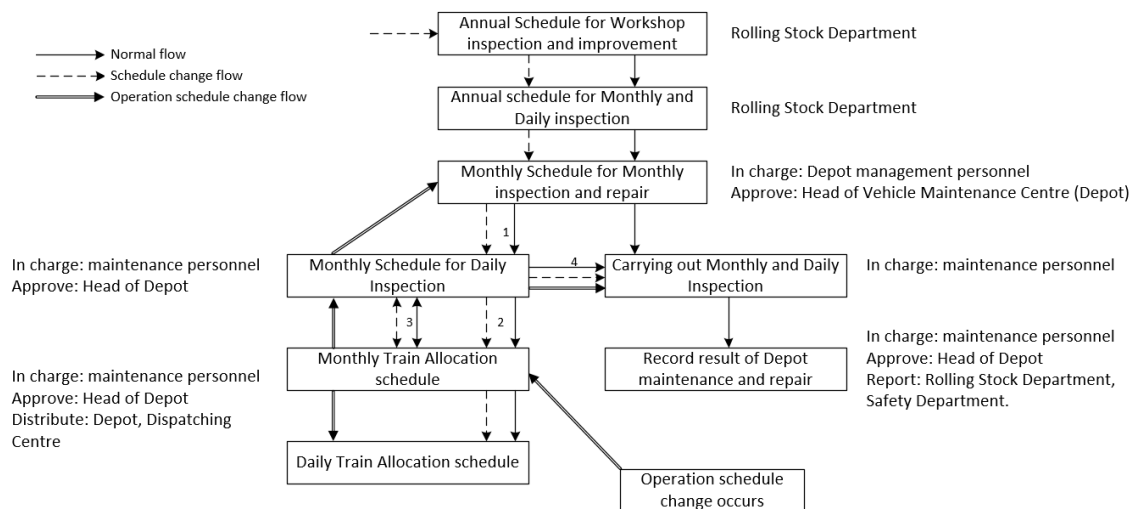
**Figure 40** Process of Maintenance and Repair Planning

An annual checklist (and also special maintenance checklist) will be used to record all information of:

- Works Orders are issued to adequately competent employees (internal or external) who possess the necessary skills to perform the operations;
- Standards compliance will be documented in the annual or special period reports.
- Field servicing will be logged as part of the vehicle's regular maintenance duties.
- Calibration of equipment will ensure that all relevant items of equipment used to measure rolling stock are calibrated correctly at all times.

Monthly maintenance allocation at the Depot: Based on the approved annual plan, the Vehicle Maintenance Centre in Hadong Station Depot prepares the detailed monthly train allocation. This plan will provide the daily and monthly inspection plans along with other

maintenance plans, and submits them to the management personnel in the Rolling Stock Department and approved by Manager Responsible for Vehicle and Equipment. The monthly inspection plan and the train allocation must be approved at least 10 days before the implementation date. The Head of Vehicle Maintenance Centre verifies that the trains are being operated as planned following the monthly inspection, taking the inspection result report into account. The maintenance result is reported to the Rolling Stock Department weekly. The Rolling Stock Department will summarise the maintenance conditions and submitted to the Manager Responsible for Vehicle and Equipment and Safety Department monthly or on any requested occasion.



**Figure 41** Flow of preparing train allocation at Depot

Daily plan: Based on the monthly plan, the the Vehilce Maintenance Centre personnel has a responsibility of preparing the detailed daily plan. The daily plan will be approved by The Head of Vehilce Maintenance Centre. The daily train allocation must clearly express the work to be implemented include the train allocation plan, and must be approved at least one day before the implementation date. The daily train allocation will be submitted to Dispatching Centre immediately after approval. If any changes or adjustments are made, they must also be reported promptly.

Form of monthly and daily Inspection plan is given in Appendix 4.

### 5.1.5 Calculation of Maintenance and Repair Demand

#### **Average demand of Maintenance and Repair**

When the average duration between medium-scale repairs is four years and the average period between large-scale repairs is eight years for 13 train sets, the average number of trains repaired (per year) is as follows.

8 years:  $13 \text{ train sets} / 8 \text{ years} = 1.6 \approx 1 \text{ to } 2 \text{ train sets/year}$

4 years:  $11 \text{ train sets} / 4 \text{ years} = 3.25 \approx 3 \text{ to } 4 \text{ train sets/year}$

1 months:  $13 \text{ train sets} / 30 \text{ days} = 0.43 \text{ train sets/day} \approx 1 \text{ train sets/day}$

10 days:  $13 \text{ train sets} / 10 \text{ days} = 1.3 \text{ train sets/day} \approx 1 \text{ to } 2 \text{ train sets/day}$

Daily inspection :  $13 \text{ train sets/day}$

However, because the operation of 13 train sets begins nearly simultaneously, their expected maintenance periods will be nearly identical. As a result, the implementation as stated in the previous calculation is difficult to be exactly applied.

Consequently, maintenance management is carried out on a kilometrage basis. Thus, while determining the number of rolling stock to be maintained, they convert the real kilometrage (train operating diagram) of each train on each line computed from the day, month, and year to the corresponding maintenance period-based kilometrage to classify the rolling stocks. The following shows the formula used to calculate the number of locomotives/trains on which largescale and medium scale repairs are conducted in a year.

$$N_{8-year} = \frac{L_{total}}{L_D} \quad N_{4-year} = \frac{L_{total}}{L_T} \left(1 - \frac{L_T}{L_D}\right) \quad (5.1)$$

In which,  $L_{total}$  is the total of kilometrage of every train on all lines in a year,  $L_D$  is the total of the kilometrage of the large-scale repair period and  $L_T$  is the kilometrage-based maintenance cycle of medium repairs.

However, it is necessary to consider and manage the possible cases where the occurrence of equipment failures installed in such trains will be earlier due to the increased travel distance, which may affect the operation plan compared with other trains. It is necessary to manage the devices and equipment which require inspection, maintenance and repairs based on the kilometrage (such as wheel grinding, brakes, etc.)

#### **Staff demand for large- and medium-scale maintenance**

Divide the maintenance work into small groups, and set the time required for one task as  $T_n$ . Total time for one task in maintenance work is  $T_T = \sum T_n$  (5.2)

$$\text{Total work time per year is} \quad T_Y = T_T * N_Y + T_{backup} \quad (5.3)$$

In which,  $N_Y$  is the number of trains maintained per year.

$T_{backup}$  is backup time for the maintenance (Preparation of working shift, Training, cleaning of Workshop, meetings, etc). Backup time per day is around 1 to 2 hours/personnel based on the given conditions in Vietnam. Therefore, in schedule calculation, assumes that backup time value is 1.5 hours per staff per day.

$$\text{Total working hours of personnel per year:} \quad P_T = 8 * (365 - d_1 - d_2 - d_3) \quad (5.4)$$

In which, working time is 8 hours/day,  $d_1$  is total weekends per year,  $d_2$  is annual national holiday (11 days),  $d_3$  - Annual paid holidays (12-17 days).

$$\text{The required number of maintenance staff is} \quad P_n = T_Y / P_T \quad (5.5)$$

#### **Staff demand for monthly and daily inspection and maintenance**

The classification of staff required for monthly inspection and maintenance is: (i) Administrative personnel (personnel management, preparation of maintenance plan and dealing with failures); (ii) Monthly inspection personnel; (iii) Rolling stock inspection personnel; (iii) Repair personnel; (iv) Operation line response personnel (restoration of failure on operation lines); (v) Other maintenance personnel; (iv) Drivers at depots; (v) Signal control personnel at depot; (vi) Rolling Stock cleaning personnel; (vii) Wheel grinding personnel

$$\text{The number of personnel required is} \quad P_n = T_T * N_m * (1 + \beta) / 8 \quad (5.6)$$

In which,  $N_m$  is the number of train sets to be inspected and repaired per day.  $\beta$  is the additional time ratio (for waiting time, break time, etc.) and assumed 0.15

The personnel for 10-day inspections are divided into several groups. Each group, consisting of two personnel, engages in rolling stock inspection. The time required for inspection of 1 train set is 1 to 2 hours. The daily inspection also arranged for these group and workload for one train daily inspection is around 0.5 hours.

Upon the opening of Line HN2A,  $T_T$  cannot be determined based on actual work. Therefore, to calculate  $T_T$  of Line HN2A, and the number of personnel and time required for maintenance work are compared based on the assumption that the maintenance plan and working items are almost the same in China and Japan.

Train inspection and repair department of Line HN2A are 53 working staffs, including 06 management staffs and 47 workers. The classification of personnel required for Line HN2A is given in Table 5.1

**Table 5.1** The number of personnel required for daily inspection and maintenance

| Classification                   | Position  | Standard arrangement             | No |
|----------------------------------|---|----------------------------------|----|
| Management Staff                 | Chief of Train inspection and repair department             | 1 person/department              | 1  |
|                                  | Deputy chief of Train inspection and repair department      | 2 people/ team                   | 2  |
|                                  | Chief Engineer  | 1 people/ team                   | 3  |
| Supervision team                 | Train inspection and repair Supervision staff               | 1 person/shift, 4 teams 2 shifts | 4  |
| Inspection and repair by segment | Main segment check supervisor                               | 1 person/shift, 4 teams 2 shifts | 4  |
|                                  | Seniorelectrification check                                 | 1 person/shift, 4 teams 2 shifts | 4  |
|                                  | Electrification check                                       | 2 person/shift, 4 teams 2 shifts | 8  |
|                                  | Senior Equipment check                                      | 1 person/shift, 4 teams 2 shifts | 4  |
|                                  | Equipment check   | 2 person/shift, 4 teams 2 shifts | 8  |
| Monthly maintenance team         | Monthly maintenance leader                                  | 1 person                         | 1  |
|                                  | Senior monthly electrification maintenance                  | 1 person                         | 1  |
|                                  | Monthly electrification maintenance                         | 2 people                         | 2  |
|                                  | Senior monthly Equipment maintenance                        | 1 person                         | 1  |
|                                  | Monthly Equipment maintenance                               | 2 people                         | 2  |
| General equipment                | Main supervisor to equipment                                | 1 person                         | 1  |
|                                  | Operator of machine type A (Crane Truck)                    | 1 person                         | 1  |
|                                  | Operator of machine typeB (Roller)                          | 1 person                         | 1  |
|                                  | Operator of machine typeC (Train washing machine)           | 1 person                         | 1  |
|                                  | Supervision of Equipment Type A (Measurement tool)          | 2 people                         | 2  |
|                                  | Supervision of Equipment Type B (small train, train repair) | 2 people                         | 2  |
|                                  | <b>Total</b>  |                                  | 53 |

### **Duty hours**

Technical inspections, medium- and large-scale repairs are performed during business hours by the assigned employees.

Regarding daily inspection personnel, a shift work system is used to ensure that daily inspection personnel are assigned to conduct inspections and operations at a depot during the

hours of 5:00 to 23:00 in conformity with the daily train operation plan. The working shift will be arranged into 3 groups:

- Shift 1: 04:00 to 13:00
- Shift 2: 12:00 to 21:00
- Shift 3: 20:00 to 04:00 next morning.

The working shift allocation of staffs need to take into account (i) labor regulations, (ii) to satisfy the workload and work requirements, (iii) to keep the minimum number of personnel necessary, (iii) to avoid taking over between shifts during busy hours.

### **5.1.6 Vehicle Modification / Renovation Procedure**

Renovation and/or modification of rolling stock is conducted halfway through their respective service lives or on special occasions when the rolling stock has a significant failure. In the case of Line HN2A, this work is conducted about 15 years after commercial launching according to the current specifications of metro lines.

When rolling stock to be renovated, the following must be considered:

- The process of change management is applied.
- Conducting a comprehensive risk analysis.
- Consideration of the proposed modification's overall effect on railway operations.
- The requirement for designing, implementing, and commissioning the entirety or a portion of the modification or reconstruction.
- The necessity of documenting and distributing information changes and alterations that influence operational safety

Primarily, while renovating rolling stock, several equipment such as the car body and bogie frame can be maintained if they are evaluated and found to be in good condition.

- Carbody: Usually, replace the display panel, internal control, electrical wiring, and electrical insulating and sound-proofing materials..
- Equipment: Overall, it should be considered to replace practically anything. After inspection, maintenance, and repair in the Workshop, additional equipment is discovered to ensure operations can be utilised. Replacing primary motors, control equipment, braking equipment, power supply equipment, and ventilation systems, among other things.
- The costs of renovation are usually about 50% of that required to purchase a new rolling stock.
- When a modification is recommended, replacement of signalling equipment (new technology) will be considered compatible with the signalling device on the railway.
- Replacement of electric devices should be considered 10 years after launch.

Verified the renovated vehicles by Registration Authority: Technical documents used in the inspection process include the following.

- Design documents for renovation

- Quality certificate (when quality certificate is necessary for a product) of the system and equipment configuration used for renovation of the vehicles, or technical documents.
- Production company's documents on the inspection and inspection for acceptance.
- Contents of the inspection include inspection of the quality of the renovating vehicles in the context of the existing technical criteria and standard, and review and evaluation of the design documents for renovation that have been verified by the registration body.
- Inspection method: Inspection on a vehicle basis.

### **5.1.7 Rolling stocks inspection**

This section of the guidelines describes the inspection items and procedures to be used to inspect rolling stock, which is designated by the semi-/overhaul and general inspection guideline. Periodic inspections of the condition and operation of rolling stock should proceed immediately after the last inspection is completed. For a semi-/overhaul (4-year/8-year maintenance), the counting should start from the month subsequent the prior examination is conducted.

#### ***Methods of inspection***

1. Visual: Conformity evaluated visually.
2. Auditory: conformity evaluated based on hearing
3. Olfactory: conformity evaluated based on odour.
4. Tactile: conformity assessed through manual contact
5. Tapping: Conformity is determined by tapping on a surface and listening to the sound made by the surface, or by using the hand to detect the resistance of the tapping tool or surface vibrations.
6. Operation: Conformity is determined by control devices during operation.
7. Measurement: Conformity is assessed through measurement.
8. Conductive: Conformance is evaluated based on whether or not gadgets are conductive.
9. As mounted: Examination performed with devices in place.
10. Dismounted: If a device is inaccessible for examination, for example, due to adjacent equipment, it must be removed from the rolling stock.
11. Overhauled: Some components of a gadget are overhauled as the device is being installed on rolling stock.
12. Dismounted and overhauled: The apparatus is dismounted and then inspected.

#### ***General Inspection of Electric Locomotives and Electric Cars***

1. Verify that all systems and gadgets have been installed correctly.
2. Check the height of lifeguards and sanding machines.
3. Check the functionality of energy collection devices.
4. Inspect the protection and control functions of devices in control circuits.
5. Inspect the insulating properties of electrical circuits that do not contain batteries or semiconductors.
6. Check the operation of the brakes.

7. Examine pneumatic brake controllers and other pneumatic equipment for air leakage.
8. Examine the air compressor's capacity and the operation of all associated equipment (e.g., pressure controllers and safety valves).
9. Check the car's angle of inclination.
10. Examine the functionality of automated door closers.
11. Check the functionality of the lights.
12. Examine the functionality of signals, intercoms, and public address systems.
13. Test the functionality of displays.
14. Examine the height of couplers.
15. Examine the operation of the automatic braking system and associated components.
16. Verify emergency braking and emergency protection system operation.

### ***Driving units***

The majority of inspections employed visual, aural, and tactile approaches to detect device surface degradation. Truck frame and swing bolster:

- Examine truck frames and bolsters for cracks, damage, deformation, or looseness, as well as for swaying.
- Examine wear plates for damage, wear, and loosening. Examine the condition of sliding components.
- Examine main motor mounts and gearboxes for cracks, damage, wear, or deformation.
- Check for air chambers that are broken, damaged, or leaking.
- Examine swinging bolster suspenders and suspender support bars, pins, and bushings for signs of wear, cracking, damage, deterioration, or looseness.

Center plate and side bearings:

- Assess for cracks, wear, and looseness.
- Check for broken or worn wear plates and for dust guards that have become loose.
- Examine oil level.
- Check trucks for worn, broken, or bent centre pins.
- Neither the central plate nor the side bearing has a bolster-less truck.

Traction device:

- Examine the body, frame, and springs of the traction device for cracks, damage, distortion, and looseness.
- Inspect for damaged, worn, or loose friction plates or rubber stoppers (for horizontal traction).
- Check for pins that are cracked, damaged, or worn.
- There is no traction device with a central plate truck.

Axle box and axle suspension:

- Roller bearing: (i) Check oil level; (ii) Check rollers, inner and outer rings, and cages for wear, deformation, cracks, peeling, damage or improper fitting; (iii) Check for cracked, damaged, or loosened wheel axle nuts, keys and snap rings.
- Axle box suspension: (i) Check links, flat springs, axle box horns and guide tubes for cracks, damage, wear or looseness; (ii) Check for cracked, peeled, damaged, deteriorated, or loosened rubber parts; (iii) Check axle guard stand-bys for cracks, damage, deterioration or looseness.

Wheels and axles: Utilized visual, auditory, and tactile techniques to detect surface degradation on wheels and axles. Utilized a measurement technique to evaluate the operational condition of wheel axles.

- Inspect tyres, cores, and snap rings for damage, wear, or looseness.
- Examine the wheel diameter, flange height and thickness, wheel diameter variations, and back gauge.
- Evaluate the vehicle for damaged axles and cracked or damaged tyre treads.

Springs:

- Inspect springs and spring washers for cracks, corrosion, deformation, or looseness.
- Examine air springs for cracks, corrosion, deformation, degradation, leaking, and looseness.
- Check for damaged, leaking, or loose differential pressure regulating valves or height control valves.
- Examine oil dampers for oil leaks and cracked, broken, or loose damper mounts.
- Monitor for cracked, broken, deformed, degraded, or loosened rubber parts.

Gear and gearbox:

- Check gears for cracks, deformations, wear, nicks, damage, looseness, and poor meshing.
- Look for broken, misshapen, leaking, or loose gears and covers.
- Evaluate for damage to the oil gauges and magnetic plugs. Examine oil level.
- Examine roller bearings for signs of wear, corrosion, or inappropriate gap.
- Check for fractured, degraded, distorted, or loose shock-absorbing rubber parts.

Flexible joint:

- Examine joints, cushion rubber, and balance springs for cracks, wear, damage, deformation, or looseness.
- Check for leaking oil. Check oil quantity.
- Assess shaft and gears for correct key-groove and tapered surface fit.

Grounding device:

- Inspect collecting rings and boxes for damage, wear, and cracks.
- Evaluate the state of the brushes.
- Examine for fractures, breakage, or deformation, and correct spring pressure.

Tachometer generator:

- Check for broken or frayed boxes, insulation, and wire leads.
- Evaluate operation.
- Examine insulation properties.

**Main Circuit Equipment** (including Control Equipment):

Power collection device - Pantograph and accessories: Used measurement and Insulation resistance tests.

- Under the frame, the main shaft, the frame pipe, the pantograph shoe, and the contact slider strips should be inspected for cracks, burning, damage, deformation, corrosion, wear, and looseness.
- Examine the pins, pinholes, and bearings for signs of wear, damage, or looseness.
- Examine the cylinders, air lines, and rubber hoses for corrosion, leaks, and looseness.
- Inspect insulators and other insulating equipment for damage or contamination. Also analyse the distance between the living part and the ventilator.
- Inspect connecting boxes for damage or loosening.
- Observe the solenoid valves and the switches.
- Verify the pantograph be lifted and lowered, and inspect its insulating properties.

Power collection device - Current collector shoe, its supporting instrument, and the beam: Utilised measuring and Insulation resistance examinations.



- Inspect for damaged or worn shoes.
- Validate the functionality and installation of movable pieces.
- Check for worn, partially worn, or loosened shaft bolts and supporting parts.
- Inspect for worn or corroded springs, cylinders, and push rods, as well as for worn or loosened rubber shock-absorbing components.
- Assess for damaged, cracked, worn, deformed, or corroded beams as well as worn or loose shock-absorbing rubber components.
- Examine insulation properties.

Power collection device - Main conductor and fuse: Used Insulation resistance tests.

- Examine insulating shields and terminals for damage. Examine the cross-sections of the main conductors, braided copper wires, and lead wires, as well as their installation, to ensure that they are properly sized and installed.
- Check for conduits and conductor-supporting fixtures that are broken or loose.
- Inspect for broken or loose boxes and fuses, as well as unusual packaging.
- Determine insulation.

Main motor – Rotor (including armature):

- Check the shafts and fans for damage, wear, and deformation.
- Examine armature commutation for damage, contamination, or discoloration.
- Inspect armature brushes for signs of wear, contamination, or loosening.

Main motor – Frame, field, lid and bearing:

- Examine the frames and field coils for corrosion, contamination, deformation, shorted coils, and damaged or loose cores.
- Check for broken conductors, shielding damage, and terminal cracks.
- Assess for broken or polluted fans, as well as end-lids, frames, and bearing inlets that are damaged, worn, deformed, or loose.
- Inspect bearings for damage, wear, or poor fitment.
- Check the level of oil.

Main motor – Terminal box

- Check for damaged, soiled, or loose boxes.
- Examine lead wires and terminals for damage, contamination, inappropriate contact.

Main motor – Assembly testing: Used measurement method, insulation resistance and dielectric endurance test.

- Verify the relative positions of all elements and the status of the assembled components.
- Assess the insulating properties.
- Verify rotational operation.

Devices in control circuit - Line breaker and main contactor:

- Examine damaged boxes. Examine the state of the chain locks and lead wires.
- Examine air line insulation and insulating joints for cracks, corrosion, contamination, deterioration, and leaks.
- Examine spark extinguisher coils, arc boxes, and arc guides for signs of corrosion, contamination, or loosening.
- Inspect the joints and sliding surfaces of movable sections for damage or wear.
- Inspect the contacts, fingers, and contact markers for damage or wear. Ensure their proper contact, security, pressure of contact, wiping action, and clearance.
- Check for frayed or disconnected copper wires in springs, terminals, crossover passageways, and braided copper wires.
- Verify that the main and sub contactor parts are synchronised.

- Assess the functioning beams and struts for cracks, damage, or looseness.
- Check for broken, corroded, or fouled magnets, as well as broken spring- or lever-contacts and dust coverings.
- Examine the solenoid valves and cylinders.

Devices in control circuit - Master controller

- Check terminals, lead wires, braided copper wires, and check lids for damage or looseness.
- Check operation and functioning of all parts.

Devices in control circuit - Semiconductor for main circuit:

- Examine damaged boxes. Check the condition of chain locks and lead wires and ensure they were fitted securely.
- Analyse semiconductors and insulation for degradation, soiling, and damage.
- Check for damaged or contaminated cooling devices.

Devices in control circuit – Controller:

- Verify characteristics.
- Perform a check to ensure that the controller has been placed in a safe and secure manner. Make that the plugs and lead wires are in good shape.
- Examine the card frame units to see whether any of them are polluted, broken, distorted, or loose.

Main transformer and its accessories

- Main transformer: (i) Check for soiled or damaged insulators; (ii) Check for oil leakage; (iii) Check insulation characteristics.
- Main rectifier: (i) Check for soiled or damaged insulators; (ii) Check for oil leakage; (iii) Check insulation characteristics; (iv) Check performance of elements.
- Reactor and filter: (i) Check for soiling and damage; (ii) Check insulation characteristics.
- Tap changer: (i) Check for damage; (ii) Check switching; (iii) Check operating time; (iv) Check insulation characteristics

### **Braking System**

Basic brake system:

- Levers and rods: (i) Check for worn, cracked or deformed levers and rods; (ii) Check movable and sliding sections for damage or wear; (iii) Check brake discs for cracks, wear, or looseness.
- Brake cylinder and brake diaphragm: (i) Check cylinder interior, pistons, and rubber bellows for damage, cracks or wear; (ii) Check oil level.
- Automatic clearance controller: (i) Check for damage, wear, and deformation; (ii) Check for proper operation.

Hand brake system: (i) Examine the moveable and sliding parts for any signs of wear or damage. (ii) Ensure that everything is working correctly.

Air brake controller: includes brake valve, brake control, control valve, relay valve, car operator valve, direct solenoid control, electro-pneumatic control, readout changeover, and device to respond to load changing.

- Examine the moveable and sliding parts for any signs of wear or damage.
- Ensure that the valve is making contact with the valve seat, and inspect the springs for any damage.
- Check to see whether the diaphragms and packing have become degraded, damaged, or deformed in any way.

- It is required that each and every electrical component be inspected in compliance with the guidelines outlined in the General Electrical Equipment in the parts that are listed below.

Air brake receiver:

- Guarantee there aren't any broken or missing boxes.
- Examine the connecting plugs and cables for any signs of damage or breakage.
- Verify the operations and the parameters that were updated.
- Conduct an examination of semiconductors in accordance with the guidelines provided in the Electrical Equipment – AC/DC converter section.
- Inspect reset switches as in the General Electrical Equipment section.

Emergency brake switch:

- Examine the container and its cover for any signs of damage or loosening.
- Be sure to inspect the insulation for any signs of cracking, corrosion, contamination, or deterioration.
- Investigate whether the lead wires and terminals have become damaged or come loose.
- Conduct a thorough evaluation of the contacts and contact fingers, looking for signs of damage, wear, incorrect contact, soiling, and looseness.
- Verify the operation of the switching.

Pressure sensor: (i) Check for damaged/loose sensors. (ii) Check operations and adjustment.

### ***General Electrical Equipment***

Auxiliary power supply unit and motor:

- Motor generator and blower: Motors shall be inspected as described in the Main Motor section; (ii) Check for damaged rectifiers and condensers; (iii) Check generator output characteristics.
- Power converter and stationary inverter: (i) Check for fouled or damaged insulation; (ii) Check for coolant leakage; (iii) Check for looseness; (iv) Check insulation characteristics of parts, other than semiconductors; (v) Check output characteristics.
- Battery and charger: (i) Check for corroded, damaged or loosened batteries, jumper cables and terminals, check for fluid leakage; (ii) Check weight and volume of battery fluid; (iii) Check charger for proper operation and secure installation.

Relay, solenoid valve, and wiring:

- Auxiliary resistor, fuse, and switch: (i) Check for damaged, discolored or deformed resistors; (ii) Check for fouled or damaged contact surfaces; (iii) Check for looseness.
- Contactor and relay:
  - Check the insulation for any signs of damage or contamination.
  - Examine moveable and sliding parts for any signs of damage.
  - Check that there is no slack in any of the parts.
  - Ensure that everything is working correctly.
- Solenoid valve:
  - Examine the coils for any signs of damage or burns.
  - Check that there is a good contact between the valves and the valve seats, and look for any valves that have been raised.
  - Check that there is no slack in any of the parts.
  - Ensure that everything is running properly.
- Arrester: (i) Check for damaged or fouled insulators; (ii) Check for looseness.

- Wiring, conduit, and optical fiber: The insulation resistance test should be used to identify the qualities of the insulation:
  - Inspect the cables, joint boxes, and any other components for any signs of deterioration or looseness.
  - Examine the characteristics of the insulation.
  - Inspect the optical fibres and connectors for any symptoms of damage, contamination, deterioration, or loosening.
- Air compressor controller:
  - Check to see if any of the chain locks or boxes have damaged or loose.
  - Make sure that the lead wires are in good shape.
  - Conduct an inspection to look for degraded or damaged semiconductors and insulation.
  - Conduct a thorough inspection of the condenser, looking for soiling, oil leaks, and distortion.
  - Examine the cooling fins to look for any signs of soiling or distortion.
  - Perform an inspection of the input and output properties of the pressure sensors.
  - In accordance with the guidelines laid out in the Electrical Equipment – AC/DC converter section, inspection of semiconductors is recommended.

#### AC/DC converter

- Converter box:
  - Check appearance. Check for deformed or loosened covers.
  - Check for clogging in covers for areas partly opened, and mesh covers.
  - Check for deteriorated packing.
  - Check wires and insulation for evidence of overheating, discolouration, or soiling.
- Semiconductor unit:
  - Check appearance. Examine the panels for any signs of looseness, distortion, or discoloration.
  - Examine the areas around the cooling fan for signs of soiling.
  - Examine the condenser's external look.
  - Check the various terminals.
  - Examine the look of the resistor.
  - Examine the elements of the semiconductor.
  - Check gate drive, pulse transformer, and base drive unit for loosened bolts.
- Resistor unit: (i) Check fins for soiling; (ii) Check terminals; (iii) Check for discolouration and deformation by visual observation.
- Control box:
  - Check appearance and lead wires. Check for loosened parts.
  - Check circuit boards for deformation, discolouration, corrosion.
  - Check electrolytic condenser for secure installation and loosened terminals.
  - Check connector connections.
  - Check card frame units for damage, soiling or deformation.
  - Change batteries regularly.
- Switch: Check for loosened plugs and loosened terminals.
- Units: Check power surge detection unit, voltage detection unit, and no-load resistive control unit for soiling, and loosened terminals and screws.

- Reactor and condenser: (i) Check for looseness; (ii) Check for evidence of overheating; (iii) Check for odor.
- Filter condenser: Check for looseness and insulators.
- Fuse: Check for damage, discolouration, and looseness.
- Electromagnetic contactor: used measurement methods to determine contact pressure and spacing between contacts:
  - Check for any springs, terminals, crossover passageways, and braided copper wires that may be broken or have become loose.
  - Check the contacts, the fingers, and the contact markers for any signs of damage or wear. Be certain that their correct contact, security, contact pressure, wiping action, and clearance are all in place.
  - Check the terminals of the live parts for any bolts that may have become loose.
  - Be sure to inspect the insulation for any signs of cracking, damage, or deterioration.
  - Cracks, damage, and looseness should be looked for in the coils, cores, and ceramic or steel plates of spark extinguishers.
  - Check the wear on the pins and their holes in the moveable part. Examine the sliding portions and joints to ensure that they have been put in a rigid manner.
  - Check the main and sub contactors are operating in sync with one another.
- High-speed circuit breaker: used measurement methods to determine spacing between contacts and the resistance of electromagnetic coils:
  - Identify the box if there is damage. Make that the chain locks and lead wires are in good condition.
  - Be sure to inspect the insulation for any sign and symptoms of cracks, corrosion, or deterioration.
  - Cracks, damage, or looseness should be looked for in the coils, cores, and ceramic or steel plates of the spark extinguisher.
  - Examine the arc box as well as the arc guide for any signs of damage, such as soiling, burning, or looseness.
  - Make that there are no worn pins or pin holes in the moveable part. Be sure to inspect the movable pieces and joints.
  - Check the contacts, the fingers, and the contact markers for any signs of damage or wear. Be certain that their correct contact, security, contact pressure, wiping action, and clearance are all in place.
  - It is important to inspect the springs, terminals, crossover channels, and braided copper wires for any signs of damage or looseness.
  - Check synchronisation of main and sub contactors.
  - Cracks and looseness in struts and working beams should be checked for.
  - Examine the magnets to see if they are damaged, fouled, or rusted, as well as the spring contacts, lever contacts, and dust covers.
  - Conduct a voltage and current check on the operating system.
- Receiver/transmitter box:
  - Check box for damage. Check insulation for damage, soiling, deterioration or looseness.
  - Check for damaged, cracked, broken or loosened terminals, crossover passages and braided copper wires.

- Check for broken, short-circuited or discolored coils.
- Check coil insulation.
- Check arc box and arc guide for damage and looseness.
- Check spark extinguisher coil for damage, discolouration or looseness. Check spark extinguishing performance.
- Check for damaged, worn or loosened contacts. Check contact pressure and wiping action.
- Check movable section for operation, adjusted values and operation.
- Check operating voltage and operating current.

### ***General Pneumatic Equipment***

Air compressor:

- Examine the motors using the criteria outlined in the "Main Motor" section.
- Examine the crank chamber, cylinder, and piston for any signs of damage.
- Check that the valves are not elevated and that they are making the correct contact with the valve seats.
- Examine the power transmission system for any signs of damage.
- Verify the amount of oil as well as the air and oil tightness.
- Ensure proper functionality.

Air compressor - Pressure governor, air pressure switch and safety valve:

- Examine the body of each device as well as its individual components for any signs of cracking, breakage, soiling, degradation, or looseness.
- Ensure there's still contact between the valve and the seat.
- Check the valves to see whether they are damaged or worn.
- Check contact between valve and valve seat.
- Verify the operation.

Supply valve and pressure reduction valve.

- Check valve-seat contact. Check for damaged springs.
- Check for damaged, deteriorated or deformed diaphragms and packing.
- Check operation.

Air tank: Check tank body and protective fittings for corrosion and looseness.

Air lines and hoses: (i) Check air pipe, hose and dust filters for damage and looseness; (ii) Check cocks for proper open/close operation and installation.

### ***Chassis and Interior***

Underframe: Check beams and lifting beams for damage, deformation, cracks and corrosion.

Car interior and exterior:

- Conduct a damage and corrosion check on the roof, the floor, the outside surface, the interior surface, and the intercar plates.
- Check for any signs of damage to the fittings, including the windows, shades, passenger seats, sliding doors, manually operated doors, and any other components, and make sure that everything is installed correctly.

Railcar roof:

- Examine the roof paint or the fabric roofing for corrosion or deterioration.
- Conduct a thorough inspection of the roof plates, footplates, and gutters for rust, water leakage, and looseness.

- Examine the bases of the current collectors, air conditioners, and ventilators to ensure that they are not broken, corroded, or loose. Check the insulating qualities of their products.

Automatic door closers (including safety device for door closing):

- It is important to inspect the door engines, belts, arms, links, rollers, and sliding devices for any indications of damage, corrosion, deformation, or looseness.
- In line with the inspection criteria for relay, solenoid valve, and wiring that are described in the General Electrical Equipment, solenoid valves, door closing switches, and safety devices for door closing should be inspected.
- Check the door closing devices as well as the air line for any signs of air or oil leaks.
- Examine the opening and closing procedures.

Lighting: (i) Check for damaged or loosened bulbs and lighting systems; (ii) Inspect relay contactors.

Window wiper: (i) Check for damaged wiper bodies and loosened wipers; (ii) Check operation; (iii) Check for damaged or loosened cylinders and motors; (iv) Check for damaged or loosened washer tanks and pump motors.

### **Other Equipment**

Signalling devices and on-board communication devices (including whistling and emergency notification devices): Check all devices for damage, soiling and looseness.

Display units: Check for damaged or loosened bulbs and lighting systems.

Instrumentation: (i) Check for damaged or loosened instruments; (ii) Check pressure gauge operation; (iii) Check speed meter operation; (iv) Check operation of electric instruments (voltmeters, ammeters, etc.).

Couplers: (i) Check coupler bodies, knuckles, anchorages, and pin holes for cracks, deformation and wear; (ii) Check coupling operation and coupler heights.

Automatic train supervision devices (ATS) (including automatic train controller, train selection device and automatic train operation device):

- On-board coil and receiving device: Check for damage, soiling and looseness.
- Speed detecting device (including tachometer generator): Check for damaged or loosened parts.
- ATS device (receiving, speed checking, logic and power supply sections): Check for damaged or loosened parts.

Cooling system:

- Unit cooler's main frame, cover and adiabatic material: (i) Check for secure installation; (ii) Check main frames and covers for cracks and damage; (iii) Check adiabatic and packing for peeling, deterioration and damage; (iv) Check insulating base and anti-vibration rubber for damage and deterioration; and (v) Check for clogged drain-pipes and holes.
- Main circuit board: (i) Check for soiling, damage and looseness; (ii) Check for proper operation of temperature display setter; (iii) Check insulation characteristics; (iv) Circuit breakers are to be inspected as described in the "General Electrical Equipment" section.
- Temperature and humidity sensors: Check for soiling, damage, looseness.
- Filter: (i) Check for soiling, damage and looseness; (ii) Check for clogging in filter; (iii) Check operation and function; (iv) Check insulation characteristics.
- Contactor fuse box: (i) Check box and insulation for soiling, damage and looseness; (ii) Inspect contactors and fuses.

- Air conditioner operating switch: (i) Check for soiling, damage and looseness; and (ii) Check operation.

***Test Operation after Maintenance of Rolling Stock***

1. Starting, acceleration and deceleration
2. Operation of braking system
3. Creaking, screeching, and vibration
4. Meter and gauge readings
5. Operation of automatic train operation devices
6. Condition of systems and equipment after test operation: (i) Main motor bearings; (ii) Devices in main circuits; (iii) Overheating or oil leaking in axles.



## 5.2 Railway Equipment – Inspection and Maintenance

### 5.2.1 Purpose and Scope

This procedure, which focuses on communication, signalling, electric power, and station equipment, establishes requirements for equipment maintenance work to ensure the stable operation of facilities and the continued operation of technological functions necessary for safe railway transportation.

The requirements for equipment maintenance work in the sectors of communication, signal, power, and station equipment are specified in this rule. **Communication equipment** is utilised to ensure safe operation and to facilitate passenger service communication. The **signal equipment** comprises of an interlocking device and a signal system that regulates train operation to ensure railway safety. **Electric power equipment** is the system that distributes electricity from a distribution board to the equipment at each station and to trains departing from an electric power substation.

For railway equipment, the inspection cycle and maintenance procedures are followed exactly as specified by the manufacturer. The procedures and recommendations that follow are primarily recommended for inspection and maintenance planning purposes, detailing the elements that must be inspected for railway equipment.

### 5.2.2 Maintenance schedule planning

The maintenance schedule planning for railway equipment will be classified into 3 levels such as long-term maintenance plan, monthly maintenance plan and daily workload.

At the long-term plan level, based on the manufacturer's instructions on equipment inspection and maintenance mode along with the Base Data control Table (including information on maintenance dates, actual equipment status, replaced items, ect), the in-charge engineer of the Maintenance Centre (Station Equipment, Electrical and Signalling Maintenance Centre) established the draft of Periodic Maintenance Plan (might be in the yearly or two-year cycle). The long-term maintenance plan needs to be prepared at least 6 months before the applied maintenance work.

This plan is reviewed and modified by adding the equipment status after an extraordinary inspection of item improvement if necessary. Thenceforth, the relevant department (such as Signalling Department, Station Equipment or Power Department) will check and recommend on the accuracy and feasibility of the maintenance plan and submitted the reviewed plan to the Manager Responsible for Vehicle and Equipment for approval. The Safety Department will receive the approved long-term maintenance plan and accumulate it in the Equipment safety document.

The summary of the equipment's long-term maintenance plan will be reported to Hanoi Metro headquarter as in the report of equipment utilisation and feedback to maintenance centres as the foundation of monthly plan preparation.

The monthly workload planning level is prepared and corrected by the in-charge engineers of the corresponding maintenance centre based on the following inputs: (i) Maintenance and repair guidelines of manufacturer for the equipment; (ii) The long-term inspection and maintenance plan; (iii) Occurences of extraordinary inspection and repair requests; (iv) Change of working days due to a holiday or other factors.

The responsible department (such as Signalling Department, Station Equipment or Power Department) will check and recommend the monthly working plan and submit the reviewed plan to the Manager Responsible for Vehicle and Equipment for approval. The plan preparation and approval process need to be completed at least three weeks in advance. When the approved plan is feedback to maintenance centres, the work instructions and personnel arrangement will be completed and announced to all engineers and workers.

If a maintenance request occurs after the monthly plan has been authorised, the appropriate changes to the Monthly workload plan and Work instructions must be made concurrently, at least 5 days prior to the monthly plan being executed.

Daily workload, which can be known as work instructions, is created by responding engineers of the Maintenance Centres based on the following inputs: (i) Monthly workload planning; (ii) The implementation process or time usage to respond to inspection or repair requests; (iii) Change of working plans.

The Deputy Manager of Maintenance Centres will check and recommend the daily workload and send it to the Manager of Maintenance Centre to approval. The workload needs to be confirmed one day in advance and announced to engineers and workers at the beginning meeting (daily training of staff) of work shifts. The maintenance team leader will arrange the worker into detailed actions to complete inspection repair tasks of the team. When the work shifts end, the team leader needs to prepare the operating report and submit it to the corresponding Manager of Maintenance Centres.

When an additional task/ request is added after the monthly workload is approved, the preparation of modified monthly workload and work instruction is implemented simultaneously to ensure the reasonable workload of workers.

### **5.2.3 Communication equipment inspection contents**

#### ***Overall Inspection of Equipment***

- Acceptability of the operating status
- Acceptability of the installed condition
- Check whether a problem resulted from environment, weather, etc.
- Check presence or absence of stains, damages, etc.
- Check presence or absence of abnormal odors, noises, etc.

#### ***Train wireless device***

Device body (each communication equipment room, field and equipment of OCC): Acceptability of wiring and mechanism

General function: (i) Acceptability of function and control: Acceptability of acoustic quality, alarmactivation, etc; (ii) Suitability of transmission and reception level; (iii) Acceptability of interface with relevant equipment; (iv) Suitability of spurious level.

Inspection cycle: daily.

#### ***Telephone equipment for business use***

Telephone switchboard body: (i) Acceptability of function and (ii) Acceptability of wiring and mechanism

General function: Acceptability of interface with relevant equipment.

Inspection cycle: 2 years.

### ***Electric clock system***

Electric clock system body: (i) Acceptability of function and control: Precision of time, and the acceptability of time correction function; (ii) Acceptability of wiring and mechanism

General function: Acceptability of interface with relevant equipment.

Acceptability of interface with relevant equipment.

Inspection cycle: 2 years.

### ***Security camera system***

For operation (Driver, conductor and station staff), including camera and monitor: (i) Acceptability of function; (ii) Acceptability of wiring and mechanism

For security (stations, OCC etc.), camera, monitor and video player: (i) Acceptability of function; (ii) Acceptability of wiring and mechanism.

Inspection cycle: one years.

### ***Announcement system***

Device body: (i) Acceptability of function and control: Acceptability for announcement in real voice and siren; (ii) Suitability of sound pressure.

General function: Acceptability of interface with relevant equipment.

Inspection cycle: one years.

### ***Passenger guiding system***

Device body : Acceptability of function and control

Platform indicator: Acceptability of function

Check the Acceptability of wiring and mechanism

General function: Acceptability of interface with relevant equipment.

Inspection cycle: 2 years.

### ***Communication equipment at depots***

Ground equipment for testing equipment on the vehicle side of the train radio system (simplified ground equipment)

Telephone equipment for professional use, entry phones, etc.

Security camera.

Announcement system.

## **5.2.4 Railway Signal equipment inspection contents**

### ***Overall Inspection of Equipment***

- Acceptability of the operating status
- Acceptability of the installed condition
- Check whether a problem resulted from environment, weather, etc.
- Check presence or absence of stains, damages, etc.
- Check presence or absence of abnormal odors, noises, etc.

### ***Orbital unit***

Acceptability of insulation state of rails

Acceptability of impedance bond, terminals, wiring and mechanism

Track circuit: (i) Suitability of voltage, etc; (ii) Suitability in train detection

Signal bonds: Acceptability of terminals.

### ***Signal including supporting materials***

Acceptability of wiring and mechanism.

Appropriateness of voltage.

#### ***Electric switch***

Acceptability of lock.

Acceptability of manual changeover.

Acceptability of function and control.

Suitability of voltage, etc.

Acceptability of wiring and mechanism.

Acceptability of lubrication.

#### ***Interlocking device***

Device body: Acceptability of function and control.

General function: Acceptability of interface with relevant equipment.

#### ***ATC (Automatic Train Control) device***

Device body: (i) Acceptability of function and control; (ii) Appropriateness of ATC signal on-the-spot.

General function: Acceptability of interface with relevant equipment.

#### ***CTC (Centralised Traffic Control) device***

OCC device, Station equipment and Transmission device need to be test: (i) Acceptability of function and control; (ii) Acceptability of transmission; (iii) Acceptability of interface with relevant equipment

#### ***Other devices (Signal)***

Sign marker devices: Acceptability of condition (Some sign markers use reflection board and LED other than paint)

PRC (Programmed Route Control) device (Small CTC device used at depots): (i) Acceptability of function and control; (ii) Acceptability of transmission; (iii) Acceptability of interface with relevant equipment

Supporting materials (Supporting column, supporting structure, piping, etc.): (i) Acceptability of condition; (ii) Acceptability of measures against damage caused by rats and disasters.

### **5.2.5 Electric power equipment inspection contents**

#### ***Overall Inspection of Equipment***

- Acceptability of the operating status
- Acceptability of the installed condition
- Check whether a problem resulted from environment, weather, etc.
- Check presence or absence of stains, damages, etc.
- Check presence or absence of abnormal odors, noises, etc.

***Circuit breaker*** : (i) Acceptability of wiring and mechanism; (ii) Suitability of insulation resistance; (iii) Acceptability of operation and condition (including lubrication).

***Transformer*** : (i) Acceptability of wiring and mechanism; (ii) Suitability of insulation resistance; (iii) Acceptability of operation and condition of accessory device.

**Rectifier:** (i) Acceptability of wiring and mechanism; (ii) Suitability of insulation resistance; (iii) Acceptability of operation and condition of cooling system; (iv) Acceptability of operation and condition of accessory device.

**Distribution board:** (i) Suitability of voltage, etc.; (ii) Acceptability of display; (iii) Acceptability of wiring and mechanism: Acceptability of relay; (iv) Suitability of insulation resistance; (v) Acceptability of sequence control (program-based control of conditions); and (vi) Acceptability of control after the conditions are met.

**Power management device:** Acceptability of function and control of OCC equipment, of operation unit equipment. Acceptability of interface with relevant equipment in control functions and displays.

**Grounding wire:** Acceptability of grounding wire; and Suitability of earth resistance.

***Supporting materials (including supporting insulator)***

Acceptability of various power poles, supporting brackets, accessory fixtures, insulation materials, etc.

Acceptability of trough, fire-proof compartment, etc.

Acceptability of measures against water leakage, water immersion, damage caused by rats and disasters.

Measurement of track clearance.

**Positive feeder:** (i) Suitability of insulation resistance (= Leak current); (ii) Acceptability cables, connections, etc; (iii) Acceptability of installed condition and (iv) Acceptability of accessory device.

**DC breaker:** (i) Acceptability of wiring and mechanism; (ii) Suitability of insulation resistance; (iii) Acceptability of operation and condition and (iv) Acceptability of accessory device.

***Return circuit and grounding wire***

Acceptability of negative feeder.

Acceptability of return wire bond.

Acceptability of accessory device.

Acceptability of grounding electrode and grounding wire.

***Third rail***

Suitability of insulation resistance (= Leak current).

Acceptability of installed condition of third rail.

Acceptability attached cables, connections, etc.

Acceptability of accessory device.

**Land marks and sign markers:** Acceptability of installed condition.

## 6. SAFETY SOLUTIONS FOR OPERATED LINE – TRACK AND CIVIL STRUCTURE MAINTENANCE

### 6.1 Purpose and Scope.

Maintenance of an urban railway is necessary to ensure that it remains in good operating condition and does not come to a halt for any reason. Additionally, the urban railway must maintain uninterrupted high-density operations. However, equipment will undoubtedly deteriorate with time due to repeated use and take time to be repaired and replaced. Regardless of the previous, the urban railway must operate in accordance with the plan once operations begin. This method will strengthen customers' perception of the urban railway as a reliable mode of transportation, hence increasing the number of users.

Among the several varieties of urban railway equipment, this document concentrates on civil structure maintenance and divides the task into three categories: inspection, planning, and repairs. Each item associated with track and civil structures must be maintained in good condition, potential failures must be avoided through appropriate measures, and necessary repairs must be carried out on a timely basis through appropriate measures to ensure the continued safe operation of urban railways and to maintain the relevant structures in good condition.

The following procedures define the requirements for track and civil structure maintenance on the individual metro lines operated and managed by HanoiMetro. Additionally, this regulation applies to companies and individuals directly involved in maintaining track and civil constructions in the Hanoi urban railway network.

### 6.2 Maintenance plan of Track and Civil Structures

#### 6.2.1 Track Maintenance Plan

30-year maintenance plan: The 30-year plan is structured in such a way that any unexpectedly substantial investment expenses may be shared over the whole business without jeopardising safe urban railway operations. Every component of urban railway equipment must be changed at a certain period. However, if the replacement of a significant number of pieces of equipment is necessary concurrently, a sizable sum of money will need to be set aside. Therefore, in addition to the annual repair costs, we must coordinate and clearly describe the investment costs for equipment upgrades over a 30-year period, based on the durable years of each piece of equipment specified during the design phase and the current state of the equipment as determined during daily inspections.

5-year maintenance plan: This plan aims to understand better the actual expenses associated with repairs and investment by making relevant components more achievable. Making relevant components more manageable entails organising things around repairs and investment around a 30-year plan, inspection-based judgement, and expected real work. Annual revisions to the 30-year and 5-year plans are desirable.

The 5-year maintenance plan, in particular, must be reviewed on a yearly basis. The 5-year plan details which firms are slated to open over that time span and their priority order. Thus, the five-year maintenance plan serves as a guide for gaining a comprehensive picture of the management position, not just for the departments asking budgets, but for all employees,

including management. The component of the 5-year maintenance plan that covers the future year becomes the plan for the following year.

The Track Department will be responding to prepare the 30-year and 5-year maintenance plan and submit it to Manager Responsible for Vehicle and Equipment. The Manager Responsible for Vehicle and Equipment will represent the Metro Line Operator to explain these schedules to Head Quarter of HanoiMetro.

#### Annual Maintenance Plan, Monthly Plan and Daily Inspection Plan:

While the maintenance plan details the work to be performed during the specified year, it is not possible to carry out the work only on the basis of the plan. To ensure that the job is completed on time, we must break complex activities into detailed maintenance work schedules and determine precisely who is responsible for what and when. As a result, the yearly maintenance plan's tasks must be separated into monthly and daily maintenance plans. Changes in actual maintenance work normally occur because we sometimes need to urgently address the sites that are affected by climate and natural conditions. Additionally, changes to the maintenance plan occur when scheduled work is not completed on time owing to the use of inexperienced staff.

When doing maintenance, the company require a daily maintenance plan that assigns the day's work to each shift in accordance with the monthly maintenance plan. This daily maintenance plan details the tasks that the maintenance personnel is responsible for throughout their shift. Additionally, it guarantees an accurate hand-off of duties between shifts to avoid any oversights. Each maintenance task completed during each shift is noted on the daily maintenance schedule. These records include critical information for developing future plans. Specifically, we can develop practical strategies only after evaluating and comprehending these records. Additionally, these records give valuable information for building human resource cultivation and employment strategy.

The staff in charge of plan preparation in Track Maintenance Centre will prepare the annual and monthly maintenance plans. The team leader of each repair team will discuss to maintenance worker and arrange daily shift.

### **6.2.2 Civil structure inspection cycle**

#### Viaducts inspection cycle

- Checking viaducts is carried out at least one times for three months.
- Checking the target locations using a service vehicle for high-elevation work one time in 2 years and record if cracks are detected. In this inspection, it is necessary to register the evaluation of the following items (i) inspection of area in the vicinity of the viaducts, (ii) place and dimensions, (iii) reasons and progress of crack state, and (iv) judgment on the influence of cracks.
- Extraordinary inspections: When the accidents occur, the Safety Department will collaborate with the Construction and Maintenance Department to inspect and evaluate the current state and promptly develop countermeasures. Such events may include unexpected accidents that affect the safe use of structures or safe train operations, accidents due to disasters such as typhoons, floods, earthquakes and fire hazards, and sudden train-related accidents.

#### Tunnel inspection cycle

- Every month: Check the tunnel visually while walking through it during the time period when trains are not running.
- Once/1 years: Check the tunnel visually using the lamp during the time period when trains are not running. In this inspection, it is necessary to register the evaluation of the following items (i) place and dimensions, (ii) reasons and progress of crack state, and (iii) judgment on the influence of cracks.
- Once/10 years: Check the tunnel in detail using the lamp during the time period when trains are not running. Inspect the tunnel ceiling using the service vehicle for high-elevation work.
- Extraordinary inspections: When the accidents occur, the Safety Department will collaborate with the Construction and Maintenance Department to inspect and evaluate the current state and promptly develop countermeasures. Such events may include unexpected accidents that affect the safe use of structures or safe train operations, accidents due to disasters such as typhoons, floods, earthquakes and fire hazards, and sudden train-related accidents.

Parts of buildings inspection cycle:

Wall surfaces, Ceiling, Window, Roof, Drainpipe: one time/year.

Soil tank, Water-purifier tank: 3 times/year.

Pressure tank, Booster feed tank, Water receiving tank: one time/year.

Hot water supply system, Gas powered hot water heater: one time/year.

Automatic door: 3 times/year.

Disaster control equipment, Automatic fire alarm: 3 times/year.

Fire extinguishing equipment, Water bar: one time/year.

Operator for smoke exhaust and ventilation: one time/2 years.

Lightning rod: one time/year.

## **6.3 Track Inspection methods**

### **6.3.1 Track patrol**

- At the very least once every month, a patrol must be conducted along the primary tracks to check for train noise and anomalous vibrations.
- Every member of the staff from the unit is required to stand in the train while it is inspected. In the driver's cabin, the unit chief and a staff member are positioned next to each other next to the driver. The remaining two members of the crew wait in the passenger car. These four individuals begin their examination of the track by looking at the front track.
- When a problem is discovered, the head of the inspection unit instructs the train's driver to come to a complete stop. When the train comes to a complete halt, two employees from the passenger car exit the train and conduct a thorough inspection of the tracks.

### **6.3.2 Patrol on foot**

- In order to ensure that the main tracks and side tracks are in good shape, there needs to be a minimum of a three-times-a-month patrol that is conducted on foot along the entirety of both types of tracks.



- When conducting an inspection of the track, all members of the staff walk along the track in the direction that is opposite to that in which the train is moving. They visually inspect the track to look for any deviations or issues.
- Two individuals tasked with quality control patrol the perimeter of the track. One rail is inspected by each of them in turn. The unit chief verifies the inspection results while walking down the inside of the tracks, and then notes them.
- The worker who is responsible for safety inspections moves approximately fifty metres ahead of the inspection team and stands there to alert them if a train is coming up behind them. He uses a torch and a whistle to alert others that a train is coming closer. As soon as they hear the warning signal, every member of the inspection unit staff quickly moves to a secure train shelter.

### **6.3.3 Inspection of structure gauge**

- To ensure that there are no facilities that are wider than the structure gauge, the inspection of the structure gauge must be carried out at least once every year in every segment of the main tracks and side tracks.
- The measurement car is driven by one of the staff members. The track tolerance is increased by two workers whenever the train approaches a curve. The chief of the unit stands behind them both while he or she verifies and writes down the results of the inspection on a notepad.
- The track tolerance must not be exceeded under any circumstances.

### **6.3.4 Measure the four items (gauge, cross level, longitudinal level and alignment)**

- To ensure that there are no facilities that are wider than the structure gauge, the inspection of the structure gauge must be carried out at least once every year in every segment of the main tracks and side tracks.

The measurement car is driven by one of the staff members. The track tolerance is increased by two workers whenever the train approaches a curve. The chief of the unit stands behind them both while he or she verifies and writes down the results of the inspection on a notepad.

The track tolerance must not be exceeded under any circumstances..

Allowable error: Widen: < 6 mm.

- Gauge measurement/ Measurement of cross level:  
The gauge must be measured at least once per year on all sections of the side tracks and at least twice per year on all sections of the main tracks. This is done to guarantee that the gauge has neither increased or reduced beyond a predetermined limit.  
The gauge is checked by the workers every five metres. The results of the measurements are inspected by the unit chief. One of the workers makes a record of the result of the measurement.  
Allowable error of Gauge measurement: +6/-3 mm. Allowable error of Cross level measurement: +5/-5 mm.
- Measurement of alignment:  
At a minimum of once per year for all sections of the side tracks and at least twice per year for all sections of the main tracks, alignment must be measured in order to verify that the alignment has neither increased or decreased beyond a predetermined threshold.

The gauge is checked by the workers every five metres. The string is being stretched by two workers while the alignment is being checked by a third worker. The head of the unit verifies the findings of the measurements and makes a note of them in the relevant file.

Allowable error of alignment measurement: 1/1000.

- Measurement of longitudinal level:

The longitudinal level must be measured at least once per year in all sections of the side tracks and at least twice per year in all sections of the main tracks. This is to ensure that the longitudinal level has not increased or decreased beyond a limit that has been specified. Measurement of the longitudinal level must be performed at least twice per year in all sections of the main tracks.

The gauge is checked by the workers every five metres. A third worker measures the distance from the string's current position to the top of the rail while two other workers maintain the string's straight position. The chief of the unit verifies the recorded measurements and ensures that they are accurate.

Allowable error of longitudinal level measurement: +10/-10 mm.

- Measurement of twist:

The cross level measurement is used as a starting point for calculating the rail twist measurement.

Twist must be measured at least once per year in all sections of the side tracks and at least twice a year in all sections of the main lines to guarantee that the amount of twist has not risen or reduced above a predetermined limit.

Allowable error of rail twist: < 12 mm.

### **6.3.5 Inspection of rail crack or rail damage**

- Rail must be inspected at least once every year in all sections of the side tracks and at least twice yearly in all sections of the main tracks. This is to check the top surfaces of the rails for damage, such as wearing depth, flaking, and shelling, and to check the welded joints of the rails for irregularities.
- Every single member of the group makes their way along the track. The track is inspected by two of the workers. The results of the inspection are reviewed by the unit chief. The outcome of the inspection is written down by one of the personnel Allowable error: (i) Observed on the rail head: Width: < 15mm. Length: < 100mm. Depth: < 10mm; (ii) Observed in the rail bottom: Reduction in width: < 15 mm, reduction in thickness: 7 mm

### **6.3.6 Inspection of Turnouts and crossings**

- The inspection of turnouts and crossings parts must be carried out at least once a year for all turnouts and crossings of the side tracks and at least twice a year for all turnouts and crossings of the main tracks to check tongue rails for engagement, to check top surfaces of rails for damage including wear, flaking, and shelling, and to check welded joints of rails for irregularities. This inspection must be performed at least twice a year for all turnouts and crossings of the main.
- Measure the four items (gauge, cross level, longitudinal level and alignment):  
Workers measure each item (items depend on the design of turnouts and crossings). The unit chief checks the measurement results and records them.

Allowable error: (i) Gauge measurement:  $+4/-2$  mm; (ii) Measurement of cross level:  $+4/-4$  mm; (iii) Measurement of alignment:  $+3/-2$  mm; (iv) Measurement of longitudinal level:  $1/1000$ ; (v) Measurement of back gauge, spacing between tongue rail and stock rail, clearance between tongue rail and stock rail: based on the design of turnouts and crossings.

- Wear inspection of turnouts and crossings:

Two workers measure depth of wear of the rail in the turnouts and crossings at the following locations: (i) Tongue rail: Left (1 or 2 points) and right (1 or 2 points); (ii) Crossing: At A, B and C; (iii) Guard rail: On stock side and turnout side; (iv) Lead rail: On stock side and turnout side; (v) Stock rail: On stock side and turnout side; (vi) Running rail: On stock side and turnout side

The results of the measurements are inspected by the unit chief. In the Wear Inspection File pertaining to turnouts and crossings, a labourer makes a note of the results of the measurements taken.

- Flaw inspection of turnout and crossing rails:

Two of the employees examine the tongue rail and bridge for any cracks or other damage. The results of the inspection are reviewed by the unit chief. The information concerning cracks and damage is entered into the record file by one of the workers.

- Measurement of joint clearance between tongue rail heel and rail/ between rail and crossing front end:

The joint clearance is measured by two of the personnel. The results of the measurements are inspected by the unit chief. One of the workers makes a record of the result of the measurement.

### **6.3.7 Inspection of Joints**

- Includes measurements of joint gap, inspection of joint conditions and joint parts. These checks have to be performed at least once every year on each and every segment of the main tracks, and at least once every year on each and every side track.
- The inspection of joint gaps has the goal of ensuring that there has been no rise or decrease in joint gap that exceeds a predetermined limit. During the joint condition examination, joint depressions, rail misalignment at joints, and unevenness in height at joints are all things that should be looked for. In addition, the condition of the joint bars and the joint bar bolts will be assessed during the inspection of the joint parts.
- The inspection is carried out by two workers simultaneously. The results of the inspection are reviewed by the unit chief. The findings of the inspections are recorded in the inspection record file by one of the personnel.
- Allowable error of measurement: Widen:  $< 10$  mm, Narrow: 0 mm.
- If any damage is found, the joint must be replaced immediately.

### **6.3.8 Inspection of sleeper**

- At the very least once a year, there should be an examination of the conditions of the sleepers in every section of the main tracks and the side tracks. This examination should check the distance between the sleepers and the positioning of the accessories. During the inspection of the sleeper sections, it is important to check that there are no fractures or other types of damage that could be harmful.

- The visual assessment of the sleepers is carried out by two workers. The results of the inspection are reviewed by the chief of the unit. One of the employees is responsible for updating the inspection record file with the findings of each inspection.
- In the event that any issues are discovered, the cross tie is required to be replaced without delay.

### **6.3.9 Inspection of fastening system**

- At the very least once a year, there should be an inspection of the conditions of the rail fastening system carried out in each and every section of the main tracks and side tracks. This inspection should examine the rail fastening system for looseness, loss, and any protruding track pads.
- A visual inspection of the fastening system is performed by two workers using a hammer and a wrench. In advance, make sure that the marking line that is supplied on the fastening device is checked.
- The results of the inspection are reviewed by the unit chief. One worker is responsible for updating the inspection record file with the results of each inspection.
- In the event that any issues are discovered, the securing mechanism will be changed.

### **6.3.10 Inspection of track bed**

- Due to the non-ballasted track, this inspection is not currently carried out for Metro Line 2A or Metro Line 3, but it will be in the near future when Metro Line 1 is in operation.
- At the very least once a year, there needs to be an inspection of the conditions of the ballast carried out in every single part of the main tracks and the side tracks. This is done to ensure that the cross section of the ballast sections is being maintained.
- The entire personnel of the unit is obligated to verify both the point where the curve first begins and the spot where the ballast track bed became unstable.
- The results of the inspection are reviewed by the unit chief. One of the workers is responsible for updating the inspection record file with the results of each inspection.
- In the event that any issues are discovered, the ballast track bed will be changed.

### **6.3.11 Inspection of train stop**

- Car stops on both the main tracks and the side tracks need to have their parts inspected at least once a year to guarantee that there are no cracks or other types of damage that could have an adverse effect on the car stops.
- The examination is carried out by every member of the personnel of the unit, and if any stained or damaged components are found, they are obligated to clean and restore those components.
- The results of the inspection are double checked and recorded by the unit chief.
- In the event that any issues are discovered, the parts of the train stop must be changed.

## 6.4 Track Repair Guidelines

### 6.4.1 Correction of alignment

#### Preparatory work:

The six-person group for the maintenance team is comprised of one supervisor and five subordinates.

Get the necessary instruments for the repairs ready, including specific measures, a dolly for construction inspection, a wrench, a hammer, a pen for marking the rail, a steel clearance gauge, string, measurement result records, and a flashlight..

Step 1: Measure the distance from the survey point on the stock rail side to the reference point.

- Set the survey point on the stock side rail. In a linear location and in the direction in which kilometrage increases, the stock rail shall be the left side rail. In the case of a curve, the stock rail shall be the outer rail.
- Measure the distance from the survey point to the reference point set on the structure (in this case, the structure is the beam of an elevated bridge). The reference point is set at the time of construction.

Step 2: Gauge Measurement. Gauge measurement range: Up to 15 m in the front-back direction including the work zone. The measurement is usually conducted at 5 m intervals in the alignment adjustment.

Step 3: Inspection of Structure gauge Position. In the curve, the alignment adjustment also changes the curve of the stock side rail, thereby changing the direction the train travels. Thus, the position of structure gauge is changed. Therefore, we must check the structure gauge position to secure the structure gauge. If we cannot observe the structure gauge, we must adjust the track.

Step 4: Inspection of Fastening System. Check that all parts of the fastening system are tight. Ensure that the bolts are not rusting. If any rust is seen, loosen the bolt once, lubricate it, and then tighten it again. Make sure the track pad position is not displaced. If displaced, return it to the original position.

Step 5: Inspection of Clearance between Joints. Inspection range is up to 50 m in the front-back direction including the work zone.

Step 6: Inspection of Bolts on Joint Bar. Inspect the bolts on the joint bar. If they have loosened, tighten them.

Step 7: Marking Travel Distance on Sleepers and Rails. In the alignment adjustment, the rail may be compressed both from outside and inside. Therefore, it is necessary to mark the compressed distance and direction on the stock side rail.

#### Actual repair work:

Step 1: Loosen the fastening system of the stock side rail.

Step 2: Install the gauge retention device to stably maintain the distance between the right and left rails.

Step 3: Adjustment of Alignment. Start the work from the location that requires the largest adjustment. Once adjustment at a location is completed, measure its alignment immediately. If the measurement result is acceptable, finish your work here and move to the next location to carry out alignment adjustment. The alignment adjustment must be continuously implemented until the work is completed.

Step 4: Permanent Tightening of Fastening System. After all alignment work is completed, tighten the fastening system of the stock side rail. Lubricate the bolts and prevent dust from being pinched by the bolts.

Step 5: Measurement of four items. Measure the four items (gauge, cross level, longitudinal level and alignment) in the work zone to ensure security.

### **6.4.2 Gauge adjustment**

#### Preparatory work:

The maintenance team of 6 staff includes one leader and five workers. Prepare repair tools including particular measure, wrench, hammer, steel clearance gauge, string, measurement result records, flashlight.

Step 1: Gauge Measurement. Excessively narrow or wide gauge can cause a train to derail. Normal survey point intervals in the gauge adjustment is 2.5 m. When there is a large variance in the measurement results at 2.5 m intervals, measure the gauge at each cross tie.

Step 2: Inspection of Fastening System. Examine that all parts of the fastening system are tight. Ensure that the bolts are not rusting. If any rust is seen, loosen the bolt once, lubricate it, and then tighten it again. Make sure the track pad position is not displaced. If displaced, return it to the original position.

Step 3: Measurement of Alignment. When adjusting the alignment and gauge at the same time, adjust the alignment first.

Step 4: Deciding Work Position. Decide the work position. Write the adjustment value on the rail head. Start the adjustment from the stock rail. In a linear location and in the direction in which kilometrage increases, the stock rail shall be the left side rail. In the case of a curve, the stock rail shall be the outer rail.

#### Actual repair work:

Step 1: Loosen the fastening system of the stock rail once, and then tighten it again.

Step 2: Loosen the fastening system on the opposite side of the stock rail rather than that of the stock rail.

Step 3: Adjustment of Position of Opposite Side Rail. Based on the adjustment value written on the stock rail, adjust the position of the opposite side rail.

Step 4: Permanent Tightening of Fastening System. After all alignment work is completed, tighten the fastening system of the opposite side rail. Lubricate the bolts and prevent dust from being pinched.

Step 5: Measurement of four items. Measure the four items (gauge, cross level, longitudinal level and alignment) in the work zone to ensure security.

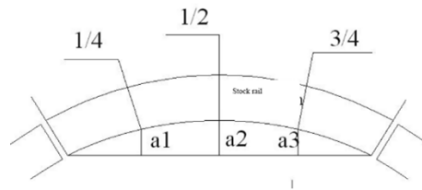
### **6.4.3 Rail Renewal**

#### Preparatory work:

The maintenance team of 6 staff includes one leader and five workers. Prepare repair tools including over-raise rail shifter, wrench, hammer, winch, measure, rail cutter, rail bending machine, rail supporting wedge, oil, steel clearance gauge, string, measurement result records, flashlight.

Step 1: Measurement of Length of Replaced Rail. When measuring the length of a replaced rail, measure it in the head of the rail using a measure. Two workers who engage in the measurement shall pull both ends of the measure. Measure the rail length a minimum of two times. The error in the above measurement must be 2 mm maximum. If the error is 2 mm or greater, you must repeat the measurement. This work is carried out at night.

Step 2: Measure the offset. Offset must be measured at each of 1/4, 1/2 and 3/4 point.



**Figure 42** Offset measured at the positions of 1/4, 1/2 and 3/4 (a1, a2 and a3).

Step 3: Measurement of Cross-section. Measure the joint clearance of the joint at the start and end points of the rail. Measure the discrepancy and unevenness between the start and end points. Discrepancy denotes the difference in the cross direction between two rails at the end points. Unevenness means the difference between two rails in the vertical direction.

Step 4: Measurement of New Rail. Measure the length of a new rail in its head. - Measure the length a minimum of two times. The error shall be 2 mm maximum.

Step 5: Cutting and Chamfering of Rail. Cut the rail using the rail cutter. 2 mm of the end shall be chamfered at an angle of 45 degrees.

Step 6: Drilling of Rail Joint. Drill a hole on the joint of new rail using the rail driller. Chamfer 2 mm wide area of the joint hole at an angle of 45 degrees.

Step 7: Setting of Bending of New Rail. Bend the new rail at each of 1/4, 1/2 and 3/4 point according to the offset specified in Step 2. Caution: When the radius of the rail is less than 600 m, use the bending machine for bending. Bend the rail to about 2/3 of the offset specified in Clause 1.2 of this article. Exercise care not to bend it excessively. When the curve radius is more than 600 m and less than 800 m, bend the rail within 5 m from the end.

Step 8: Installation of Rail Supporting Wedge. Install a rail supporting wedge in order to temporarily place the new rail. After bending the rail at Depot, move it to the rail replacement position during the preparation period. Place the rail outside the track so as not to affect the ballast track bed. Place the rail on the supporting wedge while exercising care not to affect the current bending of the rail. The supporting wedge is made of used, old sleepers. Arrange the pins on the supporting wedge that are used for fixing the rail.

Step 9: When replacing two or more rails, must set the joint clearance of the joints. Setting an appropriate joint clearance of the joint, and fasten the joint bolts for connecting the rails. In this case, be sure to insert the inner and outer bolts alternately.

Step 10: Measure the length of the connected rails. Measure the length in the head of the rail. Measure the length two or more times. Measurement error shall be 2 mm maximum.

Step 11: Decide Installation Position of Over-raise Rail Shifter. Check the position where the over-raise rail shifter is installed. Decide the position of the over-raise rail shifter in such a way that it can lift a long rail at three points and a short rail at one or two points. Place the supporting wedge of the over-raise rail shifter temporarily in the installation position.

#### Actual work:

Step 1: Removal of Rail Joint: On the day of replacement, remove the joints of the rail included in the replacement zone.

Step 2: Removal of Fastening System. Remove the fastening system included in the replacement zone. Exercise care not to pinch any dust. When removing it, also remove 10 m of adjacent rail. Reason: Axial force settles on the older rail. After the fastening system is removed, that axial force is removed, too.

Step 3: Installation Over-raise Rail Shifter

Step 4: Lifting of Rail. Use the over-raise rail shifter when lifting the replaced rail. Do not lift the rail unnecessarily high.

Step 5: Check of Track Pad. Check that the track pad is set in an appropriate position. When replacing the track pad, replace it using this opportunity.

Step 6: Setting a New Rail. Use the over-raise rail shifter when lifting the new rail. Do not lift the rail unnecessarily high.

Step 7: Adjustment of Joint Clearance of Rails. If the joint clearance of the rail is insufficient, move the rail slightly. Pinch the rail in a position slightly away from the position where it was pinched before, and then lift and move the rail.

Step 8: Temporary Tightening of Joint Bar Bolts. After the rail is set in the correct position, tighten the joint bar bolts temporarily. Insert the inner bolts and outer bolts alternately. Lubricate them, and check whether any dust is on the joint bar.

Step 9: Move of Replaced Rail to Supporting Wedge

Step 10: Remove the over-raise rail shifter.

Step 11: Tighten the joint and fastening system.

Step 12: Measure four items (gauge, cross level, longitudinal level, alignment) in the work zone to ensure security.

#### **6.4.4 Sleeper renewal**

##### Preparatory work:

The maintenance team of 6 staff includes one leader and five workers. Prepare repair tools including tamping, wrench, hammer, winch, measure, tool for solidifying the concrete, concrete breaker, shovel, oil, steel clearance gauge, string, measurement result records.

Step 1: Apply a mark to the sleepers to be replaced. Exercise care not to replace multiple cross tie at the same time.

Step 2: Move new sleepers to the temporary storage space.

Step 3: Check the fastening system, then lubricate and tighten it.

Step 4: If the space between the sleepers is not appropriate or if sleepers are not at right angles to the centerline of the track, adjust the sleepers beforehand.

##### Actual repair work:

Step 1: Scrape out the ballast or break up the concrete beforehand.

Step 2: Remove the fastening system of the replaced sleepers.

Step 3: Remove the sleepers to be replaced. When ballast is used, rake the ballast.

Step 4: Insert new sleepers. As a general rule, the center of a cross tie must be aligned with the centerline of the track. Caution: In the case of a curve, the track centerline is located at a position  $717.5 (=1435/2)$  mm away from the stock rail (outer rail).

Step 5: Tighten the fastening system of the new cross tie temporarily. Tighten it temporarily after checking that the space between the adjacent cross tie and the cross tie is at a right angle to the track centerline. Then lubricate the bolts.

Step 6: Lay out ballast temporarily (if necessary).

Step 7: Permanent Tightening of Fastening System

Step 8: Tamping down the ballast

Step 9: Level the ballast surface uniformly.

Step 10: Measure four items (gauge, cross level, longitudinal level, alignment) in the work zone to ensure security.



## **6.5 Civil structure Inspection methods**

### **6.5.1 Appearance inspection of viaducts and tunnels - Monthly**

3 time per months.

Inspection tools: Flashlight, inspection hammers, air whistle, binoculars. Inspection staff assignment: Person in charge of inspection Unit chief: 1 person, be responsible for inspection results. People in charge of inspection Staff: 2 people.

1. Each member of the staff is required to walk in the opposite direction that the train is going in when they are on duty. Members of the crew are required to walk in the direction that is opposite to the one that the train is going in. Halfway through a bridge or tunnel is the range that can be verified by the staff in a single observation.
2. Each member of the staff is required to maintain a reasonable walking pace.
3. The Unit chief and the Staff are responsible for identifying problematic sections that have a negative impact on the movement of the train while the inspection is taking place.
4. The Unit Chief is responsible for determining whether or not such sections are defective according to the Defect Judgment Criteria, as well as determining when such sections will be repaired.
5. If there are any questions regarding a spot that has already been inspected, the Unit chief and the Staff must recheck it by moving in closer to it using a ladder or another tool designed for working at high elevations. Alternately, they have the option of observing the conditions of the area under suspicion while the train is in motion.
6. If a piece that has a very serious flaw is found, the Unit chief in charge is required to issue an instruction to promptly stop the train.
7. Given that the inspection will take place within the regular time period that the train is in service, there will only be one inspection. Every member of the staff is responsible for keeping a vigilant eye for oncoming trains. Because he is responsible for recognising any incoming trains, this member of the staff is required to walk 20 to 40 metres in front of the Unit Head and the other members of the staff.
8. In the event that a train is on its way, this member of the staff is obligated to alert the Unit chief and the Staff by using an air whistle. Whenever the air whistle is sounded, the Unit chief and the Staff are required to momentarily halt the inspection.
9. The staff is required to provide a detailed description of pertinent information regarding defective areas on the Inspection Record. (Photographs are to be taken at appropriate times)

### **6.5.2 Appearance inspection of viaducts and tunnels - Yearly**

Once time/2 years

Inspection tools: Flashlight, binoculars, inspection hammers, ladder, tools for high-elevation work. Person in charge of inspection Unit chief: 1 person, be responsible for inspection results. People in charge of inspection Staff: 2 people.

1. Each member of the staff is required to stroll at a relaxed pace.
2. The Unit chief and the Staff are responsible for locating defective components (cracks, water leakages, exposed re-inforcing plates, and so on) that have a negative impact on the movement of the train.
3. The chief of the unit is the one who is responsible for determining whether or not such components are defective according to the Defect Judgment Criteria, and also determining when they will be repaired.

4. If there are still questions regarding a section that has already been inspected, the team needs to double check it by moving in closer using a ladder or another instrument designed for working at high elevations.
5. The Unit commander in charge is responsible for issuing an instruction to promptly stop the train whenever a piece that has a very serious flaw is discovered.
6. The staff is required to provide a comprehensive description of material pertinent to defective areas within the Inspection Record. (Photographs are to be taken at appropriate times)

### **6.5.3 Appearance inspection of tunnels – Ten-yearly**

Once time/10 years

Inspection tools: Flashlight, binoculars, inspection hammers, ladder, tools for high-elevation work. Person in charge of inspection Unit chief: 1 person, be re-sponsible for inspection results. People in charge of inspection Staff: 2 people.

1. The Unit chief and Staff are responsible for locating defective components (cracks, water leakages, exposed re-inforcing plates, etc.) close to a structure that has a negative impact on the movement of trains.
2. The chief of the unit is the one who is responsible for determining whether or not such sections are defective according to the Defect Judgment Criteria, as well as determining when they will be repaired.
3. The Unit head in charge is responsible for issuing an instruction to promptly stop the train whenever a piece that has a very serious flaw is discovered.
4. The staff is required to provide a detailed description of pertinent information regarding defective areas on the Inspection Record. (Photographs will be taken according to the requirements.)
5. When the unit chief and the staff began the job, the driver of the inspection car was required to put a stop to the tool that was being used for high-elevation work.

### **6.5.4 Buildings appearance and building equipment inspection**

Once time to three times /year

Inspection tools: Flashlight, binoculars, inspection hammers, ladder, tools for high-elevation work, Inspection tools appropriate for the target equipment must be used. Person in charge of inspection Unit chief: 1 person, be re-sponsible for inspection results. People in charge of inspection Staff: 2 people.

1. Unit chief and Staff must detect defective portions (cracks, water leakage, stains, etc.) that adversely affect the durability of buildings.

Unit chief and Staff shall inspect whether each item of equipment meets the specified function criteria as in the following: (i) Door: Check it for cracks and breakages. Staff members must make sure there are no problems opening and closing the door. (ii) Water pipe system: Staff members must check whether the system operates normally when a faucet is opened. They must also check the system for water leaks and flooding of the lower levels. (iii) Staff members must make sure that disaster-prevention signs and regulation indication boards are set in the specified positions. (iv) The staff member makes sure that evacuees can get to the basement via the emergency stairs. (v) The staff member checks that the fire-fighting system equipment operate as specified. (vi) Electric pump, diesel pump, water supply system for firefighting, automatic fire alarm system (smoke and temperature detection tools, sprinklers, etc.). (vii) The staff member checks that the exhaust and ventilation systems operate as specified; (viii) Lightning protection system: Lightning rod, grounding wires, earth resistance measurement system, etc. are checked to ensure they are operating normally.

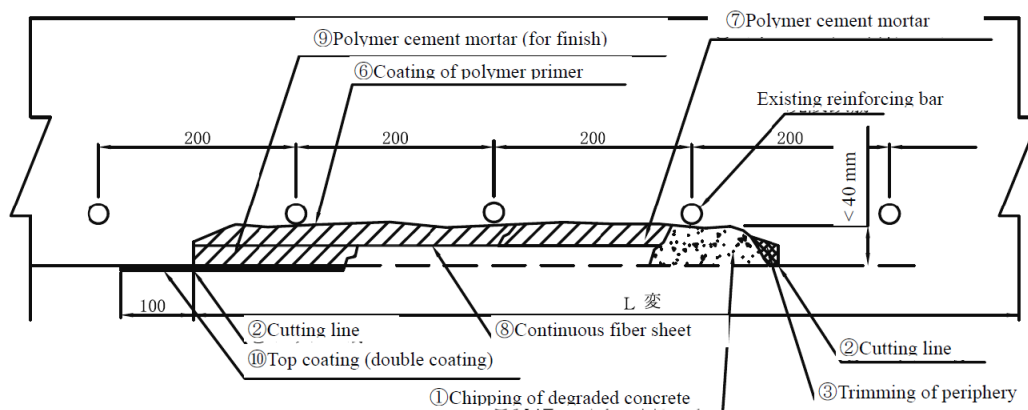
2. Unit chief must responsibly judge such portions as defective according to the Defect Judgment Criteria, and also decide their repair timing.
3. If suspicions remain about an already inspected portion, Unit chief and Staff shall check it again by getting closer to it using a ladder or other tool for high-elevation work.
4. When a portion with a very serious defect is detected, Unit chief in charge shall issue an instruction to stop using the building or equipment.
5. Staff shall describe information relevant to defective portions in detail on the Inspection Record. (Photos shall be taken as needed.)
- 6.

## 6.6 Civil structure Repair methods

### 6.6.1 Viaducts

The deterioration-related phenomena of falling concrete surfaces owing to corrosion of reinforcing bars within reinforced concrete are frequently observed on viaducts. From a design aspect, the falling surface side of the concrete is the piece that does not have to support the created stress. As a result, the repair strategy should take the following factors into account: (i) A sufficiently alkaline environment must be provided in the periphery of reinforcing bars to prevent any further corrosion; (ii) Repair materials must be closely adhered to the base material to prevent falling again.

Polymer cement mortar is an ideal repair medium for safeguarding reinforcing bars because it keeps a sufficient amount of alkalinity, adheres well to the base material, and also has great waterproof qualities. As a result, it is recommended that polymer cement mortar be used to rebuild viaducts. When the depth of the repair requires a substantial amount of polymer cement mortar, it can cure in layers during the repair. A continuous fibre sheet is occasionally put between the upper and bottom layers to avoid such difficulties. The results in a decrease in the adherence of polymer cement mortar layers.



**Figure 43** General Drawing of Repair of Elevated Concrete Bridge

(Source: Maintenance Manual, JICA 2015)

### 6.6.2 Open-cut tunnel

Firstly, several fractures are generated by the drying contraction of tunnel lining concrete, while others occur as a result of tunnel lining deformation caused by the action of tunnel loads (biased pressure or changes in load conditions, etc.). Allowing cracking to proceed will eventually result in the peeling and separation of lining surfaces, resulting in the destruction of tunnels. Additionally, irregularity is likely to occur in areas of intense stress or when lining

joints, for example. As with typical concrete buildings, it is vital to monitor the cracking process. Due to the small or non-existent clearance between the outer edges of rolling stock and the inner sides of tunnels, concrete separation and displacement of tunnel bodies quickly impair train operation safety, necessitating caution. Secondly, water leakage from the tunnel's back is a common degradation event in open-cut tunnels. Not only is a tunnel always susceptible to earth pressure, but it is also subject to water pressure if it is built below groundwater level. Although a tunnel is designed to withstand the assumed pressure and is constructed with great care, some anomalies caused by building operations are unavoidable. Then, water with a high flow property flows inside the tunnel under the influence of water pressure from the locations that are vulnerable to pressure. Because of the reinforced concrete (RC) structure of a tunnel, the reinforcing bars must be protected against corrosion. When exposed to water and air, reinforced bars corrode. Water leakage produces an environment in a tunnel that corrodes the reinforcing bars. As a consequence, we must eliminate this source of deterioration. It is essential to choose a repair technique and take care these factors:

- In order to protect reinforcing bars from being exposed to water, we need to inject water-stop materials into cracks positioned below reinforcing bars.
- A sufficiently alkaline environment must be provided in the periphery of reinforcing bars to prevent them from corroding further.

Polymer cement mortar maintains an adequate level of alkalinity, has great adherence to the foundation material, and also has excellent waterproofing qualities. Thus, after verifying that the water-stop material is properly preventing water from entering, we make a groove with polymer cement mortar to bury the seal material and complete the water-stop effect with epoxy resin sealing material.

### **6.6.3 Repair of structure**

Repair tools: hammer, chisel, concrete cutter, steel brush, inspection hammer, ladder, tools for high-elevation work (as needed). Materials: Polymer-based primer, Polymer cement-based mortar, Aramid continuous fiber sheet. Repair staff assignment: Unit chief: 1 person responsible for inspection, Staff: 3 people. Repair procedure

1. Staff shall decide on the repair location by cleaning the place with a steel brush. If the side face of the repair location is protruding, Staff shall cut it off using the concrete cutter.
2. If reinforcing bars are exposed, Staff shall process the rusted portions using the steel brush, and apply rust inhibitor to them.
3. Unit chief shall check that the above repair location coincides with the inspection result and the maintenance plan.
4. After 3) above, Staff shall clean the repair location using water.
5. After 4) above, Staff shall apply polymer-based primer to the repair location.
6. After polymer-based primer is dried, Staff shall fill the repair location with polymer-based mortar (1st layer). At this point, polymer cement-based mortar must be evenly filled in and adhered to the base metal.
7. After 6) above, Staff shall set the continuous fiber sheet on the first layer.
8. After 7) above, Staff shall fill the continuous fiber sheet with polymer cement-based mortar (2nd layer).
9. Finally, Unit chief shall check that polymer cement-based mortar has adhered firmly to the base material.

## 7. SAFETY SOLUTIONS FOR OPERATED LINE - INCIDENT MANAGEMENT PROCESS

### 7.1 Incident Management Purpose and Scope

The aim of this Procedure is to inform HanoiMetro staff of the procedures to be followed in the event of an incident involving an item of operating rolling stock. The following is the general principle for handling incidents:

- Thoroughly safeguard the safety of people and property and respond appropriately and quickly.
- In the accident, the organisations and people involved in the urban railway are responsible for resolving the incident cooperatively.
- Evacuees should be rescued urgently, and the incident site, national property, and evacuees should all be protected.
- Notify and report an accident in a reasonable timeframe to the appropriate organisations and individuals.
- All organisations and personnel notified of the accident must immediately report to the situation and take appropriate action.
- Reopen the affected line to train traffic as soon as possible. Make an attempt to operate trains according to the timetable.
- Prevent the recurrence of the accident by taking preventative steps.

The next sections of this chapter detail the accident response procedure, including the organisation of the Task Forces team and instructions on the duties of Hanoi Metro sections in an accident. This is followed by the processes for repairing and inspecting vehicles, equipment, and infrastructure prior to returning operation.

Additionally, an accident inspection is undertaken immediately following the occurrence of the accident, and notification of the appropriate authorities as well as a media release is required for serious accidents.

Generally, the type of accidents and incidents in HanoiMetro Company are summarised and divided into two general severity category as in following:

Class A accidents:

- A collision between rolling stock.
- A collision between rolling stock and people.
- The derailment of rolling stock.
- A violation of the network regulations for rail infrastructure management.
- Disaster: mainly includes natural disasters such as strong storms, tornadoes, hail, thunderstorms, floods, earthquakes, mountain landslides, landslides, etc. constitutes or may cause railway traffic to flood, derail or tip over, etc.
- Social safety events: Mainly covers terrorist attacks, major criminal cases (bomb threat, toxic gas threat, train robbery (passenger), arson, destructive explosion), toxic chemical leak, radioactive pollution, mass concentration of people causing trouble in urban railway stations.
- Fires and explosions on train or in the station leading to passenger panic.

Class B accidents:

- A derailment, other than a running line derailment.
- A collision involving rolling stock, other than a collision described in Class A.
- The passing of a stop signal, or a signal with no indication, by rolling stock without authority.

- An accident or incident where rolling stock exceeds the limits of authorised movement given in a proceed authority.
- A failure of signalling or communications system that endangers, or that has the potential to endanger, the safe operation of trains or the safety of people, or to cause damage to adjoining property.
- Any slip, trip or fall by a person on railway premises.
- A person being caught in the door of any rolling stock.
- A person suffering from an electric shock directly associated with railway operations.
- An accident or incident involving dangerous goods that affects, or could affect, the safety of railway operations or the safety of people, or cause damage to property.
- Any breach of a network rule, other than described in Class A.
- Any breach of the work scheduling practices and procedures set out in the rail transport operator's fatigue risk management program.
- Any violation of Drug and Alcohol usage regulation.
- The detection of an irregularity in any rail infrastructure (including electrical infrastructure) that could affect the safety of railway operations or the safety of people.
- Minor fire and explosion event.

Based on this classification, the investigation level and notification level of an accident/incident occurred in HanoiMetro Company are recommended by Safety Department and decided by Manager Responsible for Safety as in the table 7.1:

The Investigation Team Leader will collaborate with members of the Task Force and the Safety Department to formulate standards for data collecting and associated investigation processes. The Investigation Team Leader will collaborate closely with the appropriate Maintenance Center in order to conduct the investigation process and its associated consequences.

**Table 7.1** investigation level and notification level of an accident/incident

| Severity Class    | Incident Type Description   | Level of Investigation   | Level of Notification  |
|-------------------|---|--|--|
| Level 1 – Class A | A significant event that generates intense public interest.<br>Normally, a catastrophic accident occurs that results in considerable property damage or a large number of casualties.<br>Over 10 deaths or over 50 injuries or economical loss over 10 bil. VND | The inspection is conducted by highly experienced independent investigators from National Traffic Safety Board and Ministry of Transport. Supervised by National Safety Board. | National Traffic Safety Board.<br>Ministry of Transport.<br>Hanoi Authorities. |
| Level 2 – Class A | A serious incident that is unlikely to draw widespread public awareness but results in severe property damage or casualties.<br>3-10 deaths or 20-50 injuries or 3-10 bil. VND loss.  | The inspection is conducted by investigators from the Ministry of Transport. The investigation is supervised by National Traffic Safety Board                                  | National Traffic Safety Board.<br>Ministry of Transport.                       |
| Level 3 – Class A | In addition to Class A, a significant incident that has a significant effect on railway operations.<br>1-3 deaths or 10-20 injuries or 1-3 bil. VND economical loss.  | The inspection is conducted by Hanoi Department of Transport and supervised by the Ministry of Transport.  | Ministry of Transport.<br>Hanoi Authorities.                                   |

|                      |  |  |  |
|----------------------|--|--|--|
| Level 4 -<br>Class B | A class B accident/ incident which had the potential to be more serious had circumstances been only slightly different.<br>5-10 injuries or economical loss between 500mil. To 1 bil.VND | The inspection is conducted by Department of Safety and supervised by Hanoi Department of Transport.           | Hanoi Department of Transport.                             |
| Level 5 -<br>Class B | A class B accident/ incident which although reportable had a low potential for serious outcomes.<br>Under 5 injuries or economical loss between 100 - 500 mil. VND                       | The internal inspection is conducted by Department of Safety and supervised by Manager Responsible for Safety. | Hanoi Department of Transport.<br>Head quarter of Company. |
| Level 6 -<br>Class B | An occurrence of minor consequence<br><br>No injuries or economical los under 100 mil. VND   | The internal inspection is conducted by responsible Maintenance Centre and supervised by Department of Safety. | Manager Responsible for Safety.                            |

## 7.2 The general procedure and guidelines for accident responding

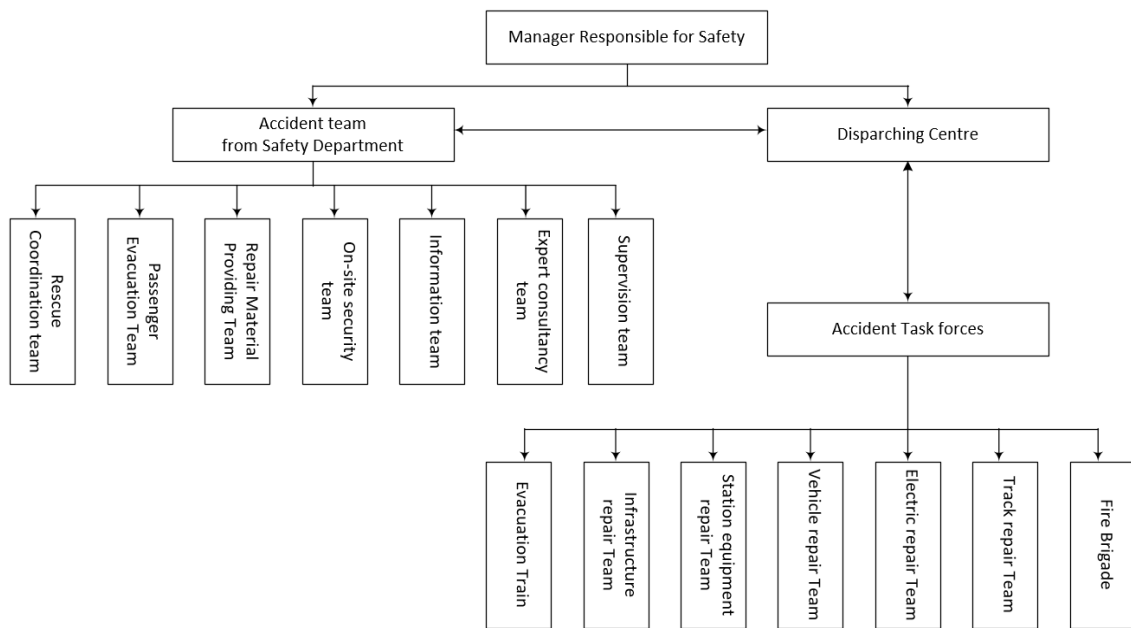
### 7.2.1 Accident Treatment Structure

Manager Responsible for Safety:

- Conduct research, make decisions, and organise work to respond to problems that occur inside the company's operations, establish and perfect the emergency response mechanism, operate, prepare, or respond to emergencies, and maintain a professional emergency rescue team.
- Monitor the performance of the company's emergency response system and, in reaction to changes in the operating environment, continue to develop the system;
- Overall organisation, command, management, response to operational problems, decision-making, and general regulation.
- While investigating and responding to occurrences, it is necessary to maintain communication with appropriate ministries, agencies, and senior management units.
- Responsibilities include arranging or cooperating with supervisors to conduct investigations, evaluate data, and enhance work for incident post-processing.

Accident Team from Safety Department:

- Accident team is the incident's command centre, located in a safe place near the scene of the incident.
- Specifically, responsible for directing and managing the event site while also supervising the rescue coordination activities;
- Responsible for facilitating an efficient flow of information on the scene of the event;
- The master plan for coordinating emergency response work, the general regulation team, the technical expert team, the emergency response monitoring team, the logistics assurance team, the resource assurance team, and the rescue and care team.
- Logistics and information-gathering;
- Organize or contract emergency response activities with higher organisations such as government departments, agencies, and so on.



**Figure 44** Accident Treatment Structure

Task force on accident site:

- If the accident is caused by a breakdown of rolling stock, the Task force's chief is the Head of the Vehicle Maintenance Centre. For other types of incidents, the Task Force is commanded by the Head of the Station Center which controlled the track segment where the accident occurred.
- Responsible for the overall supervision of equipment rescue operations on the scene of the disaster;
- Coordination of technical teams, handling incidents according to each team's tasks.
- Supervise emergency responders as they attempt to reclaim the site.
- Create a strategy for rescuing equipment while also carrying out the rescue under the unified leadership of the person in charge of rescue;
- Conduct thorough equipment inspections before to resuming operation, testing work, and clearing the route, among other things.
- Arrange or assist higher authorities within government ministries in their incident response activities.

Dispatching Centre:

- Prior to the establishment of the Accident Treatment Structure, the Dispatching Center functioned as the emergency command centre, beginning the emergency response plan, arranging the emergency responders to send in the rescue task, and confirming the action situation.
- The Dispatching Center serves as the focal point for incident information transmission, collecting and disseminating incident data, detecting and verifying incident data in a fast and accurate manner, generalising the incident, and making preliminary judgements regarding the incident's severity. impact, the most effective method of entering the rescue site.
- Maintain close communication to the emergency response organization's structure, stations, trains, and parts of trains throughout the emergency response process.



- Report swiftly to the leader, the superior external unit in charge of reporting, validating news, reporting, and disseminating information to the agency, based on the severity of the occurrence and the difficult nature of the issue. High command structure for emergency response.
- Organise and organise the company's departments to assist in incident response during an emergency;
- Assess the impact of the incident on the whole operation based on the status of emergency response and rescue, while organising to produce an operation adjustment plan.

## 7.2.2 The procedure of warning classification and information reporting

### Principle of information reporting

- Need for timely, accurate, comprehensive, and decentralised reporting. Any employee who finds or learns of an event shall promptly and without delay, interruption, or omission, follow the established notification process.
- Internal notifications of confirmed information are made first by managers, followed by leaders of the Maintenance Centre and Safety Department, and then group information.
- Report extremely significant occurrences (complex circumstances) using the concept of concurrent notification to the Manager Responsible for Safety, the Accident Team and Task Force, the Hanoi Metro headquarters, and the government rescue agency.
- For the time being, the event scene is difficult to judge; it might be reported on the scene scenario first, then confirmed and prepared to report. If an error is discovered in the report's content, it should be remedied quickly.
- If the train is delayed by more than 8 minutes or needs to adjust the time of the first train, the Dispatching Center and the Station Center need to notify passengers through the loudspeaker of the delay or adjustment within 10 minutes. If it is expected that it will be difficult to restore the normal operating sequence in a short time, relevant information should be published continuously.
- The procedure of warning and report process is clarified in Figure 46.

### Class V – White warning

- Estimated accident damage (as in Table 7.1): Level 5.
- Leading to operating interruption or station closure over 30 mins.
- It is necessary to mobilise technical support of many units.
- Head of Dispatching Centre approved warnings or remove warnings.

### Class IV – Green warning

- Estimated accident damage (as in Table 7.1): Level 4.
- Incidents tend to be extensive, can level up warnings.
- Manager Responsible for Operation approved warnings or remove warnings.

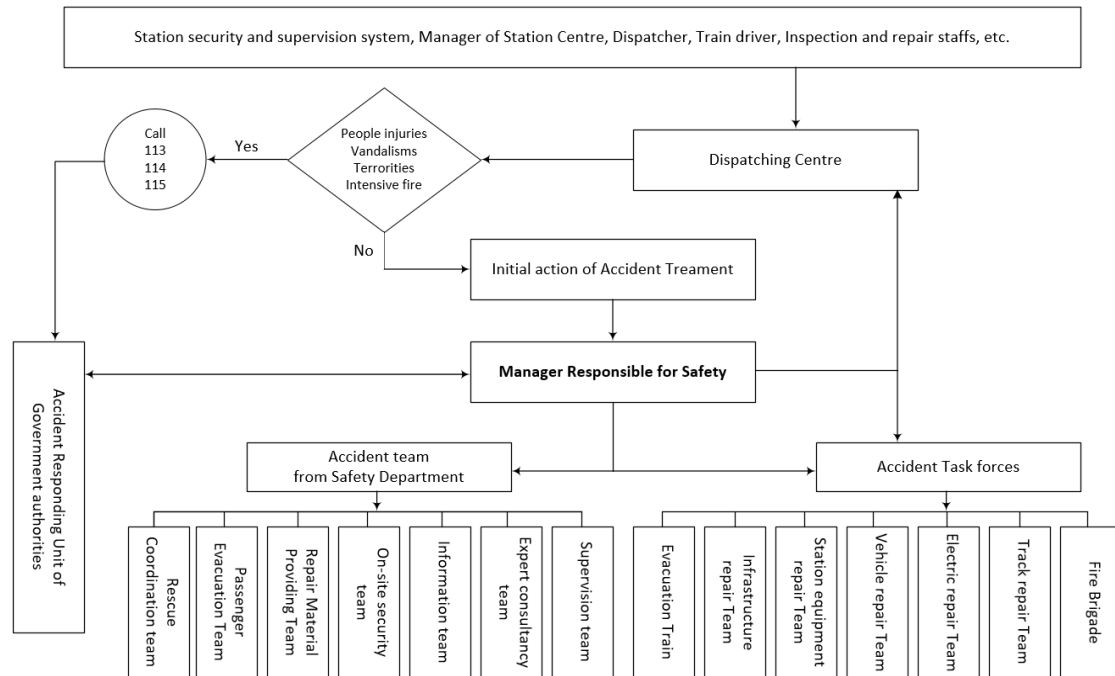
### Class III – Yellow warning.

- Estimated accident damage (as in Table 7.1): Level 3.
- Incidents tend to be extensive, can level up warnings.
- Higher authorities announced yellow warnings. Dispatching centre directly publishes corresponding information.

### Class II – Orange warning

- Estimated accident damage (as in Table 7.1): Level 2.
- A huge traffic incident occurred, the status of the incident gradually expanded, causing panic among the public.

- Higher authorities announced orange warnings. Dispatching centre directly publishes corresponding information.



**Figure 45** Classification of warning

#### Class I – Red warning

- Estimated accident damage (as in Table 7.1): Level 1.
- A special serious traffic incident occurred, the status of the incident gradually expanded and prolonged, causing panic among the public. Government directly supervises incident handling and investigation.
- Higher authorities announced red warnings. Dispatching centre directly publishes corresponding information.

### 7.2.3 The general procedure of Accident Responding

**Step 1:** After receiving the report or confirming the occurrence of an accident

Dispatching Centre:

- Dispatchers must quickly implement the backup plan or instructions for dealing with the crisis and notify higher authorities.
- Immediately organise the on-site personnel, including train drivers, station personnel, and station repair personnel, in accordance with the backup plan or troubleshooting instructions to proceed.
- Conduct an internal investigation and notify the government rescue department immediately following the notification process.
- Notify the appropriate rescue team of your intention to depart and confirm your departure situation.
- When a train is impacted, quick changes should be made to the train.
- Notify train drivers and the Vehicle Maintenance Center to prepare adequately for the departure of the rescue technical ship, while also organising a technical team to the scene.

- When the train is interrupted, the Dispatching Center collaborates with the rescuer to plan the related emergency.

**Maintenance Centres:**

- Following notification of the warning, member organisations assigned to the Task force quickly report to the gathering site and carry rescue and communication equipment to the scene.
- Organise more personnel to the location based on the magnitude of the issue.
- Inform the Dispatching Centre of the internal announcement and the rescue team's departure.

**Other departments and Centres:**

- Depending on the severity of the situation, functional departments mobilise personnel within the department to respond promptly to the site in accordance with the provisions of the emergency rescue system framework.
- When an employee sustains an injury to his or her body, the Staff and Service Management Centre and the Safety Department mobilise personnel to the site.

**Step 2:** Response sequence of department members of the Accident Team and Task force arriving after arriving at the scene

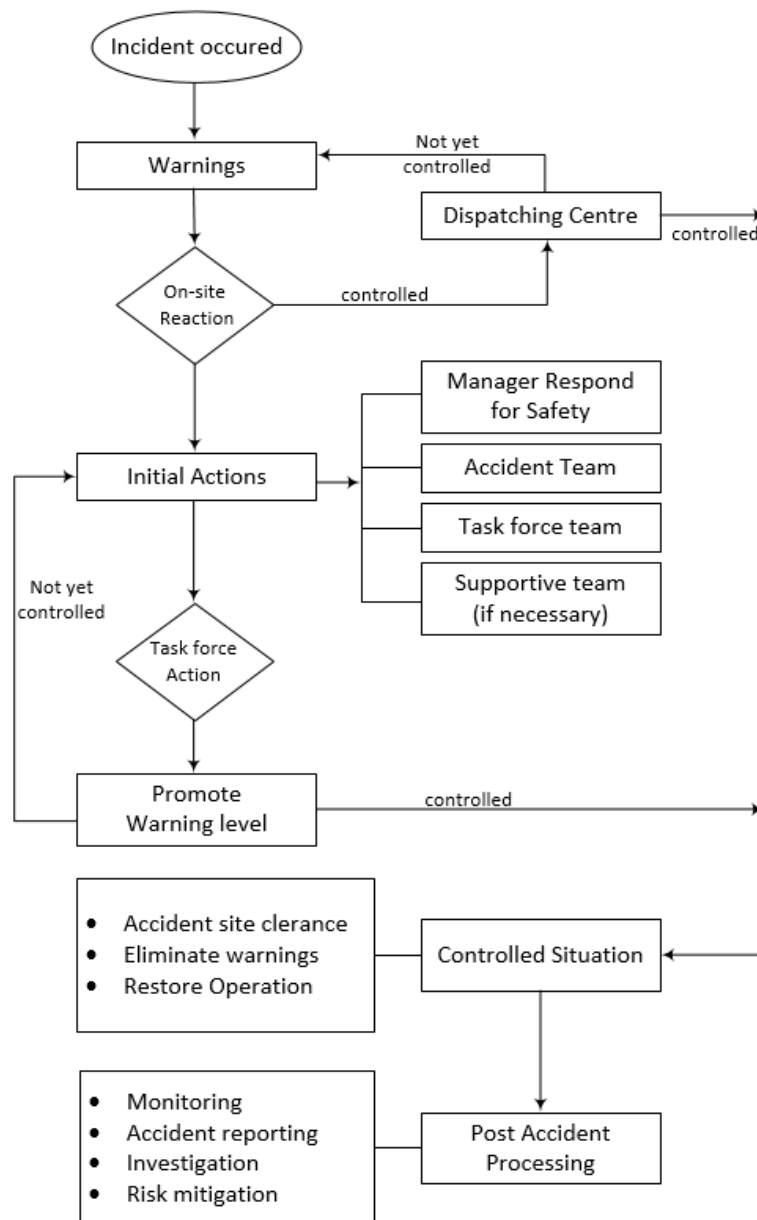
- If the scene has not been evacuated, through Dispatching Center approval, rescue workers can carry out preparatory work such as confirming the accident situation.
- When the Task Force arrived on the site, it quickly communicated with the Accident Team to establish and promptly implement the following tasks:
  - Arrange the site inspection, prepare a rescue plan, and submit it for approval to the site manager.
  - Clearly describe the rescue unit responsibilities.
  - Appoint a person to be responsible for safety supervision during the rescue.
  - Appoint a contact for communication with the Dispatching Center.
  - Implement rescue efforts.
- The Task Force leader must provide a contact method (complete name, hand-held radio, or mobile phone number) to the Dispatching Center and must continually communicate critical rescue steps to the Dispatching Center.
- If the incident is difficult and requires over than two sections to resolve, the rescue teams are not permitted to enter the rescue and move the scene on their own before defining the rescue strategy.
- The Task force leader coordinates and executes the rescue strategy. Emergency rescue operations are carried out by rescue teams in accordance with the assigned rescue plan, which is carried out by the team leader, and other team members are not permitted to command rescue activities on behalf of the person leading the rescue operation.
- Changing the rescue plan requires the Manager Responsible for Safety's approval.
- When field personnel identify a rescue operation scene posing a danger to persons, rolling stocks or equipment safety, they have the obligation to halt field activities and immediately contact the Task force leader. Stop the rescue scenario and organise the processing in accordance with the applicable task order.
- At the scene of a mass death or collective injury, all departments are responsible for protecting the scene and ensuring that associated situations are handled in accordance with applicable laws and regulations.

**Step 3:** Information reporting and warning setting

- Consistent, accurate, and timely disclosure of information about the development of operational events and emergency response activity is required. Reporting and

publishing news, incident management by the PR unit in compliance with applicable operating business standards, universally reported and publicised.

- The disclosure of information primarily consists of the following: the fundamental state of emergency response management, the actions and effectiveness of emergency response management.
- Evaluate the success of rescue efforts, the situation's degree of control, and, if required, raise the warning level and provide the supportive force.



**Figure 46** The general procedure of accident responding

**Step 4:** Finishing the emergency reaction.

The Dispatching Center notifies the components to resume regular operation following the conclusion of emergency response procedures when:

- the accident / incident scene has been controlled,
- the environment has been restored to compliance with applicable standards,
- the risk of a secondary incident has been eliminated,

- the transformation has been completed with the confirmation and approval of the field command,
- and the Task force has completed its job of managing the emergency response on the scene.

**Step 5:** Post-accident processing

- Monitoring: Maintenance Centers undertake periodic patrols using field and specialised monitoring methods in conjunction with ongoing inspection and monitoring of the impacted region.
- Accident reporting: Report of accident/incident site investigation and rescue needs to be submitted to Manager Responsible for Safety within 12 hours after accident. Assessment report of Accident Treatment needs to be submitted to Hanoi Metro Headquarter and Government authorities within one weeks after accident.
- Investigation: Organise or coordinate inquiry work in accordance with applicable laws, regulations, rules, and regulations. The company's incident investigation team works by summarising, assessing, and making recommendations for improvement, which are then applied by the appropriate department in charge of implementation, while also monitoring failure solutions.
- Risk mitigation: Technical specialists responsible for conducting technical analyses, providing technical assistance, and issuing risk mitigation instructions.

## **7.3 The accident responding procedure relating to Rolling Stocks**

### **7.3.1 The procedure of Initial Action responding to the accidents:**

The accident is promptly reported to the currently controlled Station Centre Management and the Dispatching Centre, Station Management Department, the Safety Department, the Construction and Maintenance Department, the Vehicle Maintenance Centre, and the Driver Training Centre respectively.

Operators who have received appropriate emergency response training act in compliance with the applicable regulations and procedures for the rail infrastructure on which they are operating at the time of the incident.

The manager of each workplace must emphasize to their maintenance employees the serious importance of speed in order to avoid significant problems caused by delays.

The Vehicle Maintenance Centre's personnel shall collaborate with Station Center Management and other personnel to determine the appropriate response to guarantee the safety of passengers and personnel, with special emphasis on the following critical contents:

- To rescue and evacuate the passengers and maintenance personnel.
- To ensure their own safety and that of other maintenance personnel.
- To prevent disasters and collateral accidents.
- To report and inform the accident.
- To safeguard the property.
- Other important matters
- The maintenance personnel must wear gloves when engaging in inspections, rescue and restoration.

When an accident occurs, the on-duty personnel responsible for the accident shall, in response to requests from the Dispatching Centre (OCC), either rush to the scene to collect pertinent information or dispatch inspection personnel to the scene and have them report

on the accident's status to the Head of Vehicle Maintenance Centre. The supervisor assigned to the incident, the Head of the Vehicle Maintenance Center, or other designated staff as defined in the duty regulations shall rush to the incident location with emergency machinery and materials.

The head of the Track Department, the Signalling Department, the Power Department, and the Engineering Maintenance Center must prepare essential emergency machinery and materials in advance, taking into account the line's specifications and operations. When notified of an accident or a request for assistance, all departments and staff shall respond as quickly and efficiently as possible and communicate the results to the requesting personnel. Simultaneously, they must take immediate action, such as delivering employees, emergency machinery, and materials to the accident site.

When the inspector arrives at the incident site, he must communicate the accident's circumstances briefly and properly to the on-duty accident response professionals. The inspector on the accident site must ensure the safety of passengers and pertinent personnel while also carrying out necessary emergency measures and repair work.

Handling upon Arrival at the Accident Site: The Head of the Vehicle Maintenance Centre or another authorised person must quickly examine, design, and propose a restoration policy based on the accident's circumstances. He must determine in advance the personnel configuration that will be on-site to aid in managing the accident, taking into account the type of assumed accident (collision, derailment, overturn, fire hazards, etc.) and the specifications of each line (Inspector, restoration personnel, assistant, informer, etc.). They must deploy persons and equipment in line with the request to ensure that the accident is restored in accordance with the restoration policy.

The maintenance personnel must be trained and have received instruction in the basis of restoration work so that they understand the necessary accident handling procedures and measures. The basis of the restoration work must be implemented in compliance with the safety regulations.

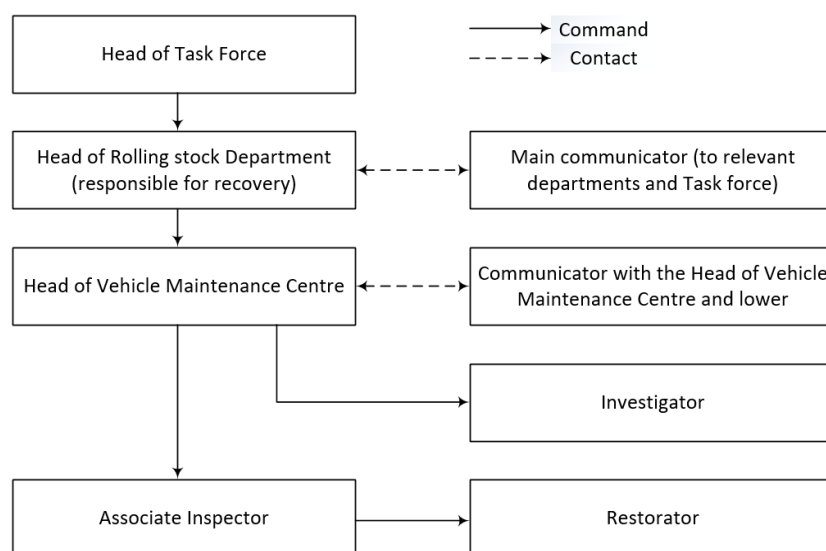
Besides, it is necessary to carry out the evaluation of fatigue factors and the alcohol and drug tests by Driver Training Centre. The appropriate rules/ procedures is clarified in Chapter 8.

### **7.3.2 The procedure of Work Assignment at accident site**

The Task Force is promptly established to carry out the restoration. The Manager Responsible for Safety shall serve as the Head of the Accident Task Force. Other maintenance staff who are directed to respond to an accident or disaster must attend to the accident location immediately. The list and contact information for the Rolling Stock Department's maintenance personnel must be clearly provided so that appropriate personnel can contact them as necessary. The organisation is composed of the following duty positions with the functions and assignment as described below.

- Head of Rolling Stock Department: shall advise the Taskforce to define restoration policy, instruct the Head of Vehicle Maintenance Centre and related personnel to implement and manage restoration activities.
- Main communicator: This personnel assists the Head of Rolling Stock Department and the Task Force, and acts as mediator between the Task Force and personnel who are not at the site. The personnel is responsible for communicating necessary information to the relevant departments and, as needed, requests their support.
- Head of Vehicle Maintenance Centre: The personnel is responsible for organising the restoration work according to the agreed upon restoration policy.

- Communicator with the Head of Vehicle Maintenance Centre: The personnel assists the Head of Vehicle Maintenance Centre and acts as mediator between Head of Vehicle Maintenance Centre, restoration personnel and the Task Force. The personnel is responsible for accurately informing the restoration policy-based instructions of Head of Vehicle Maintenance Centre and, at the same time, reporting relevant details about the restoration site to the Head of Vehicle Maintenance Centre.



**Figure 47** Responsibilities of each personnel in communication and reporting

- Associate Inspector: The personnel assists the Head of Vehicle Maintenance Centre in direction of restoration and implementation of restoration. Generally, the supervisor on duty in the Vehicle Maintenance Centre who is responsible for accidents becomes in charge.
- Investigator: The personnel investigates the circumstances of the accident, and retains records and evident of the accident.
- Restorator: The personnel is in charge of restoring work at the accident site.

Emergency Machinery and Materials:

- The emergency machinery and materials used for dealing with an accident are usually deployed in the Vehicle Maintenance Centre.
- The emergency machinery and materials must be periodically inspected, maintained and kept in good operating condition. Maintenance records of the equipment, machinery and materials must be created.

Evidence be used in an investigation must be located onsite, evaluated, and protected.

### 7.3.3 The Procedure of Restoring the Rolling Stock Failure after Returning to Depot

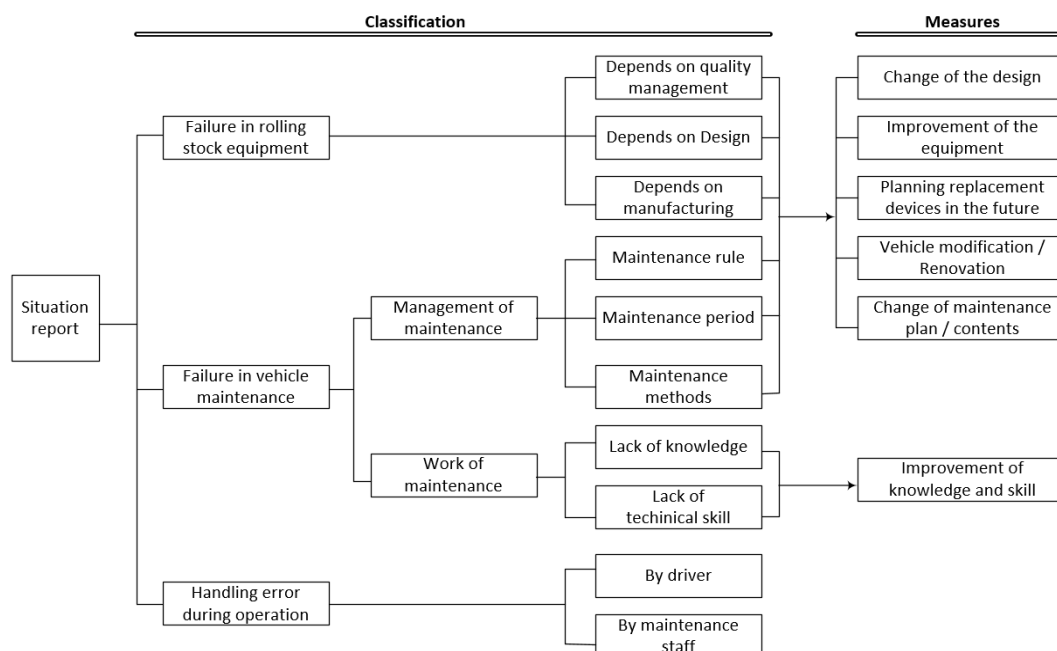
After the site investigation is complete, rolling stock must be arranged for safely moving to an appropriate maintenance facility in Depot for additional inspection, testing, and/or repairs. Investigate the failure after observing relevant circumstance:

- Analyse the fundamental cause of the failure and give a recommendation for corrective action. Railway accidents must be investigated and inspected in conformity with existing regulations.

- In the initial stage, HanoiMetro is lacking experience dealing with failures and restoration work.
- As a consequence, the participants in the failure investigation and resolution process include not only each division within the company but also the contractor that provided the equipment and the affected organisations. The Operator Unit - OU (Metro Line Operator) is responsible for investigating and resolving failures.
- Head Quarter of HanoiMetro is responsible for soliciting technical assistance from the contractor and other appropriate external organisations as needed. When conducting an investigation into a failure, which includes determining the cause of the equipment's previous failure and compiling failure-related information from maintenance records and materials, firm employees must take the lead.
- They will consult with the manufacturer as necessary to undertake a more thorough assessment. The investigation shall be conducted indefinitely or until the precise cause is found.
- If reasons of failure cannot be determined, it is acceptable to use the same or a substitute device once it has been determined to be safe.

Depending on the condition and reason of the failure, maintenance workers in charge must either perform restoration immediately or report to higher people to expeditiously repair failure. It is necessary to inspect additional portions of rolling stock for the same problem or risk of failure.

The type of failure and mitigation of hazard is clarified in Chapter 4. Several types of failure, and countermeasures for example is as in the Figure 48



**Figure 48** Several types of failure, and countermeasures for rolling stocks

Reports of Maintenance and Repair need to be submitted to the Rolling Stock Department and the Safety Department:

- The section in charge of investigation and restoration must prepare detailed records on causes and countermeasures, and report it to Manager Responsible to Vehicle and Equipment and Manager Responsible for Safety.
- In all cases, Metro Line Operator must report to Head Quarter of HanoiMetro on circumstances of including train delay time (if any).



## 7.4 The accident responding procedure relating to Passenger injuries

This procedure was designed to control the treatment of passenger injuries within the operational service area; in order to mitigate the impact of passenger injuries on railway operations, this standard should be implemented. It covers the investigation, identification, processing, statistical analysis, and reporting of passenger injury incidents.

Classification of passenger injuries:

- Very minor injury: This indicates that the degree of injury is clearly minor, insufficient to produce noticeable harm to human health, and will not result in system operation.
- Minor injury: refers to external physical, chemical, and biological elements that operate on the human body, resulting in some degree of tissue or organ damage or structural partial malfunction, but does not constitute a major injury.
- Major Injury: refers to injuries that result in physical impairment, cosmetic damage, hearing loss, vision loss, or loss of other organ functions, as well as another serious injury to human health.

### 7.4.1 Responsibilities in an accident relating to passenger injuries

Station Management Department and Station Centres:

- Responsibilities include on-site handling in the event of passenger trauma, including immediate treatment to the injured and site evidence collection.
- Responsible for conducting preliminary investigations, conducting accountability analyses, and determining accountability on passenger injuries
- Responsibilities include calming passengers, negotiating compensation, and filing insurance claims. Responsibilities include utilising, and monitoring the emergency treatment fund.
- Responsible for implementing injury prevention measures for passengers.
- Responsible for establishing and maintaining passenger injury records.

Safety Department:

- Guide to resolving consumer injury claims.
- Coordinate the treatment of passengers injured on the network.
- Responsible for determining and resolving the guest's injury event.
- Responsible for conducting statistical analyses of passenger injury incidences and coordinating the execution of preventative measures.

Public relation unit:

- The public relations department is responsible for receiving media interviews and publishing press releases about passenger injuries.

#### ***Principles for handling passenger injury incidents***

- When dealing with an injury occurrence, all staff must maintain the public reputation and preserve the company's primary benefits, as well as uphold the obligation secure the victim, and give necessary assistance to passengers.
- Immediate response is necessary when dealing with injury events. Call the emergency number first, then rescue the injured, limit damages, and gather evidence.
- Collecting as much situational evidence and the participants' signatures as feasible, to preserve original information, based on facts and impartial records.

#### ***Liability of the Hanoi Metro for passenger injuries***

- Incidents during transportation or in the area of the platform, exit and entrance of the station caused by the fault of the carrier.

- Caused by railway personnel during daily operation;
- Caused by railway construction work;
- Caused by the train's emergency brake;
- Door clamped (except for passengers scrambling to get on and off);
- Caused by breakdown of railway equipment facilities (vertical elevators, escalators, gates);
- Railway equipment damage has not been repaired in time and no warning or protection has been put in place;
- No warning signs or warning signs were damaged at the station;
- Clipped (unless passengers scramble to disembark, no tickets);
- Water, oil or obstacles on the platform of the train, station, not cleared in time or without setting up protective warnings (except in case of force majeure and during the cleaning cycle);
- Other situations that are not entirely the fault of the passengers.

#### **7.4.2 The procedure of passenger injuries treatment**

Information report:

If there is a passenger injury on board, the train driver or on-site staff should notify the station at the first time (or notify the station ahead via Dispatching Centre).

Procedures for station personnel dealing with passenger injuries:

- When a passenger reports an injury, it is prudent to hasten to the site to assess the person's physical health, segregate the evacuation viewers, alert the line, and phone the emergency number, local police, and insurance company, as appropriate.
- A cognizant passenger who can speak properly and accurately explain the condition (such as an injury, sprain, or dizziness) can administer basic first aid and determine whether the individual is hurt. The staff needs to assess the situation and ask the passenger if it is necessary to call an ambulance.
- For passengers who are lost consciousness, On-site workers should promptly contact the emergency hotline. After receiving the report, the vehicle control room should make emergency calls using a landline phone equipped with a recording feature, and then alert the police and Dispatching Centre.
- If the passenger's surroundings are dangerous (e.g., on stairs, ramps, escalators, or with the rider facing down), immediately utilise a stretcher to transport the passenger to a safer location (must be monitored by a camera).
- If the passenger is aboard the train, he or she should be moved to a secure area on the platform.
- In exceptional circumstances (such as significant injury or death), it is preferable to remain stationary after dispersing passengers, inform the Dispatching Center, wait for emergency assistance, and report to the police for management.
- After responsible personnel arrive on the site, the camera recording procedure should be performed (including the use of fixed safety cameras and photography equipment capable of capturing images).
- Assist emergency personnel in scene managing.
- If a passenger dies, aid the police with the investigation, maintain contact with the police and inform the coroner to ascertain the cause of death.
- Establish an incident investigation team immediately to collect and preserve evidence such as audio and video recordings, report incident handling reports to higher management and relevant departments, and monitor occurrences in real-time, compiling reports at each stage.

- The Inspection Team and the Safety Department will be given this evidence.

Handling after the accident:

- For incidents that can be negotiated and handled, after the negotiation process is completed, an agreement of the Station Management Department is drawn up and signed with the parties.
- For special passenger injury incidents, the Station Management Department takes the lead and all relevant departments participate in completing the overall aftermath.
- If the insurance company covers the complete cost of the passenger's injury treatment (excluding special compensation costs), the station management will handle it and is not required to submit it to the Safety Department for approval.
- If a portion of the passenger's injury treatment fee is to be paid from the emergency treatment fund, it will be handled by the Station Management Department if approved by the Safety Department.
- If the operator bears the cost of treating the customer's injury, the Station Management Department will form a negotiation team comprised of relevant staff from the Safety department, Public relations unit, Accounting and Statistics department, and equipment liability management department to conduct negotiations jointly.
- If a one-time settlement is not agreed upon, the emergency charge is paid in advance. Following completion of the treatment, the payment will be based on the actual expenses incurred during implementation.
- Expenses spent in the course of addressing customer injuries shall be reimbursed to the insurance company by the Station Management Department. Expenses incurred by witnesses in resolving events involving passenger harm will be reimbursed in advance from emergency treatment fund.

Manage injury records

The Station Management Department will develop a passenger injury record, in principle each passenger injury record document will include the following contents:

- Summarise of handling incidents of passenger injuries;
- A copy of the person's identity card (or a copy of the certificate of the authorized customer and a copy of the identity card);
- Medical records, certificate of diagnosis, certificate of discharge and drug list upon admission;
- Invoice related expenses;
- Agreement.

### **7.4.3 The typical procedures relating to people injuries**

- o People falling on tracks
- o Evacuate passengers from the train having incident at the station area
- o Evacuate passengers from the train having incident while in operation
- o Large traffic of passengers stuck at the station
- o Passengers fall into the elevator shaft

Appendix 5 indicated an example procedure for accident of People falling on tracks.

## **7.5 The accident responding procedure relating to vandalisms or terrorities**

### **7.5.1 Purpose and classification of protecting from vandalisms or terrorities**

Urban railways are a high-impact target because to their high population density, which may disrupt the transportation system's operation and create panic in the community if attacked. This procedure is used to strengthen the ability to prevent vandalism and terrorism.

The procedure outlines each unit's responsibilities for securing the workplace, forecasting the danger of attack, and enhancing the capacity to respond to sabotage or terrorist assault.

Classification of terroritory protecting warning:

- Protection Class 3 (daily): Take the daily minimum precautions of security.
- Protection Class 2 (warning statement): Utilise additional security measures and maintain them for a certain amount of time owing to mass gatherings in station areas, greater passenger traffic during major festivals, public holidays, and significant politic - economic events.
- Protection Class 1 (emergency): This level of protection is applied when there is information of a terrorist threat or there is a notification from the security services that a terrorist attack is possible.

Classification of hazardous site:

- Class 1 – Highly Dangerous: Station, Tracks, Trains, Dispatching Centre, Main transformer of Power supply system.
- Class 2 – Dangerous: Vehicle Maintenance Centre (Depot), Maintenance Material Centre.
- Class 3 – Normal: Office buidling.

Responsibilities

- The Executive Director of Hanoi Metro is responsible for counter-terrorism management. For each Metro line, the Manager Responsible for Safety is responsible for operating and directing anti-terrorism teams.
- Responsible for training, leading workers' anti-terrorism security plans, and summarising and reporting on the present condition of the Safety Department's anti-terrorism activity.
- The Safety Department is responsible for implementing the security strategy for Protection Classes 2 and 3.
- The security strategy for Protection Class 1 - Emergency is being executed by the Task Force for Terrorism, which has been approved by the Manager Responsible for Safety and the Hanoi Metro Headquarters.

### **7.5.2 Regulation for safety and security in station areas and track sections**

- Doors and equipment rooms of station equipment areas must be closed and managed. Doors and equipment room doors of each equipment area must be locked. It is strictly forbidden for couriers, parcels, and food delivery personnel to enter the area. When entering and exiting, you must have a valid employee card or building permit. External personnel need to register and be authorised by the Manager of Station Center to enter this area.
- Video surveillance is used to control the security of the entire station area. In addition, security staff will patrol the station area at certain intervals to control but

risks may arise such as foreign objects, suspicious people. When detecting any foreign objects, need to notify Dispatching center and the police if necessary.

- For passengers carrying large luggage, station staff must cooperate with security staff to conduct checks on passengers' items. If anyone with suspicious items is found, report it to the police.
- The station is absolutely prohibited from storing or using flammable or explosive items. Flammable products that must be temporarily kept and utilised for equipment maintenance must be contained in an explosion-proof cabinet and should not exceed the storage quantity permitted.
- During the construction process, the construction plan must be informed in advance and approved. Prior to construction, the person in charge of construction should verify the identity of all personnel operating and inspecting construction tools and materials before proceeding with the procedure. During construction, all registered employees must wear an employee identification card.

### **7.5.3 Regulation for safety and security in train**

- Driver cabin door needs to be locked.
- Anyone requesting to access the driver's cabin must go in with a valid ticket or dispatching order. No more than two individuals are permitted in the driver cabin, and their presence must be documented in the driving logbook.
- When a train driver notices a suspicious individual on board, he or she should promptly contact the Dispatching Center and Station Center to arrange for the inspector to board the train at the next station. This inspector is responsible for monitoring the suspect until he leaves the station. When aberrant symptoms appear, it is critical to promptly alert the Station Center.
- If there are any suspicious objects aboard the train, station personnel must inspect them personally. If objects appears to be connected to an electrical device such as a watch, timer, or cell phone, immediately evacuate passengers and contact the police.

### **7.5.4 Regulation for safety and security in Dispatching Centre, Vehicle Maintenance Centre and Maintenance Material Centre**

- The building is completely shut, and all doors must be secured.
- Establish security checkpoints at the depot or warehouse access and departure points; security personnel must record all visitors.
- On the Class 1 level of the control centre building, there is a security mission point that is staffed 24 hours a day.
- All staff entering the control centre building must enter through the main gate in principle.
- It is completely prohibited for express delivery workers, food delivery personnel, other employees, and strangers to enter the building without accompanying the company's employees.
- Visitors from other units and construction personnel must be escorted by an operating company employee who is registered at the security office.

#### ***Enhanced measurements for Protection Class 2 (warning statement):***

On the basis of fulfilling the requirements of Protection Class 3 – Daily statment, the following additional precautions are taken:

- The company's on-duty workforce is responsible for arranging the operating company's anti-terrorism efforts. All departments and centres have people on call 24 hours a day to gather and report on situational information and to manage the unit's anti-terrorism efforts.
- Increase 10%-20% of security personnel according to the situation, strengthen the patrol duty of important locations.
- All repair team members maintain communication 24 hours.
- Each department and centre conducts a comprehensive assessment of major components, doors, locks, and fences to ensure they are in good condition.
- Check the condition of emergency relief materials. Emergency response equipment and vehicles are on standby to ensure that emergency rescue work can be carried out effectively in the field case of a terrorist attack.

***Enhanced measurements for Protection Class 1 (emergency statement)***

- On the basis of fulfilling the requirements of Protection Class 3 – Daily statement and Protection Class 2 – Warning, the following additional precautions are taken:
- Establishing the Task force for Counter-terrority, the Executive Manager of Hanoi Metro and Manager Responsible for Safety needs to be on duty at the office to administer emergency response.
- Increase the number of security staff by 30% -50% according to the situation, arrange from two or more security officers on duty at important points and conduct 24-hour continuous inspection.
- Security personnel wearing anti-terror equipment, coordinate with police forces. Maintenance Centre leaders needs to be on duty at the office, repair team repair team is in a state of emergency response.
- Suspend the operation of certain lines and stations if necessary, conduct the evacuation of personnel in specific areas.

### **7.5.5 The general procedure for terroritory attack occurences**

**Step 1:** Inform the occurrence information:

- Any employee who discovers or receives information about a terrorist incident should immediately follow the prescribed notification process, without delay, interruption or omission.
- Station Center reports directly to 113 - Emergency contact of polices. If someone is injured, call 115 – Ambulance. Information needs to be continuously communicated to the authorities.
- Direct counterterrorism incident information is reported from the Task force, aggregated by the Safety Department's Accident Team. This information needs to be approved by Hanoi Metro Headquarters before being published by public relation unit.
- Task force personnel use the telephone to notify the Dispatching Centre, , traffic, electricity and environmental control personnel, and notify the dispatching staff, the Station Centre, the Staff and Service Management Centre, drivers on the main line.
- When the station and the dispatcher are interrupted by wired or wireless communication, the station manager arranges staff to go to the Dispatching Center, meet the relevant people to get contact information.

**Step 2:** Responding to accident

- In the event of a terrorist attack such as an explosion, fire or toxic gas on the main line and at the station, the rescue team and functional departments of each department will immediately be dispatched to the scene after order received.
- The typical procedures for vandalism and terrorism responding: (i) detect suspicious objects; (ii) detect suspicious people; (iii) Threatened with a bomb.

**Step 3: Reporting**

Each department maintain records of counterterrorism work in the sectors under its authority. The anti-terrorism work files will explain and thoroughly represent their management's counter-terrorism efforts in the area, and will include the essential charts for rapid updates as situations change.

## **7.6 The accident responding procedure relating to fire and explosion**

### **7.6.1 Purpose and Clarification of Fire and Explosion accidents**

When there is a fire event, this procedure is applied to provide hierarchical administration, defined duties, rapid reaction, and orderly coordination. Procedures regulate the mechanism's response to all fire and explosion situations efficiently and immediately, minimising casualties and property damage, and ensuring the safe production.

Classification of fire and explosion based on occurring locations:

- Fire and explosion in station lobby or platform.
- Fire and explosion in station technical area.
- Fire and explosion in running train or operating track section.
- Fire and explosion in power supply system.
- Fire and explosion in other areas.

Classification of fire and explosion based on the estimated severity:

- Hazard class 1: The fire broke out in a small area, there were no flammable items around. It is possible to judge that the fire does not spread. The amount of smoke generated is quite good. The fire can be extinguished immediately.
- Hazard class 2: The fire is intensive and leads to produce a huge amount of smoke. Therefore, it was impossible to accurately estimate the fire's threat and damage. Passengers panic and attempt to remove themselves, which can result in jostling and stamping occurrences during evacuation.
- Hazard class 3: There has been an attack or deliberate sabotage, such as intentional arson or bombing. It is resulting in interrupting the entire network and affecting large adjacent areas..

Hazard characteristic of fire and explosion accidents:

- Passenger traffic is large and concentrated in a small space. When a fire occurs, in addition to causing direct damage to passengers, it can also lead to secondary disasters such as panic, stampede when fleeing, mass casualties.
- When an explosion occurs, the entire track line will be affected causing interruption of operation for a certain time.
- Passenger rescue from elevated/underground stations and track section involves several challenges.

## 7.6.2 Fire and explosion safety instructions

Responsibilities of fire and explosion safety:

- Manager Responsible for Safety and the Safety Department is responsible for formulating and educating fire safety laws, as well as assessing fire prevention duties performed in Hanoi Metro.
- Managers of Departments and Centers are responsible for inspecting their units' work and arranging firefighting efforts in the fire emergency. Departments and centres are responsible for organising and managing emergency teams and fire protection equipment.

Fire protection equipment management:

- Must guarantee that evacuation routes and safe exits are clearly marked within their area of responsibility, and that firefighting equipment is deployed efficiently.
- Extinguishers and hydrants within the area of responsibility should be examined on a regular basis to ensure they are in good working order.
- The procurement plan for fire protection supplies, equipment inspection records, and incident data should be collected and preserved for one year.
- The following activities are absolutely prohibited: (i) Destruction of fire protection equipment; (ii) Unauthorised usage fire protection equipment or water; (iii) Occupy the evacuation passage; (iv) Install obstacles that affect evacuation such as fences over safety exits or evacuation passages; (v) Lock the safe exit, cover the sign indicating the safe path.

Control the hazard sources:

- Combustible materials must be properly controlled within the station.
- The station area's materials selection should adhere to applicable fire prevention requirements,
- Smoking is strictly prohibited in train stations, platforms, management offices, and train compartments, as indicated by signs NO SMOKING.
- In train stations, platforms, controlling rooms, and on trains, electric stoves and heaters are prohibited.
- At all levels of power distribution, protective circuits and alarm devices shall be installed.
- Construction need to be designed and tested for fire protection before operated.

Fire prevention inspection:

- Daily inspection: (i) condition of fire prevention equipment and materials; (ii) the evacuation pathway is safe or not; (iii) whether there is a violation in using electric fire in prohibited areas.
- Monthly inspection: (i) Situation of overcoming potential fire hazards as well as implementation of preventive measures; (ii) Situation of safe evacuation route, evacuation signs, emergency lights and safe exits; (iii) The current situation of the accessibility of the fire truck, the source of fire fighting water; (iv) Knowledge of fire prevention of key workers and other employees; (v) Fire protection records.
- Yearly inspection: The inspection content is similar to that of a monthly inspection but is more detailed and comprehensive to verify good equipment condition and ensure compliance of fire preventing regulations. The yearly inspection is usually combined to fire fighting practice at the company focusing level to ensure excellent fire prevention knowledge of all staff.



### **7.6.3 Principle of Fire and Explosion accident responding.**

The station's lobby is on fire:

- Passengers must be evacuated from the station.
- Provide an empty train to evacuate passengers to adjacent stations if the fire is serious.
- When a train arrives at the station, swiftly arrange people to board the train in order to evacuate to the adjacent station.

The station platform is on fire or explosion:

- Determines if the track section running through the platform can remain operational or not; if it cannot, the train in the affected region must be stopped.
- Arrange for the train to reverse direction; if the train is unable to return to its original location, evacuate the train immediately from the fire and explosive position. When the train comes to a stop at the station, if the door has not been opened, let the train to exit the fire area promptly.
- Evacuate people in accordance with the safety concept of fire/explosion in the station lobby.

Fire in running train or operating track section.

- Quickly stop the train at the next station, then proceed in accordance with the safety concept of fire/explosion in the station lobby.
- The driver unlocked the door, allowing the smoke to escape.
- If the locomotive catches fire, exit by the rear door. If the train's back ends up on fire, exit through front door. If a fire occurs in the train's midsection, evacuate to both the front and rear of the train.
- Evacuate in the opposite direction of the wind.

Other fire and explosion cases:

- Employees should be coordinated to quickly extinguish the fire and evacuate individuals to a safe location, depending on the circumstances.

### **7.6.4 The process of fire and explosion incident responding**

- The Dispatching Center operates on a pre-warning system that instantly distributes internal information and places emergency reaction instructions. When a train is affected, train order is promptly adjusted.
- The Station Centre coordinated promptly to dealing with the fire in the station area. Evacuate passengers and rescue the injured if required. Coordination with the fire department is necessary to extinguish the fire and rescue the victims.
- If there is a fire on board, the train driver takes action to extinguish the flames. Support units from the Station Centre rushed to the train, aiding with evacuation procedures and rescuing people.
- Proactively undertake rescue at the fire location or establish a Task force and Accident Team in accordance with the guidelines in Part 7.1.2, depending on the urgency.
- Hanoi Metro's public relations unit obtains information about the occurrence and its impact from the Safety Department or Accident Team. Publicly announce incident details and the company's response efforts through media sources such as social

media, television, and newspapers to preserve the company's reputation and avoid spreading fake news that creates confusion in the community.

- Maintenance Material Department ensure the supply of appropriate fire fighting and rescue materials.
- The typical procedure for fire and explosion responding
  - Fire on elevated track
  - Fire in station

## **7.7 The accident responding procedure relating to disaster**

### **7.7.1 Purpose and classifications of disaster warnings.**

The procedure is used to establish and improve plans for responding to disasters and hazardous weather events. Procedures for stipulating responsibility for warning and responding scenarios to dangerous natural disasters.

Classifications of disasters might occur in urban railway operations:

- Earthquake: Earthquake can cause dangerous consequences such as (i) collapse of viaduct or railway station, (ii) train derailments or collisions to collapsed construction, (iii) fire or electric shock due to short-circuit or break of power supply cable, (iv) people and objects falling from the bridge ground to the ground causing injury or death. Classifications of earthquake warning is as in the following:
  - Level 4 – normal damage: causes the death of less than 10 people (including missing people) or causes certain economic damage; earthquakes of magnitude is 4.0 – 5.0 in crowded area.
  - Level 3 – slightly significant damage: causes the death of over 10 people and less than 50 people or causes great economic damage; earthquakes of magnitude is 5.0 – 6.0 or 4.0 – 5.0 in crowded area.
  - Level 2 – significant damage: causes the death of over 50 people and less than 300 people or causes serious economic damage; earthquakes of magnitude is 6.0 – 7.0 or 5.0 – 6.0 in crowded area.
  - Level 1 – extremely serious damage: causes the death of over 300 people or causes economic damage at least 1% GDP; earthquakes of magnitude is over 7.0 or 6.0 – 7.0 in crowded area.
- Storms and heavy rains (including hails): are common phenomena that occur in the North of Vietnam in the summer. Storm and heavy rains can lead to (i) flooding, falls and drowning, (ii) electrical failure of the power supply system and electric shock to passengers, (iii) collapse of infrastructure and stations, and (iv) unsafe train driving. Warning of storms and heavy rain is clarified in five-coloured level as in the following:
  - Level 5 – white warning: likely to be affected by typhoon within 48h.
  - Level 4 – blue warning: likely to be affected by typhoon within 24h, wind speed can reach level 6.
  - Level 3 – Yellow warning: likely to be affected by typhoon within 24h, wind speed can reach level 8, and may be accompanied by a heavy rain warning within 6h.

- Level 2 – Orange warning: likely to be affected by typhoon within 12h, wind speed can reach level 10. This warning may be accompanied by a heavy rain warning within 3h and rainfall of over 50mm.
- Level 1 – Red warning: likely to be affected by typhoon within 12h, wind speed can reach level 12. This warning may be accompanied by a heavy rain warning within 3h and rainfall of over 100mm.

The consequences associated with a typhoon such as whirlwind, thunder, or hail are also used in conjunction with the five-coloured warning level above.

### **7.7.2 The procedure for natural disaster responding**

#### **Step 1 : Warnings announcements**

- The Safety Department will issue a warning level and disaster response plan after obtaining warning information from the Hydrometeorological Department. The Manager of Safety approves and reports to the Hanoi Metro Headquarters.
- Station Centers and Maintenance Centers prepare rescue teams and technical repair teams based on the warning level. The key personnel must be on duty at the maintenance centres and keep communication to the Dispatching Centre and the Safety Department.

#### **Step 2: Establish a Task force and implement the natural disaster response process**

- When an earthquake or storm orange warning occurs, form a Task force and implement rescue plans, evacuate passengers and staff, repair infrastructure and equipment according to typical processes such as (i) Earthquake; (ii) heavy rain and (iii) whirlwind
- When the on-site situation is challenging to control or spreads, develops rapidly and exceeds the control capacity of the Task force, the Accident team quickly contacts authorities such as police, military arms, ambulance, departments for construction and transport of Hanoi to mobilize more rescue forces.

#### **Step 3: End of emergency respond**

- After the disaster warning is removed, if emergency rescue is not issued, the corresponding emergency response action will be terminated one hour after the Safety Department issues the warning message.
- Or after the emergency rescue is complete, the hazard is basically eliminated, the secondary accidents are under control, the disaster of warning is also be removed.
- Technical teams of maintenance centres monitor any potential hazard and report the assessment of disaster responding actions to Safety Department within 24h.

## **8. SOLUTIONS FOR LONG-TERM DEVELOPMENT-SAFETY CULTURE**

### **8.1 Human factors in Railway Accident**

#### **8.1.1 Concept of Human factors in railway system failures**

Transportation projects need a large scale of investment, and several projects are the mega projects which are “complex ventures that typically cost one billion dollars or more, take many years to develop and build, involve multiple public and private stakeholders, are transformational, and impact millions of people” (Flyvbjerg, 2017). Moreover, despite billions of dollars being spent on development, construction, operation, and innovation every year in these projects, there are still thousands of lives lost due to various types of transportation accidents in different project phases or in operation. According to Hall (1997) and Andersen (1999), human errors are involved in approximate 70 – 90% of transportation accidents in general and over 70% of railway accidents in particular.

Additionally, Feyer and Williamson (1998) calculated that up to 90% of all industrial accidents were caused by human error. As a result, human error exposes businesses to danger, such as the train network's dependability and profitability. Identifying and estimating the likelihood of failures in new or changing railway systems, as well as analysing important mistakes that have already happened, enables the possibility of reducing the frequency of errors through accident mitigation and reduction measures.

Human factors is defined as “the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimise human well-being and overall system performance.” (IEAEC, 2000). It is a multidisciplinary topic of study that encompasses information from disciplines such as psychology, cognitive science, anthropometry, practical physiology, engineering, statistics, operations research, and industrial design (Chapanis, 1996).

Primarily, the human component in railways is influenced by a variety of disciplines, including psychology of personnel, construction engineering, industrial design, environmental and organisational factors, and operational activity. At each stage of a railway project's life cycle, the compliance of engineers/operators with the preceding disciplines will have an effect on the rate of human failure, and thus on the accident probabilities. To analyse and mitigate the adverse consequences of human error on system safety, the classification of human behaviours that may result in error occurrences is provided as in the following: (Woodson, 1981): (i) Human beings are often quite reluctant to admit mistakes; (ii) Humans frequently disregard or mistake instruction labels; (iii) The majority of people overlook the importance of rechecking regulatory guidelines for errors; (iv) Humans sometimes behave unpredictably in crisis situations or become easily confused by unusual things; (v) Humans are notoriously inaccurate in estimating clearance, distance, and speed; (vi) Normally, humans perform tasks while considering about other things; (viii) Personel generally consider manufactured items as being safe; (ix) Usually humans tend to hurry at one time or another.

According to Baysari et al. (2008), based on 162 accident analyses in Australia from 1998 to 2006, their research indicated 29 unsafe acts of driver including skill-based errors (50%), decision error (20%), perception error (2%), routine violations (20%) and exceptional violation

(8%). In Vietnam railway industry, based on railway accident statistical data, there were 316 incidents from 2010 to 2017, and human errors are the major reasons of 42% accidents, mostly in driver errors such as lack of concentration (26% of human-error related accidents), wrong predictions (22%) and actions or violations (18%); or infrastructure errors caused by poor human performance in maintenance (around 10% of total accidents). (Vietnam National Safety Board, 2016, VR, 2016, 2017).

### **8.1.2 Factor influencing to Human performance in railway system**

#### ***Personality***

To assess the staff's attitude to professional working and rule compliance, there are two groups of characteristics listed in the following: i) Positive: Extraversion, Conscientiousness, Internal Locus of Control; ii) Negative: Agreeableness, Neuroticism.

Extraversion describes ambitious, outgoing, pro-social and communicative behaviour and is a strong predictor for leadership responsibilities. Conscientiousness is characteristic of people who are self-disciplined, industrious, focused and organised. Locus of Control shows great initiative and willingness to contribute to outcomes, like career progression or job change (Judge et al., 1999, Hartman & Betz 2007, Bandura & Wood, 1989). In summary, these types of positive working characteristics include a targeted work orientation, the demonstration of positive work patterns, and the sequential development of competencies. As a result, individuals with these qualities are more likely to prevent breaching rules, mitigate the negative impacts of stress/distraction, be more trustworthy and perform better in the system.

Agreeableness can be perceived as a benefit in teamwork circumstances and in avoiding confrontation. Additionally, agreeable people are less active. Staff with characteristic tend to make mistakes of routine work and exceptional violations. The final type of characteristics, Neuroticism, indicates an inhibited effective career management and is associated with low career self-effectiveness (Ng et al., 2006, Hartman & Betz, 2007). As a result, neurotic personnel may lack motivation in increasing their performance, struggle with distraction and stress management, or have difficulties maintaining contact/communication.

The current study investigated key aspects of train drivers' roles and performance, including route knowledge and the psychological components of train driving such as researches of Farrington et al. (2005), McLeod et al. (2005). There are few researches that investigated the potential causes of human error (Reason, 1994) and the extent to which the in-cab environment supports the driver's ability to maintain situational awareness. A part of reducing potential for driver error and of increasing their effective (on-time) performance lies in the design of their jobs and job aids (Kecklund et al. (2001) as well as understanding and optimising – neither too high nor too low – their workload.

#### ***Stress and fatigue / Power of concentration***

Stress and fatigue can have psychological and/or bodily components. However, this research is highly concerned about mental tiredness in the railway industry.

ORR (2012) defines it as 'a state of perceived weariness that can result from prolonged working, heavy workload, insufficient rest or inadequate sleep'. There are several causes of tiredness, ranging from common characteristics such as insufficient sleep and irregular sleep-wake cycles to outside influences such as workload, individual motivation, and interest in the task. In general, there are three main groups of factors that cause stress and fatigue: (i) Work-related factors: working time, the number of duties, the length and complexity of each duty,

resting hours; (ii) Individual factors: age, medical and pharmacy conditions, alcohol and drug usage; (iii) Environmental factors: resting environment.

According to RSSB (2015), stress and fatigue can limit the worker's capacity to identify accidents and process information, reducing their ability to respond and make decisions. Ascending levels of stress (Hancock and Szalma, 2008; Mearns and Hope, 2005) can lead to these consequences as in the following: (i) Reduced working memory capacity, (ii) Diminished attention, (iii) Poor concentration/alertness, (iv) Lower primary perception of the situation, (v) Inattention to the available information, (iv) Narrowing of the individual's attentional field, (vii) Incorporation of only a restricted number of core aspects.

Results of stress and fatigue are errors in human behaviour, are especially: (i) Irrationally response in emergencies, (ii) Staff get easily confused with unfamiliar things, (iii) Poor estimation of clearance, distance, and speed as in above by staff. In recent years, systems design and human performance concepts have transferred from other industries and systems, into the railways. This research has dealt with the mental workload of signallers (Pickup, 2005); teamworking and situation awareness (Bristol, 2004); reasoning (Jorna, 2007).

### ***Safety Critical Communication***

Gibson et al. (2017) investigated 95 railway incidents in United Kingdom from 2012 to 2015 which involved communication factors and identified 541 incident factors from these incidents. From these, 383/541 incident factors were communication incident factors, with the remaining 158 being broader system issues. Moreover, there is usually more than one communication issue, that resulted in a single incident, because this problem can emerge in multiple parties, equipment issues, information transferring and the accuracy of information.

According to the statistical data from this research identification, up to 80% of the contributory factors related to the 'sender', who have information and need to communicate to other person/components is including three types of failure: i) Not using the communication protocols (eg using the phonetic alphabet and using repetition) (32%), (ii) Leaving out important details, saying something that is vague, wrong or overly complex (31%), (iii) Not starting a communication at all (15%). On the other hand, the role of 'receiver' generates to 11% of incident factors with the problem of misunderstanding the information.

Furthermore, in aspect of protocol failure, Gibson (2017) also indicated that the lack of repetition is the most common failure. Therefore, the issue of improving communication protocol's quality is essential to ensure safety critical communications that match the requirements of national agreed protocols. Moreover, the introduction of electronic communication is one of the effective systemic solutions. Introducing and applying the electronic format of communication will increase the volume of data and the transparency of work. The information monopoly of the paper system and its characteristics is difficult availability of information will be removed. An electronic communication system allows immediate informing of all participants in the production process about the status of works and the problems during the work.

### ***Violating regulations***

Occasionally, individuals violate the rule because they are unaware of its existence, or because they do not understand it well enough, or just because they fail to realise that a circumstance requires it. Alternatively, they may have simply forgotten about the regulation. The vast majority of the time, individuals do not violate regulations purposefully but for entirely legitimate reasons. In principle, violations occur as a consequence of conflict

between an organisation seeking to manage employee behaviour and the person wanting to perform its role as efficiently as feasible..

The classification of violations is generally divided as categories (RSSB, 2008, Lawton, 1998):

- **Situational violations:** Some types of breach can lead to situational violations and usually arise under challenging conditions where someone sees an economical way to keep the job going. For instance, a driver may continue driving even after losing sight of the shunter during a movement. These infractions are high-risk and frequent, occurring during staff members' everyday activities. Violations are unavoidable in poorly built or understaffed work areas or equipment. Under these conditions, it is difficult, if not impossible, for workers to remain within the rules, much less to comply with all requirements. While the business effectiveness increases, this sort of infringement is frequently overlooked. Managers may even anticipate or condone such infractions.
- **Routine violations:** When a breach of regulation occurs regularly in daily tasks due to the rule was unnoticed or unremarked, this action can become a routine violation. They are often high frequent but at low risk. People usually assume that the skill of the individual more than offsets any risk they might be taking. In such cases, individuals may also believe that the rules they are ignoring no longer apply to them. These routine transgressions end up being part of the normal way of working within a particular workgroup.
- **Exceptional violations:** This type of violation may occur as a consequence of an uncommon circumstance that combines numerous rare events and necessitates an immediate response. Exceptional infractions are frequently associated with a high risk, but low frequency of occurrence and have the potential to result in a significant accident. They arise when someone is confronted with a new situation and is required to use their knowledge in order to solve it.
- **Personal optimising violations:** The cause of these types of violations is poor monitoring, which might result in an error. In a variety of scenarios, staff members must estimate and apply additional skills in the absence of knowledge. Finally, those who are not totally accountable for safety are more likely to engage in unsafe work practises than those who are fully responsible for the consequences of an accident or incident.

Rule breaking can generate several different outcomes: i) for individuals, the violation can be a routine and a part of personality, thus, they take more risks in their career; ii) for companies/organisation, rule-breaking on a large scale may cause serious disruption to productivity and loss of reputation due to the accidents; iii) for society the economic and social costs of railway accidents are huge.

### ***Working environment / Organisational factor***

This factor includes work patterns, the culture of the workplace, resources, communications, leadership, etc. Such factors are often overlooked during the design of job specification but have a significant influence on individual and group behaviour. Several problems in the working environment / organisational ability can influence human failures as: (i) Poor work planning, leading to high work pressure, (ii) Lack of safety systems and barriers, (iii) Inadequate responses to the previous incident, (iv) Management based on one-way communications, (v) Deficient co-ordination and responsibilities, (vi) Poor management of health and safety.

## **8.2 The role of Safety Culture in System Safety Improvement**

### **8.2.1 Concept of Safety Culture**

According to Lee (1996), an organisation's safety culture is the combination of individual and group beliefs, attitudes, perceptions, competences, and patterns of behaviour that influence an organization's commitment to, and style and proficiency in, health and safety management. The concept of safety culture is based on the attitudes and beliefs, motives and values shared by all members of the organisation, the establishment of visions and standards of work behaviour, the leadership of the manager, and the involvement of all employees. A good safety culture, according to the report of the Railway Safety Act (2006) review, emphasises the importance of the relationship between policies, technologies, and employee attitude toward safety control. These concepts were also highlighted in Pidgeon's (1991), Glendon and Stanton's (2000), and Cooper's (2000).

In general, safety culture may be described as a combination of behaviours (ways of doing) and mindsets (ways of thinking) that are commonly considered by an organization's members when it comes to mitigating the most significant hazards associated with its activities. Safety culture is critical in analysing and comprehending the role of each component in railway accidents. The ultimate goal of safety culture research is to develop a systematic, psychological, and legally compliant solution for mitigating the impact of human failure by ensuring that everyone shares the same values, attitudes, competencies, and pattern of behaviour, thereby decreasing the probability of errors. The SMS's ultimate goal is to establish a successful safety culture. The instruments outlined in the SMS plan serve as a foundation for railways to accomplish this goal. A railway company's strong safety culture can help reduce public and employee fatalities and injuries, property damage caused by railway accidents, and the environmental impact of accidents.

### **8.2.2 The influences of safety culture in operational safety**

To begin, a safety culture prioritises assessing and controlling the most important hazards, which are typically large occurrences and injured/fatal accidents (obviously including human failure in these incidents). In a safe culture, collective data and risk assessment results are stored in a shared database, and employees have the opportunity to share, explain, and discuss important risks; as a result, all employees in the organisation are informed and made aware of the most critical dangers. Although the most serious dangers differ by activity, location, and employment, they must be known and discussed by all personnel in the organisation. Additionally, a clear understanding of the most significant risks will assist the employee in concentrating on the numerous barriers that prevent and restrict the occurrence of an incident; as a result, they may investigate the system's problem prior to the failure occurring or take reasonable action after the failure occurs.

Second, the safety culture is formed around three interdependent components: technical safety, the safety management system, and human and organisational elements. Technical safety encompasses the following actions: facility design, equipment quality, redundancy, fault sensors, and automated protection systems; thus, investment in design processes, technology development, and resource allocation will help preserve the organization's safety atmosphere. To increase safety quality, the safety management system standardised all processes, procedures, and standards for operation and management. The safety management system may be implemented simply to meet external standards, or it may be



used to bring together disparate employees to discuss risky scenarios that are likely to arise and the most effective preventative actions. Finally, the human and organisational elements demonstrated the substantial harm caused by human errors, promoting the efficiency and safety of human operations. Human failure can be significantly reduced by training, motivating, and giving proper working equipment or a cooperative environment (Cooper 2000, French & Steel, 2017).

Thirdly, balancing rule-based safety and managed safety. There are two elements of safety management methods: rule-based safety which based on the best possible anticipation of situations that could occur, and the implementation of safety barriers and work rules; managed safety which focus is on proactive and appropriate individual or collective initiative when faced with a situation. These two elements are not mutually exclusive since, for example, managed safety can include the adoption of rules by employees. Moreover, the rules that constitute rule-based safety can also change based on the experience gathered in managed situations. Safety management must also encourage coordination between the two, through better integration of operational experience feedback and field experience in working instructions. This is a crucial part of the role of front-line management. Certain organisational structures lead to an unbalanced approach, with rule-based safety being seen as the only aspect to develop. This approach often gives an illusion of control over safety. In many high-risk companies, managed safety is not given enough attention in the safety culture (French & Steel, 2017).

### **8.2.3 The principle and methods of applying Safety Culture**

#### ***The three principles of Safety Culture***

Principle 1: People are solutions. Individuals are positioned at the centre of solutions and enabled to participate in the process of establishing safety. Recognise the adaptability of all staff. Everyone is encouraged to raise their hand for safety at any moment, resulting in the development of ideas and innovations that possibly contribute.

Principle 2: Safety is the presence of positives. Safety as the existence of positives provides a broad view of the system and attempts to strengthen organisational resilience. It is a metric that examines what works and how we may learn from when things are done properly and securely. It promotes involvement at all levels, fosters an awareness of and appreciation for achievement, and assists in the management of all high-impact risks.

Principle 3: Safety is an ethical responsibility. Individuals need to operate within a strict safety framework. Systems and processes are meant to facilitate work and are centred on risk management. Understanding the daily variation in the workplace is critical to ensure that our systems are flexible to changing situations. Leaders of each component, each Department and Centre have dialogues about the positives — about reinforcing behaviour – rather than the negatives – about blame, compliance, and punishment. HanoiMetro recognises that safety is a human responsibility and that accountability is placed at the point of employment.

#### ***Fundamental concepts in implementing a safety culture in HanoiMetro***

##### **1. Focusing on high consequence risks**

Numerous actions within urban railway operations pose significant vulnerabilities to humans if not managed properly. The SMS plan's emphasis on high consequence risks enables staff at all levels of management to make educated risk management decisions. Severe haz-

ards are monitored by Hanoi Metro's Risk Assessment processes, which are detailed in Chapter 5. They are identified in the standard and give straightforward advice on the numerous minimum mandatory procedures that must be in place, proved, and effective in order to manage fatal and severe risks in our activities.

This method enables engineering teams to function within a more constrained and simplified framework, allowing the Safety Department to oversee more actively. Additionally, it may be used as an audit tool following activity to ensure key controls were implemented; nevertheless, it is more critical to utilise the tool throughout the planning, procurement, monitoring, and maintenance cycles. Each workplace is obliged to examine the operational risks associated with particular job functions and to establish a schedule of Risk Assessment reviews proportional to the scope of the workplace's operations. Each department and centre must customise the risk assessment tool's criteria.

## 2. Understanding hazard situation and learning from experience

Risk assessment is based on the hazard identification and data of failure rates throughout the operational process. However, besides only focusing on facts or statistics, emphasising narrative and promoting innovation will even provide safer and more positive results. This is accomplished through group engagement techniques such as collective insight, but also through discourse and the examination of work as envisioned. Recognize the variety of daily performance and develop resilience. This is the foundation of adequate safety. The requirements to gain this situation is suggested in the following:

- **Collective insights:** A collective insight is one of the tools used to engage with employees. It generally focuses on a site-specific high-risk activity. A leader facilitates a discussion with a work crew to review (i) Hazards associated with the work; (ii) How well they are controlled; (iii) What else can be done to make the workplace safer; (iv) Actions to be presented for closeout and feedback to the staff.
- **Positive investigation:** Understanding what works focuses on successful tasks rather than failures and aims to understand what factors contribute to success in order to do more productive tasks. Additionally, the investigation may discover and urge the elimination of any redundant or superfluous procedures and other shortcomings that may have gone unnoticed in the absence of the inquiry but are not designed to complicate systems or ways of work.
- **Positive Observation:** Positive observations are recorded when personnel observe behaviour or work areas that are above operational expectations and standards. This enables managers to detect novel techniques that operate outside of the norm and to promote positive behaviour in individuals and work groups.

## 3. Empowering the workforce through engagement and trust.

Railway operations experience (ICSI, 2018) demonstrates that solutions are generated by individuals accepting responsibility, rather than by following top-down accountability requirements. Individual characteristics are viewed as a resource that helps individuals to develop their unique ability for safety production.

- **Safety Critical Messages:** Significant safety announcements are made top-down by the Safety Department, which synthesises operational and maintenance failures, as well as practical responses, to provide concise safety instructions that are broadcast to the entire company. Additionally, the bottom-up notification method is utilised by organising seminars and exchanges amongst business divisions to share best practices in safety monitoring and management.

- **Skill Training:** Master Trainers may be invited technical and management professionals from the Ministry of Transportation or transportation institutions to train on new regulations or technological and management advancements. Additionally, competent engineers from the company are asked to share their experiences with the organization's overall operation and maintenance methods, as well as with external units. Besides, regular staff training must be taken seriously and efficiently executed.

#### 4. Leadership to changing traditional thinking

Any member of the Department or Centre has the potential to be a safety control leader. All employees are required to communicate safety-critical messages to their peers via team leaders throughout the organisation or workplace. Company leaders' commitment to change demands them to consistently challenge and modify industry and traditional health and safety standards and procedures.

When evaluating safety performance, a strong focus is placed on effective teamwork and line management assistance. Consequently, an individual's performance is not only related to their own contribution, but also to that of their direct team, thereby boosting one team's involvement and fostering the safety culture.

### 8.2.4 A practice to establish and improve the safety culture

The importance of cultural characteristics as an essential informal “ingredient” for sustainable safety management has now been identified and a legal basis developed in the fourth railway package established safety culture in 2016. On top of that, the rule (EU 2018/762) states that top management must promote a “positive safety culture” and that the organisation must submit a strategy to improve its safety culture (EU Agency for Railways, 2020).

**Table 8.1** Requirements for a positive safety culture (EUAR, 2020)

| No          | Characteristics   | Self-assessment |                |
|-------------|---|-----------------|----------------|
|             |   | Available       | Needed improve |
| <b>F1</b>   | <b>Controlling major risks</b>  |                 |                |
| <b>F1.1</b> | <b>Risk awareness.</b><br>Individuals at all levels are aware of major risks and understand their personal contribution to safety   |                 | X              |
| <b>F1.2</b> | <b>Resilience</b><br>The capability to operate safely under unexpected situations is developed.   | X               |                |
| <b>F1.3</b> | <b>Questioning attitude</b><br>Individuals at all levels avoid complacency, challenge assumptions, encourage and consider opposing views.   |                 | X              |
| <b>F2</b>   | <b>Understand Workplace Reality</b>   |                 |                |
| <b>F2.1</b> | <b>Working conditions</b><br>The organisation recognises that working conditions (time pressure, workload and fatigue) influence safe behaviours                                    | X               |                |
| <b>F2.2</b> | <b>System complexity</b><br>The organisation recognises that its technologies and systems are complex and can fail in unpredictable ways  | X               |                |
| <b>F2.3</b> | <b>Reporting</b><br>Routine and abnormal deviations from expected performance are recognised and reported. Measures to identify and mitigate organisational silence are implemented |                 | X              |

|             |  |   |   |
|-------------|--|---|---|
| <b>F3</b>   | <b>Learn From Experience</b>   |   |   |
| <b>F3.1</b> | <b>Analysis</b><br>Reporting is systematically analysed to identify those factors that allow organisational learning and improvement |   | X |
| <b>F3.2</b> | <b>Improvement</b><br>Safety related feedback is perceived as an opportunity to improve performance and is acted upon                |   | X |
| <b>F3.3</b> | <b>Learning from others</b><br>The organisation actively seeks learning opportunities  | X |   |
| <b>F4</b>   | <b>Integrate Safety Consistently</b>   |   |   |
| <b>F4.1</b> | <b>Safety vision</b><br>The organisation develops and implements a safety vision to support the achievement of business objectives   |   | X |
| <b>F4.2</b> | <b>Resource allocation</b><br>Safety is a primary consideration in the resources allocation  | X |   |
| <b>F4.3</b> | <b>Decision making</b><br>Individuals at all levels are convinced that safety and operations go hand in hand                         | X |   |

According to technical assistance report to this project, twelve attributes derived from positive safety culture practices are presented to establish an organisational culture that supports railway safety fundamentals. The detailed explanation of these attributes and self-assessment of these solutions in current safety situations of Hanoi Metro Company is provided in the Table 8.1.

Based on the self-assessment of safety culture requirements, the SMS suggested three solution groups to fulfil the requirements such as:

- Human resource management: to deal with requirements F1.1 and F4.1
- Analysis and Reporting: to deal with requirements F2.3 and F3.1
- Employee Involvements: to deal with requirements F1.3 and F3.2

The suggested primary solution from research of EUAR (2020) compliance to three solution groups are clarified in the following table. The solution groups of Human resource management and Employee Involvement mainly relating to the staff reactions. They will be referred in this Chapter. The solution group on Analysis and Reporting are related to the Data Management and Enhancing the project management capabilities, therefore, it will be described in the Chapter 9.

**Table 8.2** Three solution groups for improve safety culture

| <b>No</b> | <b>Solutions</b>  |
|-----------|---|
| <b>1</b>  | <b>Human resource management</b>  |
| 1.1       | <b>Roles, responsibilities and authorities are understood and accepted</b><br>Roles, responsibilities and authorities within the organisation are defined, effectively communicated and regularly reviewed taking into account major risks and workplace reality. Particular attention is placed on staff conducting safety related tasks, including contractors, to make sure everyone knows, understands and accepts its role and contribution to safety. |
| 1.2       | <b>Competence management ensures a knowledgeable workforce</b>  |

|     |   |
|-----|---|
|     | The organisation has a competence management system, targeting all staff, that reflects the requirements of operations and contributes to the railway safety fundamentals.  |
| 1.3 | <b>Managers exhibit behaviours that set the standard for safety</b><br>Managers shape the organisational culture. This is why they are expected to be safety leaders, in particular by sharing the organisation's safety vision and leading by example. Their presence is effective through observation, coaching and reinforcing standards and expectations.   |
| 2   | <b>Analysis and Reporting</b>   |
| 2.1 | <b>Healthy regulatory relationships exist and ensure that the accountability for safety remains with the operating organisation</b><br>Healthy regulatory relationships are those relationships between regulatory bodies and the railway organisations that support the achievement of sustainable and safe performance of the railway system through regulatory activities. They are based on transparency and trust, common understanding of safety issues and responsibilities, and use of proportionate power. |
| 2.2 | <b>Processes, tools and documentation support sustainable and safe performance</b><br>The organisation has implemented a living safety management system, leads to the accomplishment of the safety vision. Documentation, procedures, rules, and technical solutions support railway safety fundamentals and are actively used by staff.   |
| 2.3 | <b>Organisational structures support sustainable and safe performance</b><br>The organisation has built its structures (organisational chart, processes, procedures, formal rules) to be consistent with the safety vision. The organisational structures take into account the control of major risks, workplace reality and continuous improvement.   |
| 2.4 | <b>Safety information is openly shared within and across organisations</b><br>The organisation has defined safety information, and the means for disseminating it within and outside the organisation, including contractors, other railway organisations, regulatory and investigating bodies. Staff is aware of the importance of sharing safety information with the objective of delivering sustainable and safe performance.   |
| 2.5 | <b>Managers ensure that incentives, sanctions and rewards reinforce behaviours and outcomes that support the accomplishment of the safety vision</b><br>The organisation creates a transparent, consistent and shared understanding of what is acceptable and unacceptable. This is proactively supported and demonstrated by managers throughout the organisation, for example by providing timely feedback on both safe and unsafe behaviours.  |
| 3   | <b>Employee Involvements</b>  |
| 3.1 | <b>Collaboration within and across organisations is nurtured to operate safely.</b><br>The organisation recognises it is one component of a larger socio-technical system and implements arrangements to facilitate sharing within and across organisational boundaries. Staff interacts and openly exchanges relevant information, formally and informally, within their team, their department, with other departments and with other organisations (e.g. suppliers, contractors, stakeholders).                  |

|     |  |
|-----|--|
| 3.2 | <p><b>Trust, respect and openness permeate the organisation and characterise inter-organisational relationships at all levels.</b></p> <p>The organisation and its management truly see value in an open culture where ideas and opinions can be articulated and discussed, even if they create ambiguity and friction. Trust and respect throughout the organisation enable reporting and sharing. Managers are aware that trust is difficult to build and easy to lose, and behave accordingly. Frontline staff feels comfortable to report to the management.</p> |
| 3.3 | <p><b>Safety information is openly shared within and across organisations</b></p> <p>The organisation has defined safety information, and the means for disseminating it within and outside the organisation, including contractors, other railway organisations, regulatory and investigating bodies. Staff is aware of the importance of sharing safety information with the objective of delivering sustainable and safe performance</p>  |

## 8.3 Human resources management

### 8.3.1 Safety Training

A rail safety worker should understand their role and responsibilities as part of the safety management system. The rail transport operator should therefore ensure its rail safety workers have a working knowledge of the safety management system and how their work relates to it.

The safety management system must include systems and procedures:

- for the training of rail safety workers who are to participate in the implementation of the safety management system or who may otherwise be affected by the implementation; and
- to encourage the awareness, understanding and participation of rail safety workers in the safety management system.

It must also include provision for induction and ongoing training with regard to rail safety including information, instruction and training on new work practices, procedures, policies and standards, specified hazards and relevant control measures.

#### ***Principle and requirements***

Operation and Maintenance Centers design a safety training programme for their units based on national and company regulations. In which the daily training materials (operational procedures, operating procedures, risk handling procedures, and emergency response) are clarified.

Firstly, personnel must be trained in safety, understand safe working methods, and comprehend pertinent safety rules. Furthermore, employees develop safe operating skills in their positions and quickly suggest a handling solution. In terms of production safety, employees must be aware of their rights and obligations. Finally, it is necessary to respect the rule that “No one who has not been properly trained in safety can work”.

Safety training records for new employee, safety training cards of employees who change jobs, employees returning to work after a leave of absence, and assessment records must be approved by the Safety Department before assigning working task for employee.

Safety training cards and assessment records must be kept in perpetuity, which can be eliminated upon employee resignation. Other safety training records must be kept for 5 years, after which they may be removed by regulation.

***Classification of required training levels.***

Training before assigning working task for employee.

There are three levels of training levels before work assignments: Company level; (ii) Department or Centre level including all departments, dispatching centre and maintenance centres; (iii) Team level: technical team, dispatching/ management team, driving team.

The training will be assigned for each type of employee as in the following:

- New employees (including contracted workers, occasional employees, probationers, interns) must go through 3 levels of safety training before working at the company level, the department (centre) level and the team level. The minimum safety training period is 24 hours of study.
- Employee who changes their working position need safety training at department and team levels. The minimum safety training period is 16 hours.
- Employees who return to work from an over-three-month absence (sick leave, maternity leave, long-term leave) need safety training at the Department level and team level. The minimum safety training period is 16 hours and the minimum working under supervision time is 30 hours.
- Employees who return to work from an under-three-months absence only need a safety training at the team level. The minimum safety training period is 8 hours and the minimum working under supervision time is 30 hours.

Regular training (Day training):

- Group 1: Leaders, heads of departments, and managers of maintenance centres must undertake at least 32 hours of safety training the first time, followed by at least 12 hours of retraining each year.
- Group 2: Other employees re-train for a minimum of 12 hours each year.

### **8.3.2 General Contents of Safety training**

***Safety training at company level*** – minimum 8 hours.

- Safety conditions in each company units.
- Fundamental knowledge of safe manufacturing, including production characteristics, equipment condition.
- The organisation structure of the company for the purpose of ensuring production safety is the primary rule governing safe production.
- Rights and obligations on production safety of operational staff.
- Banners and warning signs for workplace equipment.
- Case studies and typical workplace lessons about accidents and rescue, as well as accident reporting protocols.
- Fundamental knowledge of fire prevention and rescue.
- Occupational safety and labour protection knowledge.

***Safety training at department level*** – minimum 8 hours

- Overview of the department (centre), including (i) operating flow, (ii) work environment factors and risk factors encountered, (iii) incidents of injury or health hazards encountered on the working tasks, (iv) safety responsibilities and mandatory

standards, (v) installation of safety equipment, (vi) use and maintenance of personal protective equipment.

- Basic knowledge of safety techniques and guidelines for safe production management such as critical hazard locations, labour protection regulations.
- Measures to prevent accidents and occupational hazards, self-first aid, evacuation and emergency treatment at the scene.
- Analyse typical accident cases as well as common accidents in the centres
- Knowledge of fire prevention and fighting of the department, duties of the fire brigade as well as general knowledge of fire fighting of the fire brigade.

***Safety training at operational / technical team*** – minimum 8 hours

- Working characteristics of particular team such as work environment, hazardous areas, equipment condition, precautions, emergency exits.
- Regulations on safe operation and responsibility.
- How to use protective equipment and safe production requirements.
- Work coordination, occupational health and safety.
- Incidents that happened in the previous working group.

Safety education at the department and team level can be based on the working conditions of employees in order to conduct training, ensure safe operation in their respective job positions, and assure knowledge and abilities in emergency response.

Each safety training level is required to undertake a quality assessment following the completion of each training course. The assessment may take the form of an oral examination or a written examination.

The Safety Department must receive all assessment and testing data, as well as the employee's 3-level safety training cards. Additionally, test results are retained throughout the employee's working period.

Notes for specific contents in training process:

- Employees who are injured on the job must receive safety training before to returning to work. The safety training should involve, at the very least, incident analysis and comprehension. Safety coaches must direct their teams' abilities, safe operations, and safety policies. Employee must develop new abilities, overcome operational errors, and collect information in order to avert incidents.
- For employee who take long-term leave, after returning to work one month, they must conduct safety training. The main content is to firmly regulate safe operation, familiarize himself with the features of machinery and equipment, and perform practical operations.
- For employees who have been suspended from work due to violations of safety rules that resulted in an incident, the safety training is minimum 24 hours. The training need to concentrate on reasons for being suspended from work and setting out on-site practical training.

***Regular training contents*** – Group 1: Leaders and Managers

- National production safety rules and policies, as well as pertinent laws, regulations, and requirements.
- Basic and advanced knowledge of production safety, as well as production safety techniques.
- Regulations governing hazard management, incident prevention, emergency response, and accident investigation.
- Hazards and precautions in the workplace



- Extensive experience in sophisticated manufacturing safety management both domestically and internationally;
- Analyses of typical accidents and emergencies

**Regular training contents** – Group 2: Other Staffs

- National production safety rules and policies, as well as pertinent laws, regulations, and requirements.
- Knowledge of production safety, as well as production safety techniques.
- Reporting and statistics on casualty incidences, as well as investigative actions to address occupational health issues.
- The nature and scope of emergency management, incident planning, and response.
- Extensive experience in sophisticated manufacturing safety management both domestically and internationally.
- Analyses of typical accidents and emergencies.

For employees in risk response departments, in addition to 3-level training and regular training, they must obtain professional training and safety management in compliance with the National Safety Board and Ministry of Transportation's regulations.

Additionally, technical departments are constantly planning workshops within and between maintenance centres to share experiences and collaborate.

### **8.3.3 Stress and fatigue management**

***Purpose***

Fatigue management is mandatory for all railway personnel. It is considered that office-based workers who perform ordinary day job on weekdays only will have a minimal degree of risk and will not be required to take any specific actions. The management of fatigue may include measures to address the following issues:

- Shift employment, in which employees are rostered to work during periods when most people sleep;
- Protracted periods of work, during which employees may be compelled to work weekends in addition to weekdays
- Extended shifts as a result of shutdowns
- Periods of work in locations where the elements have an effect on an individual's level of weariness.

***Symptoms and impacts of Fatigue***

The most common symptoms associated with fatigue are: (i) Increased sleepiness; (ii) Lack of concentration; (iii) Temporary memory loss; (iv) Slowed reaction times; (v) Irritability; (vi) Headaches and general body aches; (vii) Mood swings; (viii) Reduced physical strength and capabilities; (ix) Reduced hand-eye coordination; (x) Poor judgement; (xi) Effects to general health and well-being such as loss of appetite and weight.

Fatigue impacts to human failure is provided as in the following: (i) Loss of attention; (ii) Feeling apathetic and lethargic (low energy); (iii) Inability to anticipate danger; (iv) Short term memory problems; (v) Poor decision making; (vi) Increased reaction time; (vii) Lower vigilance and alertness levels; (viii) Reduced ability to solve problems; (ix) Impatience and increase risk taking; (x) Short unplanned naps (micro sleeps); (xi) Poor performance.

***Requirements in Working time management to avoid stress and fatigue***

- Scheduling of work and non-work periods, including time-on-task and rest opportunities in shifts and the total period of time in which work is being carried out.

- No more than 12 hours will be worked at a time, including travel, unless in the event of an unforeseen occurrence necessitating labour over the 12 hour restriction. A supervisor may authorise an extension of time up to a maximum of 14 hours. Extensive approval by the Manager Responsible for Safety will be required for working hour extensions in emergency and evacuation situations.
- Rest intervals must allow for a minimum of a ten-hour respite between working shifts. Minimum break times each shift shall include a 30-minute meal period and two 15-minute rest periods during the work period immediately preceding and following the main meal period.
- Maximum number of work days not to exceed 12 work days in 14 calendar days. Assure that employees have at least 48 continuous hours off in a 14-day period.
- A minimum of 24 hours off following any block of planned night shifts
- Be able to substitute or relieve workers when unplanned or unavoidable extended hours endanger their health and safety. The substitute is ensured that (i) an employee can be considered fit-for-work if they have obtained a minimum of 6 hours sleep in the 24 hours prior to commencing work; (ii) a minimum rest period of 10 hours shall apply between shifts.
- When unanticipated circumstances necessitate overtime or shift extensions, the following processes must be taken to choose personnel for extended hours or overtime shifts on the basis of: (i) Capacity to operate within the rostering guidelines; (ii) Recent rest times, with preference given to those with the most recent shift change; (iii) Consequences for future rostering.
- Should any of the above-mentioned requirements be prolonged, a thorough risk assessment must be conducted and approved by the appropriate person prior to the extended term commencing.

### **8.3.4 Drug and Alcohol control**

#### ***Purpose***

The policy and practise were developed as part of a comprehensive plan to ensure that employees performing rail safety activities are not adversely impacted by alcohol or other drugs. Both agreements are tailored to the unique requirements of the jurisdictions in which HanoiMetro operates. Breath analysis and drug testing of HanoiMetro rail safety personnel are undertaken on a random basis and in reaction to specific situations, such as collisions and workplace safety violations.

#### ***Health Assessments***

- Pre-employment and periodical health assessments are carried out.
- Reports of a positive test are provided to the Company and this is then managed in accordance with all other positive tests

#### ***Workplace Testing***

There are three types of workplace tests: (i) Post incident tests; (ii) For cause tests; (iii) Random tests. Authorised personnel will be appointed by the Safety Department to undertake drug and alcohol testing in terms of the Railway Safety legislation. Personnel authorised will undertake training in the processes to be applied during the drug and alcohol testing programmes and may be limited to:

- Breath tests for alcohol.
- Engagement of third parties for the testing for alcohol and drugs.

- Testing only in association with the railway operations undertaken by the Company in terms of their accreditation.

When a non-negative test result is recorded the following will occur:

- The worker is stood down from all work.
- A Confirmation Test is arranged: For alcohol tests, this is a retest within 20 minutes. For drug tests, this requires that the sample be provided to a testing laboratory.
- A written advice is provided to the worker.

#### **Confirmation Test**

- If the confirmation test is negative, the worker is notified and records of the initial test are maintained. The employee is reinstated to their previous level of responsibility.
- If the confirmation test is positive, a warning for a first offence is issued, giving an interval and place for a secondary test. This secondary test will be conducted on the employee's first shift back at work, and will be restricted to alcohol.
- If the worker fails a second negative test, his or her employment will be terminated.

#### **Post Incident Testing**

Testing must take place within defined timeframes in the respective rail safety legislation applied for that state or territory after a prescribed incident: (i) collision between rolling stock; (ii) a collision between rolling stock and a person; (iii) a collision between rolling stock and a road vehicle or plant equipment; (iv) the derailment of rolling stock; (v) a breach of the rail infrastructure manager's network rules and (vi) any other prescribed incident contained within the Rail Safety legislation for the respective state or territory.

## **8.4 Leadership and Staff Involvements**

### **8.4.1 Purpose of Leadership and Staff Involvements in Safety Culture**

This section contains guidelines for successful leadership, as well as strategies for boosting staff awareness and commitment to safety.

As a result, this section is not a rigid protocol but a compilation of railway industry management experience and safety culture from throughout the world. It focuses on the top management's management style, the importance placed on safety, the creation of a critical atmosphere, and the enhancement of two-way communication inside the organisation. Thus, the leader's initiative and staff positivity are enhanced, as is the overall company's safety culture.

Human failure concerns in Vietnam's railway system in particular, and the industry in general, demonstrate that company executives frequently prioritise financial efficiency over strong safety regulations. Additionally, personnel frequently breach production safety standards through routine and situational infractions. As a consequence, it is critical to raise safety awareness and monitoring among coworkers. Additionally, safety experiences must be shared and broadened so that all employees constantly believe that "Safety will improve production efficiency, rather than that Safety is a complicated and restrictive procedure".

### **8.4.2 Leadership to develop and sustain a safety culture**

#### ***Establish a Compelling Vision for Safety***

A compelling vision improves performance, fosters change, inspires individuals, and offers context for decision making. The "why," "how," and "when" of the desired outcome must all

be included in a well-articulated vision. To gain a compelling vision for safety, the leader of company needs to:

- Develop vision for safety.
- Conduct and evaluate regular safety culture surveys.
- Conduct training to increase staff comprehension and passion for the vision.
- Clearly convey the vision to all railway personnel and the general community.
- Benchmark progress with other organisations

### ***Value Trust, Respect, and Inclusion***

The acts that leaders do throughout the course of time and throughout the company need to be consistent. Everyone should be held to the same behavioural norms and expectations; there should be no exceptions. In addition to actively modelling respectful behaviours themselves, leaders may find it necessary to implement ongoing education about appropriate behaviour for the workforce, as well as to continue actively encouraging changes that are designed to increase fairness, transparency, collaboration, inclusion, and individual responsibility. (Leape et al., 2012). The strategies to complete these targets are such as:

- Educational and training opportunities should be available to promote respect, diversity, and inclusion.
- Develop initiatives to ensure the safety of your staff, taking into account both their physical and psychological well-being.
- Reporting should be encouraged, recognised, and rewarded.
- Implement communication and resolution programmes.
- Create agreements between patients and providers, then circulate them.
- Participate in complete openness and honesty with the general public on hazardous occurrences and improvement strategies.

### ***Select, Develop, and Engage the Management board***

In order to establish and maintain a culture of safety, it is essential to offer consideration to the management board's level of expertise, abilities, and experiences, as well as its diversity. These capabilities may include specialised competencies connected to guiding cultural improvement as well as safety competencies. An engaged management board plays a key role in organisational culture and safety.

- Regular self-evaluations of management personnel's cultural and safety competence are carried out.
- Create a list of the needed capabilities that management members must possess in order to lead the improvement of the culture.
- Request that members of management spend time communicating and supporting the safety agenda on all of the floors and units.
- Maintaining regular communication and discussion of a dashboard that details passenger feedback in addition to railway staff safety and cultural data
- Adjust the displays of the dashboards so that they exhibit the quality and safety data in a manner that is split by safety-related categories.

### ***Prioritise Safety in Selection and Development of Leaders***

Focusing an emphasis on safety education may also assist reduce the gap between administrative and department leadership, equipping all leaders with the same purpose of fostering a culture of safety in their organisations while they work toward that goal.

The selection process for leaders, both current and emerging, should be based on whether or not candidates understand, are dedicated to, and align themselves with the organisation's vision for passenger and workforce safety. Additionally, candidates' communication skills

and ability to model expected safety behaviours should be considered. To guarantee that the commitment to safety is maintained throughout all levels and functional areas of the company, safety may be a topic for individual professional development as well as organisation-wide succession planning.

The key points as in the following are need to take into account in leader improvements:

- Determine the leadership capabilities of the organisation.
- Define the processes that will be used for the development of leadership at all levels.
- Make available opportunities for continuous education in the field of safety science and culture.
- Establish programmes for instructing, guiding, and advising future and present leaders through the development of appropriate systems.
- Make changes for training that spans many departments available.
- Make it possible for employees to gain knowledge from organisations and sectors outside the company.

### **8.4.3 Improve the Staff Involvement in Safety Culture**

#### ***Ensure railway employees feel individually responsible for safety***

Employees who believe they are personally responsible for the safety of the workplace are more likely to take ownership in the process of adhering to safety regulations and are also more confident to communicate out if they observe other employees acting in a hazardous manner. Individual accountability provides workers with more freedom while also assisting the entire organisation in recognising and proactively addressing potential hazards.

- Consider offering periodical competitions for the creation of safety slogans and enlisting the participation of all employees to promote inventive methods of displaying safety reminders.
- Employees who possess the autonomy, independence, and self-direction to think, act, and take safe and acceptable activities based on their knowledge and abilities.
- Railway staff should be educated in the use of coaching, mentoring, training, and praising by direct managers.
- One-on-one meetings offer managers with the opportunity to provide information to staff, so enhancing the likelihood of changing unsatisfactory behaviours and reinforcing the positive effects of behaviours that are already working well. Discussions between a leader and an employee may promote a more connected atmosphere and lead to enhanced trust between the leader and employees.

#### ***Reward a just culture***

A just culture that emphasises on identifying and resolving system problems for railroad employees when these systems collapse. CEOs guarantee that the ideals of a just culture are adopted across the whole organisation and that they influence each decision and action. The solutions for creating a just culture are as in the following:

- Develop a policy for a just culture and align across the systems, departments.
- Employ just culture concepts in all assessments and determinations.
- Expect leaders to employ just culture mechanisms across all circumstances, including those that are not noteworthy or penalised, in order to instil corporate values and use norms.
- Develop guidelines for a culture of justice and hold employees accountable.
- Treat cultural gaps as unfavourable events.
- Include the media in public explanations of errors, data, and conclusions. Protect the railway personnel from public criticism and rumours.

***Establish Organisational behaviour expectations***

Everyone in the organisation should be aware of what that behaviour expectations and unsafe behaviours are, and everyone should also be aware that it will be implemented in the same manner across the company, regardless of position, department, or any other factors that may actually occur.

It is vital to keep in mind that the process of altering behavioural norms throughout a whole company or system can be a lengthy and difficult one. Because of this, ensuring that there is also a system to reward personnel who are recognised as modelling desirable conduct is equally as essential as ensuring that there is a mechanism to reward individuals who are identified as modelling desired behaviour.

- Define the needed processes and anticipated behaviours that apply throughout the whole organisation.
- Determine the appropriate organisational reaction to behaviour that is rude or disruptive.
- Actively encourage reporting and conversations about safety, and offer feedback that is completely transparent.
- Hold all executives and employees accountable for the behaviours that are required across the whole business.
- Appreciate and reward members of the workforce who engage in predetermined safe behaviours.

## 9. SOLUTIONS FOR LONG-TERM DEVELOPMENT – DATA MANAGEMENT

### 9.1 Analysis and Reporting

#### 9.1.1 Data management regulations

##### ***Purpose***

This method is used to manage the company's technical documentation, standardisation, and information interchange amongst divisions (including the company's headquarters, differentiated metro line managers, departments, and centres).

The procedure assists the administration of the company by assuring the systematic and completeness of building technical documentation, manufacturing records for rolling stock and equipment. Simultaneously, the procedure contributes to the standardisation of system operation and maintenance records, maintaining consistency and allowing for upgrades and completion.

##### ***Classification of documents***

Internal standard documents:

- Technical specifications: They are materials being used develop and implement the management manual for the company's occupational health, safety, and quality management systems. Additionally, they are the operators' procedures, processes, and technical management standards.
- Working standard document: These are regulations governing the fundamental obligations, employment requirements, and assessment techniques of a large number of workers from many divisions, including duties and responsibilities, work processes, work procedures, and evaluation criteria.
- Administrative documents: These are the documents serving the management of the company, all kinds of meeting minutes, decisions, announcements, human resource management documents of the company.

External documents

- Relevant standards of local, industry, ministerial, national and international levels.
- Relevant regulations or decisions of local authorities or Ministry of Transport, National Safety Board.
- Specifying processes through the use of external specifications, equipment, facility takeover documents, and associated equipment systems, among others.
- Contract with a third party.
- Design and construction documentation for the new metro line, such as technical design drawings and feasibility study.

##### ***Procedure of internal technical documentation***

**Rule 1:** Responsibilities of documentation management

Responsibility of Safety Department:

- Responsible for the administration of the operating company's technical papers, which includes reacting to problems and giving out technical materials.
- When it is discovered that the new line completion document impacting the safety production data is inadequate and conflicting with the actual scenario, the Safety

Department needs to require immediate correction arrangements and data handover.

- Develop and arrange the application of rules and regulations governing the administration of the operational company's technical documentation. Additionally, the Safety Department is accountable for ensuring compliance with and monitoring the company's rules and regulations.
- In charge of building, completing, renewing and perfecting "Technical document information system". This information system helps the divisions to easily find the number, the name of the document and access the necessary documents for the technical work.
- Responsible for monitoring the whole process of collecting, categorising, distributing, analysing, storing, archiving, borrowing, and utilising technical documents for the line or company.
- Procurement of technical papers, standards or relevant document.
- Handing over technical documents to external units according to the approval of Manager Responsible of Safety.

Responsibility of other divisions:

- Assign data management employees to be responsible for organising and collecting technical documentation generated during management operations. Coordination with the Safety Department to conduct management responsibilities such as document distribution, organisation, and storage.
- Management of renovations, subcontracted maintenance (repair, maintenance), and locally sourced products. After verifying and approving the items, the document management staff forwards the modified drawings and documents to the Safety Department for marking the adjustments and updating the revised information on the "Technical document information system".
- Responsible for gathering, arranging, and preserving communications pertaining to the system's or equipment's primary technical lists.
- Charged with the responsibility of urging personnel to effectively preserve and immediately return borrowing papers.
- Organise and maintain critical hazard control documentation.
- Maintain records for vehicle, facility, infrastructure, and equipment maintenance. Monitor reports of failures and incidents, as well as incident correction actions.
- All departments and centers are not allowed to hand over technical documents to external organisations.

**Rule 2:** Regulations on archiving and handing over documents

- The contractor handed over documentation directly to metro line operators, while the Safety Department manages the handover. The appropriate specialist verifies the completed paperwork and actual performance and notifies the Safety Department of any issues discovered. The Department of Safety will coordinate and resolve the situation in accordance with applicable regulations.
- Both parties must conduct a thorough review of the information and manage the handover processes with attention during the handover of technical documents. Information about archival documentation must be recorded on the information management system.
- Once a year, the Safety Department performs an inventory of technical documentation to confirm that accounts and items correspond. Verify the status of a technical document's printed edition. Degraded or destroyed technical documentation must be fixed and duplicated immediately.



- The Safety Department's data manager will transfer the documents utilised by divisions and update status on information managing system. Subsequently, the departments or centres will assign them to the appropriate groups.
- The head of departments and centres is the initial point of contact for technical data management.
- Each department and centre will choose administrators who will be responsible for converting, revising, organising, and borrowing the department's documents.
- Utilize tier-based data management.

**Rule 3:** Regulations on lending documents

- Employees can borrow books and technical documents through the Technical document information system. The quantity of papers should not exceed three at a time and must be returned within three months.
- Special documentation, such as renovation documents, contract for repair and maintenance, subcontracts, and localisation studies, must be authorised by the appropriate department or centre manager. The quantity of papers should not exceed three at a time and must be returned within one months.
- If documents need to be reproduced, approval is required from the Manager Responsible of Safety. The quantity of papers should not exceed twenty at a time and must be returned within 15 days.
- Employees must use caution while handling borrowed documents. Make no markings, tears, disassemblies, or other alterations to the manuscript.
- Corrupted documents must be recorded in the information management system as a status. Employees who cause document damage must make restitution within 15 working days.
- Employees are accountable for the preservation and security of borrowed technical materials. It is prohibited to take out drawings, contracts, technical data, and other information from the workplace.
- For employees and document managers who violate the regulations on confidentiality of records, causing economic losses to the company, or causing social insecurity (violations on anti-terrorism, vandalism) may be held respective legal responsibility.
- When employees are redeployed or resign, they must return all the technical documents they have borrowed.

**Rule 4:** The regulation of technical documents preservation period of and regulations on expirations

- All technical papers, with the exception of photographs and periodicals, are stored for an extended period of time.
- Two years is the retention time for professional journals, while one year is the retention period for all other publications. Journals that have expired are handled by certain departments and centres.
- All special technical document, with the exception of journals, will maintain two copies. When design or maintenance documents are updated, one copy of the original document is retained for reference, and two copies of the revised document are retained in accordance with Rule 2.

## **9.1.2 Internal assessment and Safety Audit**

### ***Objectives***

Internal assessment and safety auditing are processes used to determine the effectiveness of safety programmes and the company's compliance with applicable safety regulations. The internal assessment's primary objectives are as follows:

- Maintain a safe working environment by detecting hazards and adopting appropriate measures.
- Ascertain that the facility, its equipment, and activities comply with applicable safety regulations and industry best practises.
- Assuring compliance with safety legislation by ensuring that staff adhere to the company's safety program's guidelines
- Identifying problems in an organisation's safety programme.
- It will prove helpful for optimising a company's safety management system and identifying necessary corrective actions.
- Additionally, the internal assessment and advice on safety knowledge awareness and practical implementation weaknesses will help to strengthen the safety culture and personnel responsibilities.

#### ***Responsibilities for Internal assessment and Safety Audit***

- The Safety Department is responsible for organising the annual inspection and devising a plan to conduct an internal assessment.
- The Safety Department compiles and updates records of potential hazard sources using periodic reports from Dispatching Centers and Maintenance Centers.
- The Safety Department oversees and monitors the activities of maintenance centres responsible for rolling stock, infrastructure, and railway equipment.
- The Safety Department works in collaboration with the Staff and Service Management Center and Maintenance Centers to inspect and evaluate personnel' adherence to safety regulations. It is necessary to evaluate human error and to recommend training improvements aimed at increasing worker safety awareness.
- Other Departments and Centres are responsible for developing and revising departmental safety inspection standards, as well as organising revisions and monitoring for issues detected during Safety Audit process.
- The other Departments Centers daily and weekly safety inspections at the workplace, correcting errors in the production process.

#### ***Procedure of Internal Assessment and Safety Audit in Hanoi Metro Company.***

##### **Step 1: Planning the Internal Assessment and Safety Audit**

- Daily inspection: Each individual on site is expected to conduct informal inspections of their work areas, identifying hazards and dangers and addressing them as necessary.
- Weekly inspection: Within the scope of management, the manager of the Department (Centres) and team leaders will inspect and evaluate the safety at the work area. Existing issues and essential improvements will be discussed in the meeting scheduled for the start of next week to notify each department's employees.
- Monthly inspection: The Safety Department with the Manager of Departments or Centers to synthesise and analyse each department internally. If critical hazards or significant problems exist during maintenance, it is required to organise a critical safety inspection for each item.  
The inspection plan is carried out from the 20th to the 25th of every month. The results are summarised and delivered to the company's managers during the following monthly meeting.
- Irregular inspection: Before major holidays, it is essential to organise one large-scale production safety inspection (can be combined with monthly safety inspection before the holiday). At least five days before to the holiday, the pre-holiday inspection plan should be completed.

Following incidents involving rolling stock or complete line operation, a critical safety inspection should be conducted.

**Step 2:** Carrying out the Internal Assessment and Safety Audit

- Conduct a risk assessment for important hazards. Vehicles, infrastructure, and equipment are evaluated for their technical condition. The content of each part inspection is provided in Appendix 6 .
- Verify the status of Correction Actions for any issues identified during the previous check. Verify the status of post-accident troubleshooting.
- Examine the condition of rescue supplies and equipment, including explosive-proof equipment. Conduct an audit of hazardous chemical management.
- Monitor the evolution of workplace safety regulations. Evaluating the compliance with manufacturing safety requirements, as well as inspecting and resolving infractions
- When inspectors discover violations of occupational safety standards, they have the right to make violation records and fine a penalty to relevant staffs.
- Conduct an evaluation of safety training and work to promote a safety culture.
- Departments or Centres prepare their inspection content in compliance with the applicable safety inspection items which clarified by the Safety Department.
- Departments or Centres must not substitute daily facility and equipment inspections for safety inspections.
- The Safety Department is responsible for summarising existing safety problems, proposing corrective actions from divisions, and reporting company leaders about internal assessment results.

**Step 3:** Corrective Actions

- The Safety Department discusses and reports existing safety concerns to the Manager of the Department (Centres) in order to develop corrective actions. The Manager Responsible for Safety shall accept and approve the written request for Corrective Actions, the implementation timeline, and the method of execution.
- Corrective Actions should be implemented in accordance with the requirements of applicable rules for mitigating possible dangers.
- If new issues are uncovered, a technical meeting must be convened to discuss and develop appropriate solutions. The SMS plan should be evaluated and changed as a consequence of the Corrective Actions deployment. Simultaneously, engage staff in safety training or seminars to share these experiences.
- Maintenance and troubleshooting procedures from this point on will be governed by this Corrective Actions.
- The Safety Department evaluates the results of Corrective Actions implementation of divisions and reports the results to company leaders.

## **9.2 Establishing a Railway Accident Database**

### **9.2.1 Problem of Railway Accident data in Vietnam**

During the process of carrying out the dissertation, the gathering of data required approximately 1.5 years. The data included documentation on Vietnam's Technical Design, Operation and Staff Training plan, as well as accident data from comparable systems in Europe, the United States, the United Kingdom, China, and Japan. The practical experience that the author has had in obtaining and processing data in Vietnam has revealed that this is an essential issue that needs to be handled in order to improve the safety assessment capability of Vietnam Railway. Two significant issues with the accident database are clarified as follows:

***Closed database***

The data provided in the media or widely available sources are limited to the overall number of accidents, the total number of fatalities, and the total number of individuals injured across the nation and in the most dangerous areas. In addition, certain exceptionally severe accidents will be described on television or in the press, including the time, location, and fatalities. It can be exceedingly challenging to acquire access to accident records detailing specific collisions, as well as railroad or highway accident investigations. In order to obtain these reports, it is necessary to have the appropriate permissions to access accident investigation reports.

The reason for this is due to the fact that accident reports are often kept on file at two different agencies in the area where the accident took place. These agencies are the Traffic Police and the Railway section management unit of Vietnam Railway. Since accident reports are frequently used as evidence in court litigation concerning traffic-related criminal charges, they are typically regarded as Confidential and are not made available to the general public.

In addition, the higher authorities, such as the Ministry of Police, the Ministry of Transport, and the National Safety Board, only include indications that have been summarised. Consequently, in order to get accident reports, one must physically visit each accident site and examine the information there in hard copy. The accident database that this administration in Vietnam maintains is a closed database, making it extremely challenging to utilise for risk assessment.

***Low quality of accident data***

The statistics on accidents, as studied above, only offer summarised indications such as total people and physical losses (for example, vehicle damage and infrastructure damage), but they are not categorised according to the reason of the accidents.

Because of this, it is only possible to compute accident trends across functions or accident rates for comparisons across transport modalities or comparisons between locales; nevertheless, it is not thorough enough to be used for accident analysis.

The majority of accident reports that are recorded in the accident occurrence area detail the progression of the accident based on the testimonies of witnesses and provide a description of the damage; however, these records do not indicate the cause of the event. In addition, there is not a definite and consistent method for the categorising of accident reports.

According to the instructions of the Traffic Police, the causes of the accident are limited to a total of thirteen categories. These categories include railway derailments, collisions with persons, collisions at level crossings, and driver loss of control or attention, among others.

Given these issues, it is imperative that the quality of the accident database in Vietnam, particularly the data on urban transportation and railway accidents, be improved. This is extremely pertinent to the aforementioned.

**9.2.2 Category and report contents in accident database.**

According to the practise of the UIC or the European Railway Agency, necessary accidents are categorised according to the major groups. There, it is simple to access and evaluate accident datasets, therefore enhancing references for studies on safety management. The accident categories might be included such as:

- Derailments: A derailment occurs when at least one wheel of a train or a railway vehicle in motion leaves the rail.

- Level Crossing accidents: any accident involving railway vehicles and LC users on a level crossing.
- Collisions with an obstacles: Collision with an obstacle: a collision between train and object fixed or temporarily present on or near the track.
- Collisions with another train: Collision with another rail vehicle: a front to front, front to end or a side collision between train and another train or rail vehicle, or with shunting rolling stock.
- Accident to person
- Fire in Rolling stocks
- Other types.

The detail information of accident might be clarified in categorises:

- Occurrence type: vehicle failure, level crossing, track and infrastructure failure or violated people.
- Occurrence description.
- Direct cause description: Need to be clarified the main reasons and related reasons leading to the accident.
- Underlying and root causes description
- People injuries: passenger, railway staffs or level crossing users. The severity levels must be clarified
- Total estimation of damage: loss of infrastructure, loss of material, loss of vehicle, loss of victim income.

### **9.2.3 Traffic accident data management**

The development of a traffic accident data system in Vietnam is not limited to urban or rail traffic. This database must be linked to road traffic safety data, and there is a connection between authorities about the update and utilisation of the data.

On the basis of the following tenets, suggestions for enhancing Vietnam's traffic accident data management system are presented as in the following:

- Data must be used to develop comprehensive and evidence-based traffic safety programmes;
- Technological improvements and institutional arrangements must be identified and must be sustainable;
- Data must be shared and easily accessible by stakeholders;
- The process of data collection and analysis must be straightforward to implement.

It is suggested that Vietnam establish a National Traffic Safety Portal supervised by the National Safety Board. This authority is in the best position to make connections between various database systems. They will be able to evaluate data and coordinate with stakeholders in order to develop and monitor initiatives, as well as prepare reports for stakeholders.

The steps for data collection should be as follows:

- The Ministry of Police collects accident data at the scene and imports it into the accident database in Portal.
- Ministry of Transport collects vehicle and driver license data.
- Ministry of Health collects data on human casualties

This data is aggregated and classified according to the accident location, vehicle number plate, and the ID of the participant in the accident. This information must be updated every day and can be shared with specific permissions. The Ministry of Police should manage and maintain the confidentiality of Personal ID-related data.

## 10. DISCUSSIONS AND CONCLUSION

### 10.1 Discussion on Risk assessment calculations

These train collision probabilities were calculated using logical analysis in risk analysis, along with data from the technical design of the Line HN2A, as shown above. This result must be compared to real-world operation data and experience from a similar system to ensure it is accurate. The Metro Line HN2A has been in operation since November 6th, 2021, and the most recent statistical data is for the period from November 6th to November 30th, 2021 (25 days). The statistical failure rate from the testing and validation phases was also used in the research, which was clarified in the following manner:

Testing operation phase:

- Phase 01 from 01.10.2018 to 10.12.2018 in China: including tested operating and system safety checking, operated as around 35% operation schedule. Total operation length in this phase is 85.455 train-operation-kilometres.
- Phase 02 from 11.12.2018 to 31.12.2018 in China: including tested operating at 100% system capacity with 272 trains/day. The total operation length in this phase is 70.747 train-operating-kilometres.
- Phase 03 from 06.12.2020 to 30.12.2020 in Vietnam: Testing and acceptance phase. Tested operating as 100% system capacity with 272 trains/day. Total operation length in this phase is 84.966 train-operation-kilometres.

Commercial operating (up to 30.11.2021): Operating under the working schedule of 2022-2025 with 152 trains/day. Total operation length in this period is 53.256 train-operation-kilometres.

Therefore, the total length of Train-operation-kilometres until 30.11.2021 is 294.424 train-operation-kilometres. The total of error statistical data is these operation periods given in the following Table 10.1.

**Table 10.1** Comparing the Hazard rates in theoretical calculations and Testing data

| No   | Sub-failure   | Number of failure/error rates per 10 <sup>5</sup> km-operation | Probability leading to collisions | Hazard rates (100.000 km-operation) |             |           |
|------|---|--|-----------------------------------|-------------------------------------|-------------|-----------|
|      |   |  |                                   | Real operation                      | Theoretical | Deviation |
| C3.1 | Wrong information between train driver and dispatcher                             | 3 / 1.02   | 0.002                             | 2.04E-03                            | 1.38E-03    | 0.68      |
| C3.2 | Misunderstanding between driver and dispatcher                                    | 5 / 1.69   | 0.002                             | 3.40E-03                            | 1.04E-03    | 0.31      |
| C3.3 | No information between driver and dispatcher                                      | -  | -                                 | -                                   | 5.00E-04    | -         |
| C4.1 | Train operated in Manual operating method and have not protected to against other | 1 / 0.34   | 0.001                             | 3.40E-4                             | 3.19E-05    | 0.09      |

|       |  |           |        |          |          |      |
|-------|--|-----------|--------|----------|----------|------|
|       | train operated in ATC and Limited operating method   |           |        |          |          |      |
| C4.2  | Disruption / Corruption of Train Control and Management System   | -         | -      | -        | 1.02E-06 | -    |
| C4.3  | Failure in ATC input data  | 1/ 0.34   | 0.001  | 3.04E-4  | 3.19E-05 | 0.10 |
| C5.1  | Drivers fail to check aspect of signal/reads wrong signal  | 1 / 0.21  | 0.02   | 6.79E-03 | 3.75E-02 | 5.52 |
| C5.2  | Drivers fail to react to caution signal / misjudgement   | 2 / 0.68  | 0.02   | 1.36E-02 | 3.75E-02 | 2.76 |
| C5.3  | Drivers ignored or violated safety rules   | 2 / 0.68  | 0.02   | 1.36E-02 | 5.00E-02 | 3.68 |
| C5.4  | Conflict warnings  | 7/ 2.38   | 0.02   | 4.76E-02 | 5.00E-02 | 1.05 |
| C5.5  | Bad visibility from driving cab  | 14 / 4.76 | 0.01   | 4.76E-02 | 6.75E-02 | 1.42 |
| C5.6  | Insufficient front/rear lightning in case of driving by line of sight  | 2 / 0.68  | 0.02   | 1.36E-02 | 1.35E-02 | 0.99 |
| C6.1  | Safety Brake failure or inefficiency   | -         | -      | -        | 1.32E-04 | -    |
| C6.2  | Inefficient service braking  | -         | -      | -        | 1.32E-04 | -    |
| C6.3  | Deterioration/Cracking of brake discs due to a parking brake remaining applied or remaining pressure in brake cylinder   | -         | -      | -        | 6.08E-04 | -    |
| C6.4  | Rupture of a semi-automatic coupler / Untimely uncoupling  | 2/0.68    | 0.0005 | 3.40E-04 | 3.02E-04 | 0.89 |
| C6.5  | Loss of integrity: bad operation during coupling (excessive speed)   | 3/1.02    | 0.0005 | 5.09E-04 | 5.08E-04 | 1.00 |
| C6.6  | Overspeed due to traction system failure   | 2/0.68    | 0.0005 | 3.40E-04 | 2.43E-04 | 0.71 |
| C6.7  | Wheel-set failure  | 2/0.68    | 0.001  | 6.79E-04 | 6.08E-04 | 0.90 |
| C6.8  | Low wheel/rail adhesion factor leading to increase the stopping distance (weather condition included)                    | 3/1.02    | 0.001  | 1.02E-03 | 3.04E-04 | 0.30 |
| C6.9  | Failure of suspension, bogie, connection vehicle-bogie, gauge dynamics, not respected gauge, interfaces vehicle traction | 5/1.02    | 0.0005 | 8.49E-04 | 9.13E-04 | 1.08 |
| C6.10 | Loss of car-body integrity   | -         | -      | -        | 6.08E-04 | -    |
| C6.11 | Too high traction effort or inefficient braking when a train is rescued by another one                                   | -         | -      | -        | 1.32E-04 | -    |
| C7.1  | Adhesion problem: design of the wheel-rail interface not taking into account   | 3/1.02    | 0.0005 | 5.09E-04 | 3.02E-04 | 0.59 |

|      |   |        |        |          |          |      |
|------|---|--------|--------|----------|----------|------|
| C7.2 | Adhesion problem: presence of external elements compromising the adhesion | 7/2.38 | 0.0005 | 1.19E-03 | 7.39E-04 | 0.62 |
|------|---|--------|--------|----------|----------|------|

The number of failures is the total number of errors in a type of failure which is counted and reported in the operating period, corresponding to the total length of train-operation-kilometres from the testing phase and current commercial operation until 30.11.2021. Therefore, the error rate could be calculated by dividing the number of failures by the total length of train operation kilometres (294.424 train-operation-kilometres).

This total number of failure or error rates reflected the dangerous situation/condition, however, it needs more condition simultaneously leading to an incident or accident. For example, when driver miscommunicated to OCC, it might be a dangerous situation in which the OCC do not have enough real-time information of train operation, and the driver could not receive the controlling command from OCC. However, this dangerous might not completely result in Train Collision. It only happened when the signal could not be reconnected, there are the failures in driver recognising and performing, simultaneously, ATC system and emergency brake. We use Event Tree Analysis to calculating the Probability leading to collisions, for example as in the Figure 50. The failure probability of the ATC system and vehicle technical errors is usually 1% to 2%, the failure rate of the driver is approximately 2% to 6% (Dingus et al. 2016) and the emergency brake is around 50% due to the evaluating time (Wang 2014; Ruijters 2018). Therefore, the calculation of the probability leading to collisions is deviated from 0.0005 to 0.002 based on the type of errors as in the Table 10.1.

|                           | ATC fails to take correct data |      | Driver errors in evaluation |     | Both service brake and emergency brake failure to stop the Train in safe area |      | Trigger event: Presence of another train, people or objects on track |     | Assessment |              | Probability leading to Hazards |           |
|---------------------------|--------------------------------|------|-----------------------------|-----|---|------|--|-----|------------|--------------|--------------------------------|-----------|
|                           |                                |      |                             |     | Success   | 0.98 |  | No  | 0.95       |              |                                |           |
|                           |                                |      |                             |     |   |      |  |     |            |              |                                |           |
|                           |                                |      | Success                     | 0.9 |   |      |  |     |            |              |                                |           |
|                           |                                |      |                             |     | Failure   | 0.02 |  | Yes | 0.05       | Castatrophic |                                | 0.000855  |
|                           | Success                        | 0.95 |                             |     |   |      |  |     |            |              |                                |           |
|                           |                                |      |                             |     | Success   | 0.98 |  | No  | 0.95       |              |                                |           |
|                           |                                |      | Failure                     | 0.1 |   |      |  |     |            |              |                                |           |
|                           |                                |      |                             |     | Failure   | 0.02 |  | Yes | 0.05       | Catastrophic |                                | 0.000095  |
| Failure in ATC input data |                                |      |                             |     |   |      |  |     |            |              |                                |           |
|                           |                                |      |                             |     |   |      |  |     |            |              |                                |           |
|                           |                                |      |                             |     | Success   | 0.95 |  | No  | 0.95       |              |                                |           |
|                           |                                |      |                             |     |   |      |  |     |            |              |                                |           |
|                           |                                |      |                             |     | Failure   | 0.05 |  | Yes | 0.05       | Catastrophic |                                | 0.0001125 |
|                           | Failure                        | 0.05 |                             |     |   |      |  |     |            |              |                                |           |
|                           |                                |      |                             |     | Success   | 0.9  |  | No  | 0.95       |              |                                |           |
|                           |                                |      | Failure                     | 0.1 |   |      |  |     |            |              |                                |           |
|                           |                                |      |                             |     | Failure   | 0.1  |  | Yes | 0.05       | Catastrophic |                                | 0.000025  |
|                           |                                |      |                             |     |   |      |  |     |            |              |                                |           |
|                           |                                |      |                             |     |   |      |  |     |            | Total        |                                | 0.0010875 |

**Figure 49** Principle Event Tree Analysis for Failure in ATC input

The research on test data indicated that several low significant deviation in case of Sub-failure C5.1, C5.2, C5.3. This failure group concentrated in human failure. According to the findings of the study (Luong et al. 2019), there is awareness about human error in the operation of urban railways in Vietnam. The study is based on the statistical analysis and evaluation of the perspectives of researchers, engineers, and local authorities in the railway sector in order to determine workers' perceptions of safety risks and probable safety problems in Vietnam's railway industry. Whereas the problems of stress and fatigue and the problem of violation are the most significant issues impacting human performance in railway operations. Human failure estimates are therefore established at a higher level in technical



design and theoretical risk assessment, demonstrating the importance and concern of the operator in controlling and managing human performance. This is represented in the company's safety principles, procedures, as well as safety culture which specifies in the Safety Management System of company.

Furthermore, the problem of stress and fatigue among railway workers will not be accurately and completely reflected during the testing phase due to the short time period and the high number of drivers or controlling / maintenance staff, as well as the fact that there will be almost no absences due to illness. According to (Luong et al. 2019), the problem of workload is usually a noticeable issue, and the worker is required to work for a long period of time and may suffer from sleep disorders. Workers are rarely encouraged to refrain from reporting to work after a long working shift, and they are also rarely provided with medical or psychological support. As a result, statistics from the operation report and error recording in the short testing phase will not be able to properly quantify and identify the number of errors that are indirectly caused by human performance.

Additionally, there is some testing data that is substantially greater than the calculation for wheel-rail adhesion. Up to 13 occasions in sub-failure of C6.8 C7.1 and C7.2, the train did not come to a complete stop or emergency stop in the right place. This category does not include failures of the ATP system or the driver's response to braking. These are braking system malfunctions characterised by decreased brake efficacy or a brake system's inability to respond. This is partially explained factually by the fact that Vietnam's high humidity and wet season limit braking efficiency in certain operating conditions. Additionally, the subjective reason stems from the railway infrastructure's and vehicle subsystem's upkeep. The section on Recommendations will address possible solutions.

## 10.2 Limitations and Recommendations

Fault Tree Analysis is used as the primary risk assessment approach in this study. Fault Tree Analysis is not a novel method; it has been developed for a very long period, and there are several modifications that further enhance its accuracy. In addition, the establishment of the Safety Management System has been standardised in order to implement the life-cycle management of railway projects. The thesis's primary issues may not be state-of-the-art, but a novel application strategy is required in light of restricted managerial capacity and undeveloped technology.

As in literature reviews, SMS and risk assessment methods is directed and built based on highly developed railway systems, on the basis of a thriving industry that can easily manufacture, enhance and maintain vehicles and equipment such in Europe, Canada, Australia, and UK. Likewise, workers in these countries also have high-quality skills and good work discipline. Therefore, SMS is must-be-applied and is strict regulations. However, in the case of Vietnam, the URMT Line 2A is the first and only urban rail line in Vietnam which has been put into revenue service since November 2021 with an operational safety assessment launched for the first time, and long-term remains for the whole life cycle. Meanwhile, all the national main lines with narrow gauge 1000mm are too old and outdated in terms of infrastructure and technical standards that need massive renovation. And all of them have not been evaluated for safety and complied adequately with any standardised. The same is true in many less developed countries in Asia. Therefore, the new approach of the thesis is how to apply modern management standards to a system that is still very limited in terms of techniques and skilled workers.

The dissertation demonstrate through a literature review that risk management research is diverse and comprehensive. However, few studies have been conducted on urban railway

systems, with the majority of research focusing on risk analysis for high-speed railways or intercity railway lines. Additionally, there are few case studies for growing countries with obsolete railway infrastructure and a lack of managerial expertise. In fact, in the context of Vietnam, the concepts of system safety, RAMS, and risk assessment methods are still entirely new, and not many experts understand these issues. Therefore, a system of training and research in this field is still very limited, affecting the quality of technical management of the metro system. The practice demonstrates that we require a risk assessment method that is not overly complicated, simple to develop, and sufficiently effective for the initial phase of Vietnam's railway industry renovation.

Railway accident data in Vietnam is not standardised at all, has not been classified according to Common Safety Methods, and has no accident database. The operational data and failure rate data of metro lines are unavailable as no lines are in operation yet. Therefore, the thesis uses the FTA method as the primary risk assessment method to make it easy to apply and develop and upgrade in the future. Incident data will be classified and collected based on FTA analysis to reference and correct basic calculations in the thesis.

The dissertation concludes, based on the aforementioned difficulties, that it is necessary to continue researching the topic of risk management in Vietnam, utilising the safety risk concept to learn and create risk assessment approaches. In addition, on the basis of the SMS framework developed for Metro Line HN2A, it is necessary to continue to develop a stricter and more proactive management process, with a greater emphasis on Safety Culture, in attempt to overcome the poor safety attitude in the railway industry, analysed in Chapter 3.

According to RAMS railway, safety assessment is an internal technical evaluation of the system's risk assessment, human and system performance. However, while executing urban railway projects in Vietnam, numerous inefficiencies or safety issues develop due to project management issues such as insufficient management capability, lack of control over contractor contracts, delayed progress, corruption. The dissertation suggests that, from the perspective of safety management according to the project life-cycle, it is necessary to manage the risk assessment more attentively during the System definitions, system specifications, and Installations stages to ensure that the system is correctly analysed and the requirements are set. extensive and exhaustive standards for contractors. This will facilitate the Safety Acceptance task and assure the system's effectiveness and safety.

### 10.3 Conclusions

The dissertation considered establishing the Safety Management System for LRT line HN2A and further developing for UMRT system in Vietnam. The Safety Management System includes risk assessment methods, engineering maintenance procedure, accident response plan and Safety Culture development.

**Firstly**, application of constructed fault tree and event tree models for other rail transit systems in general has been discussed in literature review. These discussions based on the common characteristics of the UMRT Line 2A which are also similar with the other lines in the near future, such as elevated or underground line, electrification uses 750VDC or other voltages, CBTC signalling with or without trackside signals, 04 coach train set or longer, operator's activities, thus lead to groups of faults and events which can be common understood when implementing assessments. For the lines with mix operations, if any, these Fault Trees and Event Trees should be built up separately.

The motivation of the study is to focus on application this for other rail transit system in general only. The details of each application for each individual line shall be based on detail

technical specifications and conditions of operations; and shall be determined according to final safety assessments of that line. The research can become a basis for rail transit system with the same level of technical specifications and condition of our line HN2A. By reviewing and analysing the methodologies and procedures for hazard identification and evaluation to risk assessment, present study selected the FTA method to apply properly and can be applied to UMRT in Vietnam as well as Line HN2A, because the practice demonstrates that we require a risk assessment method that is not overly complicated, simple to develop, and sufficiently effective for the initial phase of Vietnam's railway industry renovation. The FTA is established in technical management process. This technique is well-suited for assessing complicated systems with numerous components and variable hazard occurrences under various operating situations. This technology enables the creation of an open database for the study and update of discrete components. This is significantly highlights that the research results are accurate and deployed only with actual failures data of line HN2A. In order to enable further and more exactly risk analysis, the on time operation data need to be frequently updated accordingly during line's operation in which the research team is continuing to collect and update. These estimates need to be continued and updated as statistical data from the accident database becomes available, which will be compatible with the Hanoi Metro company's SMS. In addition, this risk assessment approach and safety management strategy can continue to be used to the Hanoi metro lines that will be constructed subsequently.

**Secondly**, rolling stock and other equipment are employed to carry out railway operations on a regular daily schedule. It is necessary to use, maintain, transport, and store in accordance with the manufacturer's recommendations to ensure that it remains safe in all situations. The procedures referred in the dissertation aim to make sure that staff involved in the operation of rolling stock is aware of and compliant with the engineering and operational systems requirements. Among the several varieties of urban railway equipment, this document also concentrates on civil structure maintenance and divides the task into three categories: inspection, planning, and repairs. Each item associated with track and civil structures must be maintained in good condition, potential failures must be avoided through appropriate measures, and necessary repairs must be carried out on a timely basis through appropriate measures to ensure the continued safe operation of urban railways and to maintain the relevant structures in good condition. The following procedures define the requirements for track and civil structure maintenance on the individual metro lines operated and managed by HanoiMetro; and applies to companies and individuals directly involved in maintaining railway infrastructure.

**Thirdly**, the Incident response methods outlined in the dissertation are intended to advise HanoiMetro workers of the processes to be followed in the case of an incident affecting an operational piece of rolling stock. The organisations and individuals engaged in the urban railway are accountable for resolving the issue collaboratively; evacuees must be rescued immediately, and the incident site, national property must all be safeguarded. In addition, these processes alert and report an accident to the necessary organisations and persons within a reasonable timeframe in order to restore the affected line to train traffic as quickly as feasible. Finally, they attempt to prevent the catastrophe from happening again by implementing precautionary measures.

The dissertation's ultimate objective is to develop an effective safety culture. The SMS plan's defined tools serve as the basis for railroads to achieve this objective. Strong safety culture at a railroad firm may assist minimise the number of public and employee fatalities and injuries, as well as the environmental effect of accidents.

## REFERENCES

- ATC (Apave – Certifier - Tricc) Consultance (2019). Safety reports: Results of Working programs of Safety Certification group in China and Vietnam. March 2019
- [AMTRS] Australian Ministry for Transport and Regional Services (2006). National Transport Commission (Model Legislation — Rail Safety Bill) Regulations 2006.
- Adams, J. (2003). Risk and Morality. University of Toronto Press Incorporated, Toronto Buffalo London.
- Adler, R. et al. (2010). Integration of component fault trees into the UML. In Workshops & Symposia at MODELS.
- Asmussen, S. (2003). Applied probability and queues, 2nd ed. ed, Applications of mathematics. Springer, New York.
- Andersen, T. (1999). Human Reliability and Railway Safety, Proceedings of the 16th European safety, Reliability, and Data Association (ESREDA) Seminar on Safety and Reliability in Transport, pp. 1–12.
- Anderson R. and Barkan C. (2004) Railroad Accident Rates for Use in Transportation Risk Analysis. Transport Research Board, No. 1863, pp.88-98. National Research Council: Washington DC
- Aven T. (2015). Risk assessment and risk management: review of recent advances on their foundation, European Journal of Operational Research, doi:10.1016/j.ejor.2015.12.023
- Bahr, N. (2015). System Safety Engineering and Risk Assessment: A Practical Approach 2nd Ed. New York: CRC Press.
- Ball, D. J., & Watt, J. (2013). Further Thoughts on the Utility of Risk Matrices. Risk Analysis, Vol. 33/ 11, pp. 2068-2078.
- Bayuk, A. (2008). Aviation safety management systems as a template for aligning safety with business strategy in other industries. The Business of Safety: a matter of Success. Symposium: Baltimore, Maryland.
- Baysari M., McIntosh A., Wilson J. (2008). Understanding the human factors contribution to railway accidents and incidents in Australia. Accident Analysis and Prevention. Vol 40, pp.1750–1757
- Bearfield G. and Marsch W. (2005). Generalising Event Trees Using Bayesian Networks with a Case Study of Train Derailment. Conference Paper in Lecture Notes in Computer Science
- Beckerley, J. G. (1957). Safety Aspects of Nuclear Reactors. New York: D Van Nostrand.
- Bernstein, P.L. (1996) Against the Gods: The Remarkable Story of Risk. New York: John Wiley & Sons.
- [BEU] (2020). Bundesstelle für Eisenbahnunfalluntersuchung: Jahresbericht 2019, Bonn, 2020.
- Beugin J., Renaux D., Cauffriez L., (2006). A SIL Quantification Approach based on an Operating Situation Model for Safety Evaluation in Complex Guided Transportation Systems Journal of Reliability Engineering and System Safety, Elsevier, Vol. 92, pp1686-1700, 2007, ISSN 0951-8320
- Blischke, W.R. and Murthy, D.N.P. (2003). Case Studies in Reliability and Maintenance, John Wiley & Sons, USA.
- Bobbio A., L. Portinal, M. Minichino, E. Ciancamerla (2001). Improving the analysis of dependable systems by mapping fault trees into Bayesian Networks. Reliability Engineering and System Safety Vol. 71/3, 249-260. [https://doi.org/10.1016/S0951-8320\(00\)00077-6](https://doi.org/10.1016/S0951-8320(00)00077-6)
- Boyle T. (2002). Health and safety: risk management. England: IOSH Services Ltd.,
- Bowles J. (2003). An assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis. 2003 Proceedings Annual Reliability and Maintainability Symposium.
- Braband, J., Brehmke, B., Griebel, S., Peters, H., Suwe, K. (2006). The CENELEC-Standards regarding Functional Safety. Hamburg: Eurailpress.
- Braband (2012). Semi-Quantitative Risk Assessment of Technical Systems on European Railways. In: Flammini F. (Eds). Railway Safety, Reliability and Security – Technologies and Systems Engineering (p. 54-64). USA : IGI Global
- Braglia, M. (2000). MAFMA: multi-attribute failure mode analysis. International Journal of Quality & Reliability Management. Vol. 17 No. 9, pp. 1017-1033.
- Bristol, N. D (2004). Shared mental models: conceptualisation and measurement. PhD Thesis, School of Mechanical, Materials and Manufacturing Engineering, University of Nottingham.
- Breemer, J. (2009). RAMS and LCC in the Design Process of Infrastructural Construction Projects: an Implementation Case. Master's thesis, University of Twente.
- Breemer, A. and E. Braaksma (2001). An approach to Improving the Performance of Rail Systems in a Design Phase. World Congress on Railway Research, 1–9.
- Britton M., Asnaashari S. & Read G. (2017). Analysis of train derailment cause and outcome in Victoria, Australia, between 2007 and 2013: Implications for regulation, Journal of Transportation Safety & Security, 9:1, 45-63
- Brooks, S., (2011). Handbook of Markov chain Monte Carlo methods and applications. CRC Press
- Brualdi, R.A., (1999). Introductory combinatorics, third edition Prentice Hall. Upper Saddle River: NY
- [BUEDRI] Beijing Urban Engineering Design & Research Institute Co., Ltd (2010). Hanoi Urban Railway Project: Cat Linh – Ha Dong Line. Technical Design and Feasibility report statement. November 2010
- [BUEDRI] Beijing Urban Engineering Design & Research Institute Co., Ltd (2009). Hanoi Urban Railway Project: Cat Linh – Ha Dong Line. Volume 1: Track, Station and Line. May 2009
- [BUEDRI] Beijing Urban Engineering Design & Research Institute Co., Ltd (2012). Hanoi Urban Railway Project: Cat Linh – Ha Dong Line. Volume 2: Traffic Organization and Operation Management.
- [BUEDRI] Beijing Urban Engineering Design & Research Institute Co., Ltd (2011). Hanoi Urban Railway Project: Cat Linh – Ha Dong Line. Volume 3: Rolling stocks. March 2011
- [BUEDRI] Beijing Urban Engineering Design & Research Institute Co., Ltd (2014). Hanoi Urban Railway Project: Cat Linh – Ha Dong Line. Volume 4: Signal System. December 2014

- [BUEDRI] Beijing Urban Engineering Design & Research Institute Co., Ltd (2015). Hanoi Urban Railway Project: Cat Linh – Ha Dong Line. Volume 8: Risk Assessments and Safety Management.
- Burke R. (1999). Project management: planning and control techniques, 3rd Edition. UK: Wiley.
- Cagno, E., DiGiulio, et al (2000). Risk and cause-of-risk assessment for an effective industrial safety management. *International Journal of Reliability, Quality and Safety Engineering*, 7/ 2, pp. 113-128.
- Carmignani (2009). An integrated structural framework to cost-based FMECA: The priority-cost FMECA. *Reliability Engineering and System Safety*, Vol.94, pp.861-871.
- Chapman C. & Ward S. (1997). Project risk management: processes, techniques and insights, 1st Ed. England: Wiley.
- Chapanis, A. (1996). Human factors in system engineering. New York: John Wiley and Sons.
- CENELEC – EN 50126 (2018). Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- Chen, S., Ho, T. & Mao, B. (2007). Reliability evaluations of railway power supplies by fault-tree analysis. *IET Electric Power Applications*. Vol. 1, Issue 2.
- Childs, P. (2019). *Mechanical Design Engineering Handbook* (Second Edition). Butterworth-Heinemann.
- Cole, J. W., T. R. Regenie, and R. J. Wilson (1985). Nuclear Power Generating Station Operability Assurance Reliability, Availability, and Maintainability Application for Maintenance Management. *IEEE transactions on power apparatus and systems* 4, 785–789.
- Chin, K.S., Wang, Y.M., Poon, G.K, Yang, J.B. (2009). Failure mode and effect analysis using a group-based evidential reasoning approach. *Computers & Operation Research*, Vol. 36, pp. 1768-1779.
- Cole, G. K. (1998). Practical Issues Relating to Statistical Failure Analysis of Aero Gas Turbines. *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering* 212(3), 167–176.
- Cook R. (2008). Simplifying the Creation and Use of the Risk Matrix. In: Redmill F., Anderson T. (eds) *Improvements in System Safety*. London: Springer.
- Cox, L. A. Jr., Babayev, D., Huber, W. (2005). Some limitations of qualitative risk rating systems. *Risk Analysis*, Vol 25, Issued 3, p.651–662.
- Cox, L.A. (2008). What's wrong with Risk Matrices? *Risk Analysis*, Vol. 28, No. 2, pp. 497-512
- Cox, L.A. (2009). *Risk Analysis of Complex and Uncertain Systems*. New York: Springer
- Cooper, M. D. (2000). Towards a model of safety culture. *Safety Science*, Vol. 36/2, p.111-136.
- Das B. (1999) Representing Uncertainties Using Bayesian Networks. DSTO, Electronics and Surveillance Research Laboratory, AR-011-177. Salisbury, Australia.
- Dey PK. (1999). Process re-engineering for effective implementation of projects. *International Journal of Project Management*, Vol 17, Issued 3, p.147-159.
- Dingus T, Feng G, Lee S, Antin J, Perez M, Buchanan-King M, Hankey J. (2016). Driver crash risk factors and prevalence evaluation using naturalistic driving data. *Proceedings of the National Academy of Sciences of the USA*. 113 (10) 2636-2641. <https://doi.org/10.1073/pnas.1513271113>
- Dindar S., Kaewunruen, M. An, Sussman J.M (2017) Bayesian Network-based probability analysis of train derailments caused by various extreme weather patterns on railway turnouts. *Safety Science*. <https://doi.org/10.1016/j.ssci.2017.12.028>
- Dinmohammadi F., Alkali B., Shafiee M. (2016). Risk Evaluation of Railway Rolling Stock Failures Using FMECA Technique: A Case Study of Passenger Door System. *Urban Rail Transit* 2, 128–145
- Ditlevsen O. (2003). Decision modeling and acceptance criteria. *Structural Safety*, Vol. 25/2, p. 165–191.
- Directive 2004/49/EC on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railways undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive), L164 p44-113, 29 April 2004, Official Journal of the European Union (2004).
- Directive 2001/16/EC (2001). Directive of the European Parliament and of the Council on the interoperability of the trans-European conventional rail system, Commission of the European Communities, Brussels, 19 March 2001
- Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety.
- Dodgson J., Spackman M., van der Veer J. and Maunders S. (2003). Train Protection - Review of economic aspects of the work of the ERTMS Programme Team. Health and Safety Executive 2003
- Doytchev D. and Szwillus G. (2008). Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria. *Accident Analysis & Prevention*, Vol. 41, Issue 6, pp. 1172-1179. <https://doi.org/10.1016/j.aap.2008.07.014>
- Dunjó, V. Fthenakis, J. a Vilchez, and J. Arnaldos, Hazard and operability (HAZOP) analysis. A literature review, *Journal of Hazardous Materials*, Vol. 173, Issued 1–3, pp. 19–32.
- EN 50129 (2018). Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.
- [ERA] European Railway Agency (2020). Report pm Railway safety and interoperability in the EU, 2020. Luxembourg: Publications Office of the European Union
- [EUAR] EU Agency for Railways (2020). Introduction to the European Railway Safety Culture Model. Safety Culture Series. Luxembourg: Publications Office of the European Union, 2020
- Evans AW. (2011a). Fatal train accidents on Europe's railways: 1980–2009. Vol 43 /1, pp.391–401.

- Evans AW. (2011b). Fatal accidents at railway level crossing in Great Britain 1946-2009. In: *Accidents Analysis and Prevention* (2011) No. 43, p. 1837-1845
- Evans AW. (2021). Fatal train accidents on Europe's railways: An update to 2019. *Accident Analysis & Prevention*, Vol. 158, pp. 106-182.
- [FAA] Federal Aviation Administration (2000). *FAA System Handbook*. Chap. 8: Safety Analysis/Hazard Analysis Tasks.
- Farrington-Darby, T., Wilson, J. R., and Norris, B. J (2005). Investigating train driver behaviour. The use of lineside information when regulating speed. In *Rail human factors: supporting the integrated railway* (Eds J. R. Wilson, B. J. Norris, T. Clarke, and A. Mills), pp. 60-69.
- Fernández-Muñiz B, Montes-Peón JM, Vázquez-Ordás CJ (2007). Safety culture: analysis of the causal relationships between its key dimensions. *Journal of Safety Research*. Vol. 38/6, 627-641.
- Feyer A. M, and Williamson A. M., (1998) "Human factors in accident modelling". In: Stellman, J.M. (Ed.), *Encyclopaedia of Occupational Health and Safety*, Fourth Edition, Geneva: International Labour Organisation, 1998.
- Flammini F., Gaglione A., Mazzocca N., Pragliola C. (2009). Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures. *CRITIS'08 3rd International Workshop on Critical Information Infrastructures Security*, p. 180-189. Berlin Heidelberg : Springer-Verlag
- French S. and Steel T. (2017). The Investigation of Safety Management Systems and Safety Culture. Discussion paper 2017-20. *OCED International Transport Forum*, 08/2017
- Fussell, J.B. (1973). Synthesis tree model – A formal methodology for fault tree construction. *Journal of Nuclear Engineering and Design*, Vol. 52, pp. 337-360.
- Gagniuc, P.A. (2017). *Markov Chains: From Theory to Implementation and Experimentation*. John Wiley & Sons, Inc., Hoboken, NJ, USA. <https://doi.org/10.1002/9781119387596>
- Galante E., Bordalo D., Nobrega M. (2014). Risk Assessment Methodology: Quantitative HazOP. *Journal of Safety Engineering* 2014, Vol3, Issued 2, p.31-36
- Garcia, P., Schirru, R., Frutuoso e Melo, P. (2005). A fuzzy data envelopment analysis approach for FMEA. *Progress in Nuclear Energy*, Vol.46, Issued 3-4, pp.359-373
- Garland, D. (2003). *Risk and morality*. University of Toronto Press Incorporated, Toronto Buffalo London
- Gibson H. , Mills A., Gregory J., Harrison C., Woods M. (2017). The Role of Human Factors in Supporting Safety Learning from Railway Incidents. 27th International Railway Safety Council. Hongkong.
- Glendon, A.I., Stanton, N.A. (2000). Perspectives on safety culture. *Safety Science*, 34, 193-214
- Green, S. B. (1991). How Many Subjects Does It Take To Do A Regression Analysis. *Journal Multivariate Behavioural Research*. Volume 26, Issue 3, pp. 499-510.
- Haimes, Y. Y. (2009). *Risk modelling, assessment, and management* (3rd ed.). A John Wiley & Sons Inc. Publication.
- Hall, S.(1997). *Railway Accidents*, Ian Allan Publishing, Shepperton, U.K.
- Hancock P.A., Szalma, J.L. (2008). *Performance under Stress*. Ashgate Publishing: England.
- Hamersma, B. and M. S. Chodos (1992). Availability and Maintenance Considerations in Telecommunications Network Design and The Use of Simulation Tools. In *AFRICON'92 Proceedings*, 3rd AFRICON Conf, pp. 267-270. IEEE
- Hartman, R. O., & Betz, N. E. (2007). The Five-Factor Model and Career Self-Efficacy. *General and Domain-Specific Relationships*. *Journal of Career Assessment*, Vol. 15 / Issued 2, pp. 145-161.
- Heldman K. (2005). *Project Manager's Spotlight on Risk Assessment*. Harbor Light Press
- [HSC] Health and Safety Commission (1993). *Organising for safety: Third report of the human factors study group of ACSNI (Advisory Committee on the Safety of Nuclear Installations)*. UK: HSE Books.
- [HSE] Health and Safety Executive (2001). *A guide to measuring Health and Safety Performance*
- Henselwood F, and Phillips G. (2009). The development of risk criteria for high severity low frequency events. *Process Safety Progress* Vol 28/1, 11-14. <https://doi.org/10.1002/prs.10279>
- Høj, N. P., & Kröger, W. (2002). Risk analyses of transportation on road and railway from a European perspective. *Safety Science*, 40(1-4), 337-357
- Horny, M. (2014). *Bayesian Network*. Technical report No.5 for PM931: Directed Study in Health Policy and Management. Boston University's School of Public Health.
- Kecklund, L., Ingre, M., Kecklund, G., Söderström, M., Åkerstedt, T., Lindberg, E., Jansson, A., Olsson, E., Sandblad, B., (2001). The TRAIN-project: railway safety and the train driver information environment and work situation – a summary of the main results. *Signalling Safety* 2001, London.
- Khakzad N., Khan F., Amyotte P. (2011). Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering and System Safety* 96, 925-932.
- IEC 61508:2010 (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems*.
- [IEAEC] International Ergonomics Association Executive Council. (2000). Definition of ergonomics. [http://www.iea.cc/01\\_what/What%20is%20Ergonomics.html](http://www.iea.cc/01_what/What%20is%20Ergonomics.html)
- [IRICEN] Indian Railways Institute of Civil Engineering (2014). *Investigation of Derailments*. Pune 411001
- [IRSE] Institution of Railway Signal Engineers (2015). Understanding SIL. International Technical Committee. Report on topic 38. *IRSE News*, Issued 215, October 2015
- [ICSI] Institut pour une culture de sécurité industrielle (2018). *Safety Culture: From Understanding to Action*. "Safety Culture" working group <http://www.icsi-eu.org/>
- Johansen, I. L. (2010). *Foundations of risk assessment*. ROSS report 201002, Norwegian University of Science and Technology, Trondheim, Norway.

- Jorna, R. and Kiewiet, D. J (2007). Planning, reasoning and patterns of inferences: an empirical study into the reasoning of staff planners in the Netherland railways. In People and rail systems: human factors at the heart of the railway (Eds J. Wilson, A. Mills, T. Clarke, and B. Norris). Ashgate Publishing
- [JICA] Japan International Cooperation Agency (2015). Rolling Stock Maintenance Manuals. TA Project to strengthen the capacity of regulator and to establish operation and maintenance company of metro railway lines in Hanoi.
- [JICA] Japan International Cooperation Agency (2016). Final Report Volume 1. TA Project to strengthen the capacity of regulator and to establish operation and maintenance company of metropolitan railway lines in Hanoi City.
- [JTSB] Japan National Safety Board (2022). Statistics of Railway Accident and Statistics of Railway Serious Accident. Achieved from [https://www.mlit.go.jp/jtsb/statistics\\_rail.html](https://www.mlit.go.jp/jtsb/statistics_rail.html) on May 2nd, 2022
- Ju, H., Xiang, W., Lu, Y. & Du, X. (2011). Integrating RAMS approach on the safety life cycle of rail transit. In: Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2011 International Conf. IEEE, 801-803
- Judge, T. A., Higgins, C. A., Thoresen, C. J., & Barrick, M. R. (1999). The Big Five Personality Trait, General Mental Ability, and Career Success Across the Life Span. *Personnel Psychology*, Vol. 52 / Issued 3, pp.621-652.
- Jurtz S. (2019). Untersuchung zur Einführung von ETCS im Kernnetz der S-Bahn Stuttgart: Abschlussbericht. WSP Infrastructure Engineering GmbH: Frankfurt am Main
- Kaplan, S. & Garrick, J. (1981). On the quantitative definition of risk. *Risk Analysis*, 1, 11–27.
- Kovács B., Péterfi O., Kovács-Deák B., Székely-Szentmiklósi I., Fülöp I., László-István B., Boda F., (2021). Quality-by-design in pharmaceutical development: From current perspectives to practical applications, *Acta Pharmaceutica*, 10.2478/acph-2021-0039, 71, 4, (497-526),
- Leape, Berwick D, Clancy C, (2009). Transforming healthcare: A safety imperative. *Quality and Safety in Health Care*. 18:424–428. <http://qualitysafety.bmj.com/content/18/6/424>. doi: 10.1136/qshc.2009.036954
- Lee, W.S, Grosh, D.L, Tillman, F.A, Lie, C.H. (1985). Fault Tree Analysis, Methods and Applications – A review. *IEEE Transaction on Reliability*, Vol. R-34, No. 3, pp. 194-203
- Lisnianski A., Frenkel I., Ding Y. (2010). Multi-state System Reliability Analysis and Optimization for Engineers and Industrial Managers. Springer – Verlag: London
- Li, Y., Mi, J., Huang, H., Zhu, S., & Xiao, N. (2013). Fault tree analysis of train rear-end collision accident considering common cause failure. *Maintenance and Reliability* 2013; 15 (4): 403–408.
- Lin C, Saat M, Barkan C. (2012). Analysis of causes of major train derailment and their effect on accidents rates. In: *Transportation Research Record: Journal of the Transportation Board*, Vol. 2289, pp. 154-163
- Lin C, Saat M., Barkan (2016). Fault Tree Analysis of Adjacent Track Accidents on Shared-Use Rail Corridors. : *Transportation Research Record: Journal of the Transportation Board*, Vol. 2546, pp. 129-136.
- Lin, Chenyu; Saat, Mohd; Barkan, Christopher (2012) Analysis of causes of major train derailment and their effect on accidents rates. *Transportation Research Record: Journal of the Transportation Board*. Vol. 2289, p. 154-163
- Liu, H.C, Liu, L., Liu, N. (2013). Risk evaluation approaches in failure mode and effects analysis: A literature review. *Expert Systems with Applications*, Vol. 40, pp. 828-838.
- Liu P., Yang L., Gao Z., Li S. and Gao Y. (2015). Fault tree analysis combined with quantitative analysis for high-speed railway accidents. *Safety Science*, Vol. 79, pp. 344-357.
- Luong TA, Kunze M, Trinckauf J. (2019). Human Factor And Safety Culture In Vietnamese Urban Railway. *Journal of the Eastern Asia Society for Transportation Studies*. Vol. 13. P. 1905-1926.
- Mahboob, Q. (2014). A Bayesian Network Methodology for Railway Risk, Safety and Decision Support. Doctorate Dissertation. Fakultät Verkehrswissenschaften "Friedrich List" of TU Dresden.
- Mahboob, Q., Zio, E. (2018). Handbook of RAMS in Railway System: Theory and Practice. CRC Press:NY.
- Markowski, A, S. & Mannan, M, S. (2008). Fuzzy risk matrix. *Journal of hazardous materials*, Vol 159 / 1, pp 152-157
- Markeset, T. and U. Kumar (2003). Integration of RAMS and Risk Analysis in Product Design and Development Work Processes: A Case Study. A case study. *Journal of Quality in Maintenance Engineering* 9(4), 393–410.
- Matsumoto A, Michitsuji Y, Tobita, Y (2016) Analysis of train-overturn derailments caused by excessive curving speed. *Int. J. Railway Technol* 5: 27-45.
- McLeod, R.W.,Walker, G. H., and Moray, N (2005). Analysing and modelling train driver performance. *Appl. Ergon.*, Vol 36/6, 671–680.
- Mearns , Hope, Ford, Tetrick, (2010). Investment in workforce health: exploring the implications for workforce safety climate and commitment. *Accident Analysis and Prevention*. (42), 1445–1454.
- Middleton, M. and A. Franks (2001). Using Risk Matrices. *The Chemical Engineer* 34-37.
- MIL-STD-882D (2000). Department Of Defense Standard Practice: System Safety. Achieved at [http://everyspec.com/MIL-STD/MIL-STD-0800-0899/MIL\\_STD\\_882D\\_934/](http://everyspec.com/MIL-STD/MIL-STD-0800-0899/MIL_STD_882D_934/)
- Milius, B. (2010). Construction of a semi-quantitative risk graph, PhD thesis. TU Braunschweig.
- Morgan, M.G. (1990) Choosing and Managing Technology-Induced Risks, in: T.S. Glickman and M. Gough (eds) *Readings in Risk*, pp. 5–15, Washington: Resources for the Future.
- [NTCA] National Transport Commission Australia (2008). National Guideline for the Preparation of a Rail Safety Management System. Achieved at <https://www.ntc.gov.au/publications/?year=2008>
- Murata, T., (1989). Petri nets: Properties, analysis and applications. *Proc. IEEE* 77, 541–580.
- Murphy K. (1998). A Brief Introduction to Graphical Models and Bayesian Networks. Assessed at <http://www.cs.berkeley.edu/~murphyk/Bayes/bayes.html>

- Ng, T. W. H., Sorensen, K. L., & Eby, L. T. (2006). Locus of Control at Work: A Meta-Analysis. *Journal of Organizational Behaviour*, Vol. 27 / Issued 8, pp. 1057-1087
- Nordland, O. (2001). When is risk acceptable? In *Presentations at 19th International System Safety Conference*, Huntsville, Alabama, USA September 2001.
- Novatsis E. (2016). Chapter 18 - Safety culture and behavior. In Edmons J. (Eds) *Human Factors in the Chemical and Process Industries*, pp. 311-334. Elsevier. <https://doi.org/10.1016/B978-0-12-803806-2.00018-2>.
- [NTC] National Transport Commission (2017). *National Standard for Health Assessment of Rail Safety Workers*. Third Edition. NTC: Melbourne
- [ORR] Office of Rail Regulation (2015). *Common Safety Method for risk evaluation and assessment. Guidance on the application of Commission Regulation (EU) 402/2013*. Achieved on June 12th, 2017 at <http://www.orr.gov.uk/rail/health-and-safety/health-and-safety-laws/european-railway-safety-legislation/csm-for-risk-evaluation-and-assessment>
- Parzen, E. (1999). *Stochastic processes, Classics in applied mathematics*. Society for Industrial and Applied Mathematics, Philadelphia, Pa.
- Pasquale, T., Rosaria, E., Pietro, M., Antonio, O. & Segnalamento Ferroviario, A. (2003). Hazard analysis of complex distributed railway systems. In: *Reliable Distributed Systems, 2003. Proceedings. 22nd International Symposium on*, 2003. IEEE, 283-292.
- Paté-Cornell, M. E. (1984). Fault Trees vs. Event Trees in Reliability Analysis. *Risk Analysis*, Vol. 4, No. 3.
- Patacchini, A. (2011). *Application guide for the design and implementation of a Railway Safety Management System*. France: European Railway Agency.
- Petri C.A and Reisig W. (2008) Petri net. *Scholarpedia*, 3(4):6477. doi:10.4249/scholarpedia.6477
- Pickup, L., Wilson, J. R., Norris, B. J., Mitchell, L., and Morrisroe, G (2004) . The integrated workload scale (IWS): a new self-report tool to assess railway signaller workload. *Appl. Ergon.*, 36/6, 681–693.
- Power, G.J, Tompkins, F.C. (1974). Fault tree synthesis for chemical process. *American Institute of Chemical Engineers Journal*, Vol.20, pp.376-387.
- Railway Safety Act (2006). Published by the Minister of Justice at the following address: <http://laws-lois.justice.gc.ca>
- [RSSB] Rail Safety and Standards Board (2002). *Railway Safety and The Ethics of the Tolerability of Risk*.
- Rausand, M. (2011). *Risk Assessment: Theory, Methods, and Applications*. John Wiley & Sons: USA
- Rausand, M. and Utne, I. B. (2009a). Product safety-principles and practices in a life cycle perspective. *Safety Science*, 47:939-947.
- Redmill, F.. (2002). Risk analysis - A subjective process. *Engineering Management Journal*. 12. 91 - 96.
- Reales, C. (2014). *Reliability, Availability and Maintainability Study of a Light Rail Transit System*. Universitat Politècnica De Catalunya
- Reason, J., Free, R., Havard, S., Benson, M., and Van Oijen, P. (1994). The railway accident investigation tool (RAIT): a report on the analysis of 57 infrastructure events. Railtrack internal document, Safety and Standards Directorate
- Reason, James (2000). "Human error: models and management". *British Medical Journal*. 320 (7237): 768–770. doi:10.1136/bmj.320.7237.768. PMC 1117770 Freely accessible. PMID 10720363.
- Reniers, G. L. L., Dullaert, W., Ale, B. J. M., & Soudan, K. (2005). Developing an external domino prevention framework: Hazwim. *Journal of Loss Prevention in the Process Industries*, 18, 127-138.
- Rekabi M.M. (2018). *Bayesian Safety Analysis of Railway Systems with Driver Errors*. Master Thesis. Norwegian University of Science and Technology.
- Renn, O. (1992): Concept of Risk: A Classification. In: Krinsky, S. – Golding, D. (Eds.), *Social Theories of Risk*. pp. 53–79. Westport, CT: Praeger.
- Renn, O. (1998): Three decades of risk research: accomplishments and new challenges. *Journal of Risk Research*. Vol. 1, No. 1, pp. 49–71.
- Regulation EU 2018/762 (2018). Commission Delegated Regulation (EU) 2018/762 of 8 March 2018 establishing common safety methods on safety management system requirements pursuant to Directive (EU) 2016/798 of the European Parliament and of the Council and repealing Commission Regulations (EU) No 1158/2010 and (EU) No 1169/2010.
- Rotab Khan, M. R. and A. B. Zohrul Kabir (1995). Availability Simulation of an Ammonia Plant. *Reliability Engineering and System Safety* 48(3), 217–227.
- ROGS (2006). *The Railways and Other Guided Transport Systems (Safety) Regulations 2006*. Regulations 2006 UK The Stationery Office Limited. Achieved at <http://www.legislation.gov.uk/uksi/2006/599/contents/made> on July, 17th, 2018.
- Ruijters E. J. (2018). *Zen and the Art of Railway Maintenance: Analysis and Optimization of Maintenance via Fault Trees and Statistical Model Checking*. University of Twente.
- Sadeghi, J., Hasheminezhad, A., & Essmayil Kaboli, M. (2015). Investigation of the influences of track super-structure parameters on ballasted railway track design. *Civil Engineering Infrastructures Journal*, 48(1), 157-174
- Salimifard, K., Wright, M. (2001). Petri net-based modelling of work flow systems: An overview. *Eur. J. Oper. Res.* 13.
- Sapozhnikov, V., Sapozhnikov, V., Anders, E. & Trinckauf, J., (2009). Safety and Reliability in Signalling Systems. In: G. Theeg & S. Vlasenko, eds. *Railway Signalling and Interlocking*. pp. 24-38. Hamburg: Eurail press
- Schäbe, H.; *Neue Ansätze zur Systemsicherheit in der Bahntechnik*. Eisenbahntechnische Rundschau (ETR), 50 (2001) Heft 4, S. 185-191, HestraVerlag, Hamburg



- Schäbe H. & Wigger P. Experience with SIL Allocation in Railway Applications, Proc. of the fourth int. symposium on Programmable Electronics Systems in Safety Related Applications Cologne, Germany, 2000
- Souza A., Tavares F., Bonikowski R., Pereira V. (2019). Reduction of number of Railroad Accidents with Lo-comotive as the main cause. Final Project of Confederação Nacional dos Transportes. Brasília
- Sun YQ (2018) Mitigating Train Derailments Due to Sharp Curve and Overspeed. *Frontiers in Mechanical Engineering* 4: 8.
- Skjong, R., Vanem, E., Endresen, . (2007). Risk evaluation criteria. Technical report, SAFEDOR-D-4.5.2 DNV.
- Smith, D. J. (2017). Reliability, Maintainability and Risk: Practical Methods for Engineers (9th ed.). Butterworth-Heinemann: Elsevier.
- Soleimanmeigouni, Iman; Ahmadi, Alireza; Kumar, Uday (2018). Track geometry degradation and maintenance modelling: A review. In: Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit. Vol. 232, p. 73-102.
- Stephenson, T.A., (2000). An Introduction to Bayesian Network Theory and Usage. IDIAP Research Report.
- Taylor, James (2004). Managing Information Technology Projects. p. 39.
- Transport Canada (2001). Railway Safety Management System Regulations. Achieved at <http://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-37/> on July, 17th, 2018.
- Transport Canada (2005). Helping Build a "True Safety Culture" Through the Development of a SMS.
- Turner JR (1993). The handbook of project-base management: improving the processes for achieving strategic objectives, 1st Edition. England: McGraw-Hill.
- Van Scoy (1992). Software Development Risk: Opportunity, Not Problem. Software Engineering Institute : Pittsburgh.
- Valkokari, T. A., O. Venho-Ahonen, H. Franssila and A. Ellman (2012). Requirements for Dependability Management and ICT Tools in the Early Stages of the System Design. *Advance in Safety, Reliability and Risk Management*. Taylor & Francis Group.
- Vanem E., (2012). Ethics and fundamental principles of risk acceptance criteria. *Safety Science*, Vol. 50, p. 958-967.
- Vasvari, T. (2015). Risk, Risk Perception, Risk Management: a Review of the Literature. *Public Finance* 2015/1.
- Wagner, W. and P. H. A. J. M. Van Gelder (2013). Applying RAMSSHEEP Analysis for Risk-driven Maintenance. In Proceedings of the 22nd European Safety and Reliability Conference "Safety, Reliability and Risk Analysis: Beyond the Horizon", Amsterdam. CRC Press.
- Wilkinson G., David R. (2009) Back to Basics: Risk Matrices and ALARP. In: Dale C., Anderson T. (eds) *Safety-Critical Systems: Problems, Process and Practice*. London: Springer.
- Woodruff, J. M. (2005). Consequence and likelihood in risk estimation: a matter of balance in UK health and safety risk assessment practice. *Safety Science*, 43(5-6), p.345-353.
- [UN] United Nations (1992). Report of the United Nations Conference on Environment and Development
- [UNDRR]UN Office for Disaster Risk Reduction (2020). Hazard Definition and Classification review – Technical report. Sendai framework for Disaster Risk reduction 2015-2030. United Nations: Switzerland. Rio Declaration on Environmental and Developmental. A/CONF.151/26 (Vol. I)
- UNGA (2016). Report of the open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction. Note by the Secretary-General. United Nations General Assembly (UNGA). Document No. A/71/644. <https://undocs.org/A/71/644>
- UNGA (2017). Resolution adopted by the General Assembly on 2 February 2017. 71/276. Report of the open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction. United Nations General Assembly (UNGA). [https://www.unisdr.org/files/resolutions/N1702972\\_en.pdf](https://www.unisdr.org/files/resolutions/N1702972_en.pdf)
- [UIC] International Union of Railways (2021). UIC Safety Report 2021. Paris: International Union of Railways
- [VMoT] VN Ministry of Transport (2016) Circular 16/2016/TT-BGTVT: Assessment, certification of urban railway safety
- [USDT] United States Department of Transportation (2009). A Practical Risk Assessment Methodology for Safety-Critical Train Control Systems. Washington DC : Office of Research and Development.
- Vietnam National Safety Board (2016). Transport Safety Report 2010 – 2015
- [VR] Vietnam Railway Company (2016). Safety statistic report of Vietnam Railways 2015. May 2016
- [VR] Vietnam Railway Company (2017). Safety statistic report of Vietnam Railways 2016. June 2017
- [VR] Vietnam Railway Company (2021): Safety statistic report of Vietnam Railways 2017-2020. July 2021.
- Vu H Tr, Nguyen HA. (2019) Ensuring safety in urban railway operation in Hanoi. *Journ. Transportation, Special Issue*.
- Yang Jiangping and Wang Xishi (2000). Reliability And Safety Analysis of Automatic Train Protection System. *IFAC Control in Transportation Systems*, Braunschweig, Germany, 2000, pp. 615-619
- Wang J. (2014). Reliability Analysis for CRH2 EMU Brake System Based on Dynamic Fault Tree. Master thesis. Beijing Jiaotong University.
- Woodson W. E. (1981). Human Reliability with Human factors. Pergamon Press: New York
- Wu C., Cao C., Sun Y. and Li K. (2015). Modeling and Analysis of Train Rear-End Collision Accidents Based on Stochastic Petri Nets. Special Issue: Mathematical Problems in Petri Nets Theory and Applications. *Mathematical Problems in Engineering*. <https://doi.org/10.1155/2015/602126>
- Zheng, Shuting (2018). Bayesian Network-Based Reliability Analysis of Metro Train Brake System. Beijing Jiaotong University.

## APPENDIX

### Appendix 1: Questionnaire for railway worker attitudes on safety risks

#### Questionnaire for Workers' perception of safety culture in railway

Name of participant:

Organization:

Position:

Age

Please tick on the best suitable scale box

1 = Absolutely disagree, 2 = Disagree, 3 = Almost disagree, 4 = Almost agree, 5 = Agree, 6 = Absolutely agree

or 1 = Never, 2 = Very rarely, 3 = Rarely, 4 = Sometimes, 5 = Frequently, 6 = Very frequently

| No | Content  | Scale |   |   |   |   |   |
|----|--|-------|---|---|---|---|---|
| A  | Workers' perception of safety risks  | 1     | 2 | 3 | 4 | 5 | 6 |
| A1 | Workers' perception of safety risks  |       |   |   |   |   |   |
|    | <b>Problems of fatigue and stress</b>  |       |   |   |   |   |   |
| 1  | They were encouraged by the employer not to attend work if they had had less than 6 hours sleep in the previous 24 hours.  |       |   |   |   |   |   |
| 2  | They were allowed to be on a night shift after they had been awake for more than 15 hours prior to the start of work   |       |   |   |   |   |   |
| 3  | They were allowed to cancel their shift at short notice due to pressing personal circumstances   |       |   |   |   |   |   |
| 4  | They were put under pressure to report for duty despite feeling fatigued   |       |   |   |   |   |   |
| 5  | They needed to overextend themselves because of poor roster scheduling (e.g. working overtime)   |       |   |   |   |   |   |
| 6  | They had been fully informed by the employer regarding risks posed by sleeping disorders, symptoms and available means of detecting and treating them  |       |   |   |   |   |   |
| 7  | They received support from the employer to make effective use of off-duty time to maximize restorative rest or sleep   |       |   |   |   |   |   |
| 8  | They received support from the employer to seek medical help for conditions that interfere with restorative rest or sleep.   |       |   |   |   |   |   |
| 9  | They received support from the employer to seek professional help (e.g. counseling, therapy) to resolve personal problems that interfere with restorative rest or sleep  |       |   |   |   |   |   |
|    | <b>Problems of Medical conditions and Pharmacology</b>   |       |   |   |   |   |   |
| 10 | They had roster flexibility which allowed them to cancel their shift at short notice due to medical conditions (e.g. chronic sleep disorders, neuralgia and cardiac conditions).   |       |   |   |   |   |   |
| 11 | They performed tasks under the influence of medication (both prescribed and self-administered) which could have potentially compromised rail safety.   |       |   |   |   |   |   |
| 12 | They were allowed to/ pressured to perform tasks despite sudden sickness (e.g. flu, nausea and migraine headache) which could have affected rail safety.   |       |   |   |   |   |   |
|    | <b>Problems of Violations</b>  |       |   |   |   |   |   |
| 13 | They performed tasks under the influence of alcohol or illicit drugs which could have potentially compromised rail safety  |       |   |   |   |   |   |
| 14 | They performed safety-critical tasks without authorization   |       |   |   |   |   |   |
| 15 | They were allowed to perform duties without their performance being adequately monitored following unfavourable safety compliance history  |       |   |   |   |   |   |
| 16 | Non-safeworking personnel were allowed access to safeworking equipment   |       |   |   |   |   |   |
| 17 | They got confused about what actions to take because of unclear communication from a colleague about safety-critical tasks.  |       |   |   |   |   |   |
| 18 | They broke the monotony of the task by engaging in various forms of entertainment (reading, listening to music, talking on the mobile phone for private matters, being engaged in personal conversation with a colleague on site) while on duty. |       |   |   |   |   |   |
| 19 | They broke safeworking rules because they were overconfident.  |       |   |   |   |   |   |
| 20 | They took shortcuts which could have potentially compromised safety because it had become standard practice – everyone does it all the time.   |       |   |   |   |   |   |
|    | <b>Problem of Applicable skills</b>  |       |   |   |   |   |   |
| 21 | They performed tasks that they had NOT been fully trained in.  |       |   |   |   |   |   |

|           |   |  |  |  |  |  |  |
|-----------|---|--|--|--|--|--|--|
| 22        | They performed tasks in an unfamiliar environment/ situation.   |  |  |  |  |  |  |
| 23        | They made potentially unsafe compromises because of equipment failure/mismatch (e.g. taking shortcuts or deviating from the procedure).   |  |  |  |  |  |  |
|           | <b>Problem of concentrated ability of workers</b>   |  |  |  |  |  |  |
| 24        | They rushed to complete tasks to stay on schedule or to a timetable.  |  |  |  |  |  |  |
| 25        | They were in a work environment where they were easily distracted by other tasks or people while performing their job.  |  |  |  |  |  |  |
| 26        | They were under pressure to perform duties beyond the limits of what could have been reasonably handled by one person.  |  |  |  |  |  |  |
|           | <b>Problem of Organizational requirements</b>   |  |  |  |  |  |  |
| 27        | They were allowed to perform tasks without going through regular updating of safety-critical skills through refresher training and safety compliance audits.                          |  |  |  |  |  |  |
| 28        | When they raised safety concerns and/or reported potential safety risks, these were ignored by line and/or top management.  |  |  |  |  |  |  |
| <b>A2</b> | <b>Potential Safety Problem</b>   |  |  |  |  |  |  |
|           | <b>Communication</b>  |  |  |  |  |  |  |
| 29        | Because a change of operational/infrastructure circumstances had not been communicated to them.   |  |  |  |  |  |  |
| 30        | Lack of communication from colleagues about potential safety risks (e.g. observed defect in track, equipment and rolling stock)   |  |  |  |  |  |  |
|           | <b>Design</b>   |  |  |  |  |  |  |
| 31        | Inadequate protection at level crossings (e.g. passive level crossings).  |  |  |  |  |  |  |
| 32        | Because of inadequate defenses against error or inadequate train protection   |  |  |  |  |  |  |
| 33        | Poor design of equipment/rolling stock which could have compromised safe working  |  |  |  |  |  |  |
|           | <b>Maintenance</b>  |  |  |  |  |  |  |
| 34        | Equipment failure, poor condition of the track, rolling stock and/or signalling.  |  |  |  |  |  |  |
| 35        | Because of inadequate housekeeping (e.g. cleaning of facilities/operating equipment, tidy working environment, recovery from vandalism and ensuring clear track/signal sightings).    |  |  |  |  |  |  |
|           | <b>Management</b>   |  |  |  |  |  |  |
| 36        | Lack of the employer's effort to ensure compliance with safety rules (including those for operations, signalling, loading, inspection & maintenance).                                 |  |  |  |  |  |  |
| 37        | Because the employer had been unable to stop unsafe work practice that had been around for a long time and had become a standard way of doing things – everyone does it all the time. |  |  |  |  |  |  |
| 38        | Because they were unable to challenge decisions made by more experienced employees in the team.   |  |  |  |  |  |  |
| 39        | Lack of training in hazard identification before commencing any task.   |  |  |  |  |  |  |
|           | <b>Policies, Rules and Procedures</b>   |  |  |  |  |  |  |
| 40        | Because of lack of standardized approach to safety procedures.  |  |  |  |  |  |  |
| 41        | Because procedures did not specify appropriate safeworking actions for certain safety-related tasks.  |  |  |  |  |  |  |
| 42        | Inadequate safety standards and procedures (including those for operations, signalling, loading, inspection, maintenance and management of dangerous goods).                          |  |  |  |  |  |  |
| 43        | Because procedure manuals and checklists were hard to understand or NOT available.  |  |  |  |  |  |  |
|           | <b>External factors</b>   |  |  |  |  |  |  |
| 44        | Unexpected intrusion across the track by people, animals and foreign objects  |  |  |  |  |  |  |
| 45        | Reckless behaviour of pedestrians and vehicle drivers (e.g. cars and trucks) at level crossings.  |  |  |  |  |  |  |
| 46        | Aggressive behaviour by passengers.   |  |  |  |  |  |  |
|           | <b>Environmental Factors</b>  |  |  |  |  |  |  |
| 47        | Unforeseen weather and other environmental conditions (e.g. extreme heat, cold, and other inclement weather conditions).  |  |  |  |  |  |  |
| <b>B</b>  | <b>Workers' perception of safety management procedure</b>   |  |  |  |  |  |  |
| <b>B1</b> | <b>Purpose of safety management procedure</b>   |  |  |  |  |  |  |
| 1         | The overall effect of safety management procedures is NOT necessarily properly considered in detail   |  |  |  |  |  |  |

|           |  |  |  |  |  |  |  |
|-----------|--|--|--|--|--|--|--|
| 2         | The safety management procedures are occasionally seen as inconvenient by competent employees  |  |  |  |  |  |  |
| 3         | The purpose of safety management procedures is to prevent individual incidents recurring   |  |  |  |  |  |  |
| 4         | The safety management procedures are often crisis-oriented and written in response to accidents.   |  |  |  |  |  |  |
| 5         | The safety management procedures are taught in training but are inflexible   |  |  |  |  |  |  |
| 6         | The safety management procedures spread best practice and are refined for efficiency   |  |  |  |  |  |  |
| <b>B2</b> | <b>Safety management procedure and Profitability</b>   |  |  |  |  |  |  |
| 7         | Safety is seen as an optional expenditure  |  |  |  |  |  |  |
| 8         | Managers believe that safety management procedure saves money in the long-term   |  |  |  |  |  |  |
| 9         | Managers put the safety and safety management procedure in the top priority and understanding that they contribute to the financial return |  |  |  |  |  |  |
| 10        | Division managers spend most of their time on operational issues   |  |  |  |  |  |  |
| 11        | Line managers know how to say the right things, but do not always walk their own talk.   |  |  |  |  |  |  |
| 12        | It is important to put money towards maintenance to prevent accidents  |  |  |  |  |  |  |
| 13        | Safety is seen as costing money, and the only priority is to avoid extra costs.  |  |  |  |  |  |  |
| <b>B3</b> | <b>Workforce interest in competency and safety training</b>  |  |  |  |  |  |  |
| 14        | Training is attended when it is required by law  |  |  |  |  |  |  |
| 15        | Compulsory training during work hours gives employees a pleasant break from work that they carry out in a harsh working environment        |  |  |  |  |  |  |
| 16        | Training is seen as a process for enhancing skills and competency rather than a requirement  |  |  |  |  |  |  |
| 17        | Training needs are beginning to be identified by the employees   |  |  |  |  |  |  |
| 18        | Training is aimed at changing the employee's safety attitude rather than technique and procedure   |  |  |  |  |  |  |
| 19        | After an accident, specific training programs are made available   |  |  |  |  |  |  |
| <b>B3</b> | <b>Workplace safety control</b>  |  |  |  |  |  |  |
| 20        | There are no safety management controls applied  |  |  |  |  |  |  |
| 21        | There is little systematic use of the standard work-related safety management controls   |  |  |  |  |  |  |
| 22        | Internal safety audits, as a work-site hazard management control, are revised regularly in a defined process.                              |  |  |  |  |  |  |
| 23        | The number of inspection reports written is used to check the job safety controls by the management system.                                |  |  |  |  |  |  |
| <b>B4</b> | <b>Safety audits and reviews</b>   |  |  |  |  |  |  |
| 24        | Internal audits are structured in terms of management systems.   |  |  |  |  |  |  |
| 25        | Internal audits mainly deal with financial matters.  |  |  |  |  |  |  |
| 26        | There is no schedule for internal audits and reviews as they are seen as a punishment.   |  |  |  |  |  |  |
| 27        | There is an extensive internal audit program including cross-auditing within the organization.   |  |  |  |  |  |  |
| 28        | Regulatory audits are accepted as inescapable, especially after serious or fatal accidents.  |  |  |  |  |  |  |

## Appendix 2 : Risk matrix analysis of HN Line 2A

| No      | Potential Accident  | Detailed Potential Accident | Hazardous Situation        | Potential causes  | Trigger Events            | Risk reduction means   | Responsibilities                   | Sev . | O cc |
|---------|---|-----------------------------|----------------------------|---|---------------------------|--|------------------------------------|-------|------|
| 1       | <b>COLLISIONS – Rear-end collisions, frontal collisions – Collision with train or part of train, out of operation</b> |                             |                            |   |                           |  |                                    |       |      |
| 1.1.1.1 | COLLISION BETWEEN TWO TRAINS (INCLUDING RAIL ROAD VEHICLE)  | Rear-end collision          | Invisible vehicle          | Rupture of a semi-automatic coupler (between Simple Units)                  | Presence of another train | <p>The Driver is responsible to manage the coupling speed of the train that shall be limited to 3 km/h to prevent irreversible deformations of coupling and shock absorber devices.</p> <p>A calculation note shall be done to confirm that semi-automatic coupler assembly is able of withstanding buff or draft loads in rescue operation for an ELE (Empty load) loaded train rescuing an EL8 (Exceptional load) loaded train with no traction and no brakes.</p> <p>A validation test shall be performed on semi-automatic coupler to confirm the mechanical resistance of the coupler in rescue conditions (an ELE (Empty load) loaded train rescuing an EL6.6 loaded train with no traction and no brakes with 4% gradient).</p> <p>The supplier of semi-automatic coupler shall demonstrate that the unexpected uncoupling of semi-automatic coupler reaches the target of <math>1 \times 10^{-9}</math> failure per hour.</p> <p>A calculation note shall be done to define semi-automatic coupler's fixations on carbody shell.</p> | Operator Rolling Stock subsystem   | 1     | F    |
|         |   |                             | Invisible vehicle          | Untimely uncoupling   | Presence of another train | <p>Uncoupling activation by the driver during the rescue phase shall be forbidden.</p> <p>The uncoupling shall be prevented when the train is not at standstill</p>  | Operator RS subsystem              | 1     | F    |
|         |   |                             | Invisible vehicle          | Rupture of semi-permanent coupler (between cars)                            | Presence of another train | <p>A calculation note shall be done to confirm that semi-permanent coupler assembly is able of withstanding buff or draft loads in rescue operation for an ELE (Empty load) loaded train rescuing an EL8 (Exceptional load) loaded train with no traction and no brakes).</p> <p>A validation test shall be performed on semi-permanent coupler to confirm the mechanical resistance of the coupler in rescue conditions (an ELE (Empty load) loaded train rescuing an EL6.6 loaded train with no traction and no brakes).</p> <p>The supplier of semi-permanent coupler shall demonstrate that the unexpected uncoupling of semi-permanent coupler reaches the target of <math>1 \times 10^{-9}</math> failure per hour per train.</p> <p>A calculation note shall be done to define semi-permanent coupler's fixations on carbody shell.</p>   | Rolling Stock subsystem            | 1     | F    |
|         |   |                             | Invisible vehicle          | Loss of integrity: bad operation during coupling (excessive speed)          | Presence of another train | <p>The Driver is responsible to manage the coupling speed of the train that shall be limited to 3 km/h to prevent irreversible deformations of coupling and shock absorber devices.</p> <p>Validation test shall be done to demonstrate couplers compliance to EN15227</p>   | Operator RS subsystem              | 1     | F    |
|         |   |                             | Invisible vehicle          | Failure of the parking brake  | Presence of another train | <p>"A calculation note shall be done to confirm that parking brake is designed to maintain the train at standstill in 4 % slope, with 80 km/h wind and :</p> <ul style="list-style-type: none"> <li>- under exceptional load (EL8) with one car with no brake during 1 hour,</li> <li>- under load (EL6) with one car with no brake with no time limit.</li> </ul> <p>The calculation note shall also determine how many actuator failures are required to make train moving in EL8 before 1 hour."</p> <p>A validation test shall be performed to confirm the parking brake performances (in degraded mode).</p> <p>The supplier of parking brake shall demonstrate that the loss of parking brake on more than one car on the train reaches the target of <math>1 \times 10^{-9}</math> failure per hour.</p> <p>A dependable train detection system shall be implemented on the line to ensure a safe distance between trains.</p> <p>Signalling shall apply a safety brake in case of unrespected distance between trains.</p>           | Rolling Stock subsystem<br>Signals | 1     | F    |
| 1.1.1.2 |   |                             | Disappearance of a vehicle | Unexpected transition of operating mode (more permissive)                   | Presence of another train | <p>A dependable train detection system shall be implemented on the line to ensure a safe distance between trains.</p> <p>Signalling shall apply a safety brake in case of unrespected distance between trains.</p> <p>Red lights shall be available to indicate to driver that he is approaching a train.</p>  | RS subsystem<br>Signals            | 1     | F    |
| 1.1.1.3 |   |                             | Stopping distance too long | Inefficient of safety braking due to automatic isolation of a service brake | Presence of another train | Automatic service brake isolation function from brake electronic shall be independent from the safety brake function.  | RS subsystem                       | 1     | F    |
|         |   |                             | Stopping distance too long | Inefficient service braking   | Presence of another train | <p>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.</p> <p>Failure rate of safety brake command from Signalling shall be lower or equal to <math>1 \times 10^{-9}</math> failure per hour. "</p> <p>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.</p>   | Operator Signals                   | 1     | F    |

|  |  |  |                            |  |                           |   |   |   |   |
|--|--|--|----------------------------|--|---------------------------|---|---|---|---|
|  |  |  |                            |  |                           | Signalling shall ensure that there is always adequate safety distance between two RSK in operation to prevent collision in case of Safety Brake (assuming the minimum guaranteed deceleration rate)   |   |   |   |
|  |  |  | Stopping distance too long | Safety Brake failure or inefficiency   | Presence of another train | <p>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.</p> <p>Failure rate of safety brake command from Signalling shall be lower or equal to <math>1 \times 10^{-9}</math> failure per hour. "</p> <p>Failure rate of safety brake order transmission to brakes shall lower or equal to <math>1 \times 10^{-9}</math> failure per hour.</p> <p>Non respect of safety brake performances, including failures of load compensation and wheel slide protection, shall not have a failure rate lower or equal to <math>1 \times 10^{-9}</math> failure per hour.</p> <p>"A calculation note shall be done to confirm that safety brake is designed to reach the following performances:</p> <ul style="list-style-type: none"> <li>- under EL6.6 in nominal conditions, the deceleration shall be at least <math>1,35 \text{ m/s}^2</math>.</li> <li>- under EL6.6 with one car isolated, the deceleration shall be at least <math>0,72 \text{ m/s}^2</math>.</li> <li>- Maximum tolerable jerk for deceleration from <math>80 \text{ km/h}</math> to <math>0 \text{ km/h}</math> shall less than <math>4 \text{ m/s}^3</math>, according to EN 13452-1.</li> </ul> <p>The calculation note shall also determine how many actuator failures are acceptable to respect the degraded performance."</p> <p>"A validation test shall be performed to confirm the Safety Brake application by all the following means:</p> <ul style="list-style-type: none"> <li>- Signalling's safety brake relays,</li> <li>- Emergency pushbutton,</li> <li>- No activated cabin,</li> <li>- Low pressure detection in main pipe,</li> <li>- Driving mode change which train is running."</li> <p>A validation test shall be performed to confirm the safety brake performances (in nominal and degraded mode).</p> <p>The failure rate associated to failure of the traction cut off in case of emergency brake shall not be lower or equal to <math>1 \times 10^{-9}</math> failure per hour.</p> </ul> | RS subsystem Signals                      | 1 | E |
|  |  |  | Stopping distance too long | Air production failure (unable to compensate air leak in main pipe or air consumption)   | Presence of another train | <p>"Each air production units shall be equipped with a pressure switch triggering if the pressure in the main pipe is lower than 6,5 bars.</p> <p>Failure rate of the pressure switch leading to the non detection of low pressure shall be lower than <math>1 \times 10^{-7}</math> failure per hour per pressure switch."</p> <p>Train shall be equipped with two air production units.</p> <p>A validation test shall be performed to confirm the air production units performances (in nominal and degraded mode).</p> <p>Brakes shall be equipped with air reservoirs allowing 3 safety brakes from <math>80 \text{ km/h}</math> to <math>0 \text{ km/h}</math> in case of loss of air production.</p> <p>All pressure switches from air production unit triggering in case of pressure lower than 6,5 bars shall be in the safety brake command loop to trigger a safety brake in case of low pressure detection by anyone of them.</p> <p>"A validation test shall be performed to confirm the Safety Brake application by all the following means:</p> <ul style="list-style-type: none"> <li>- Signalling's safety brake relays,</li> <li>- Emergency pushbutton,</li> <li>- No activated cabin,</li> <li>- Low pressure detection in main pipe,</li> <li>- Driving mode change which train is running."</li> </ul>  | Rolling stock subsystem                   | 1 | F |
|  |  |  | Stopping distance too long | Failure of Car load compensation   | Presence of other train   | Non respect of safety brake performances, including failures of load compensation and wheel slide protection, shall not have a failure rate lower or equal to $1 \times 10^{-9}$ failure per hour.  | Rolling stock subsystem                   | 1 | F |
|  |  |  | Stopping distance too long | "Traction effort maintained:<br>- Spurious traction order sent by TCMS<br>- TCU failure" | Presence of another train | <p>The failure rate associated to failure of the traction cut off in case of emergency brake shall not be lower or equal to <math>1 \times 10^{-9}</math> failure per hour.</p> <p>Safety braking effort shall be greater than traction effort</p> <p>Signalling shall ensure that there is always adequate safety distance between two RSK in operation to prevent collision in case of Safety Brake (assuming the minimum guaranteed deceleration rate)</p>   | RS subsystem Signals                      | 1 | F |
|  |  |  | Stopping distance too long | Overspeed due to traction system failure   | Presence of another train | <p>A dependable train detection system shall be implemented on the line to ensure a safe distance between trains.</p> <p>Signalling shall apply a safety brake in case of unrespected distance between trains.</p> <p>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.</p> <p>Failure rate of safety brake command from Signalling shall be lower or equal to <math>1 \times 10^{-9}</math> failure per hour. "</p> <p>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.</p>   | Operators Rolling Stock subsystem Signals | 1 | F |

|  |  |  |                            |  |                           |   |  |   |   |
|--|--|--|----------------------------|--|---------------------------|---|--|---|---|
|  |  |  |                            |  |                           | Failure of traction leading to overspeed shall have a failure rate lower or equal to $3,33 \times 10^{-5}$ failure per hour per traction unit.  |  |   |   |
|  |  |  | Stopping distance too long | Undue manual isolation of a brake panel due to human error   | Presence of another train | Driver shall check daily that no brake is isolated on the train, before the revenue service.<br>Brakes electronics shall provide individual main pipe pressure value to TCMS.<br>TCMS shall check pressure values in main pipe in each car, and send an IOS with gravity "detrain" if pressure in 2 adjacent cars is lower than 6.5 bars.<br>In case of pneumatic isolation of a car by air production unit, the train shall be withdrawn from service at next station at the latest.<br>Brake isolation cocks shall be monitored by train embedded electronic.   | RS subsystem Signals                         | 1 | F |
|  |  |  | Stopping distance too long | Deterioration / Cracking of the brake discs due to a parking brake remaining applied                                   | Presence of another train | The operator or the maintenance shall address to the manufacturer all changes affecting the braking system (parts, actuators, sensor, piping) and they must be validated by the manufacturer.<br>Mechanical Brake failure leading to non parking brake release at bogie level shall be lower than $5 \times 10^{-7}$ failure per hour.<br>Parking brake monitoring failure leading to non detection of parking brake applied at bogie level shall be lower than $5 \times 10^{-8}$ failure per hour.<br>Train monitoring system shall made coherency check between brakes status train lines and local brakes status with an integrity level at least equal to SIL-0<br>Traction inhibition failure while parking brake is detected applied shall be lower than $1 \times 10^{-7}$ failure per hour.<br>"A calculation note shall be done to confirm that safety brake is designed to reach the following performances:<br>- under EL6.6 in nominal conditions, the deceleration shall be at least $1,35 \text{ m/s}^2$ .<br>- under EL6.6 with one car isolated, the deceleration shall be at least $0,72 \text{ m/s}^2$ .<br>- Maximum tolerable jerk for deceleration from 80km/h to 0 km/h shall less than $4 \text{ m/s}^3$ , according to EN 13452-1.<br><br>The calculation note shall also determine how many actuator failures are acceptable to respect the degraded performance."<br>A validation test shall be performed to confirm the safety brake performances (in nominal and degraded mode).   | Maintenance Operator Rolling stock subsystem | 1 | F |
|  |  |  | Stopping distance too long | Deterioration / Cracking of the brake discs due to remaining / spurious pressure in brake cylinder                     | Presence of another train | Mechanical Brake failure leading to non service brake release at bogie level shall be lower than $1 \times 10^{-7}$ failure per hour.<br>Service brake monitoring failure leading to non detection of service brake applied at bogie level shall be lower than $5 \times 10^{-8}$ failure per hour.<br>Train monitoring system shall made coherency check between brakes status train lines and local brakes status with an integrity level at least equal to SIL-0<br>Traction inhibition failure while pneumatic brake is detected applied shall be lower than $1 \times 10^{-7}$ failure per hour.<br>The operator or the maintenance shall address to the manufacturer all changes affecting the braking system (parts, actuators, sensor, piping) and they must be validated by the manufacturer.<br>"A calculation note shall be done to confirm that safety brake is designed to reach the following performances:<br>- under EL6.6 in nominal conditions, the deceleration shall be at least $1,35 \text{ m/s}^2$ .<br>- under EL6.6 with one car isolated, the deceleration shall be at least $0,72 \text{ m/s}^2$ .<br>- Maximum tolerable jerk for deceleration from 80km/h to 0 km/h shall less than $4 \text{ m/s}^3$ , according to EN 13452-1.<br><br>The calculation note shall also determine how many actuator failures are acceptable to respect the degraded performance."<br>A validation test shall be performed to confirm the safety brake performances (in nominal and degraded mode). | Maintenance Operator Rolling stock subsystem | 1 | F |
|  |  |  | Stopping distance too long | Low wheel/rail adhesion factor leading to increase the stopping distance (climatic conditions included) - Safety brake | Presence of another train | Signalling shall ensure that there is always adequate safety distance between two RSK in operation to prevent collision in case of Safety Brake (assuming the minimum guaranteed deceleration rate)<br>Operation shall maintain the tracks in correct state of cleanness and prevent its excessive wearing<br>A validation test shall be performed to confirm the correct operation of wheel slide protection of safety brake on tracks with low adhesion level.  | Operators Rolling Stock subsystem Signals    | 1 | F |
|  |  |  | Stopping distance too long | Loss of control command (TCMS)   | Presence of another train | "Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to $1 \times 10^{-9}$ failure per hour. "<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.<br>A dependable train detection system shall be implemented on the line to ensure a safe distance between trains.<br>Signalling shall apply a safety brake in case of unrespected distance between trains.   | Operators Signals                            | 1 | F |

|  |  |  |                            |  |                           |  |   |   |   |
|--|--|--|----------------------------|--|---------------------------|--|---|---|---|
|  |  |  | Stopping distance too long | Speed higher than expected, driver error   | Presence of another train | <p>The Driver shall be responsible to manage the train's speed and to respect lateral signalling.</p> <p>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.</p> <p>Failure rate of safety brake command from Signalling shall be lower or equal to <math>1 \times 10^{-9}</math> failure per hour. "</p> <p>Failure rate of speed limitation from traction units shall be lower or equal to <math>3,33 \times 10^{-5}</math> at train level per traction unit.</p> <p>A validation test shall be done to ensure correct speed limitation from traction equipment in restricted manual modes.</p> <p>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.</p> <p>The failure leading to the loss of speed indication on Driver Display Unit shall be lower or equal to <math>6 \times 10^{-5}</math> failure per hour per display unit.</p> <p>In case of inconsistency between speed indication on Tachometer and on Driver Display Unit, Driver shall signal it to OCC and train shall be send in maintenance at the end of the day to repair it.</p> <p>In case of inconsistency between speed indication on Tachometer and on Driver Display unit, driver shall use the highest speed indicated as reference.</p> <p>Tachometer failure rate shall be lower or equal to <math>1 \times 10^{-5}</math> failure per hour.</p> | Operators<br><br>Rolling stock subsystem        | 1 | E |
|  |  |  | Stopping distance too long | Loss of vigilance of the driver  | Presence of another train | <p>Deadman function's failure rate shall be lower or equal to <math>1 \times 10^{-6}</math> failure per hour.</p> <p>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.</p> <p>Failure rate of safety brake command from Signalling shall be lower or equal to <math>1 \times 10^{-9}</math> failure per hour. "</p>  | RS subsystem<br>Signals                         | 1 | F |
|  |  |  | Stopping distance too long | Bad speed measure (odometer failure...)  | Presence of another train | <p>Failure rate of speed limitation from traction units shall be lower or equal to <math>3,33 \times 10^{-5}</math> at train level per traction unit.</p> <p>A validation test shall be done to ensure correct speed limitation from traction equipment in restricted manual modes.</p> <p>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.</p> <p>To ensure independency of the speed measure, signalling shall use different odometers than rolling stock.</p>  | Operators<br>Rolling Stock subsystem<br>Signals | 1 | F |
|  |  |  | Stopping distance too long | "- Disruption of TCMS functions (processing time longer, problems when exchanging data's...)<br>- Corrupt TCMS functions (writing, variables modification...)" | Presence of another train | <p>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.</p> <p>Failure rate of safety brake command from Signalling shall be lower or equal to <math>1 \times 10^{-9}</math> failure per hour. "</p> <p>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.</p> <p>Safety brake control shall only be hardwired at rolling stock level.</p> <p>A dependable train detection system shall be implemented on the line to ensure a safe distance between trains.</p> <p>Signalling shall apply a safety brake in case of unrespected distance between trains.</p>  | Operators<br>Rolling Stock subsystem<br>Signals | 1 | F |
|  |  |  | Stopping distance too long | Bad visibility from the driving cab (cab ergonomics, faulty windscreen wipers)   | Presence of another train | <p>Windscreen wiper's failure rate shall be lower or equal to <math>5 \times 10^{-6}</math> failure per hour per wiper.</p> <p>Windscreen washer's failure rate shall be lower or equal to <math>1 \times 10^{-6}</math> failure per hour per washer.</p> <p>Train control failure leading to the loss of wiper and washer shall have a failure rate lower or equal to <math>1 \times 10^{-6}</math> failure per hour.</p> <p>A dependable train detection system shall be implemented on the line to ensure a safe distance between trains.</p> <p>Signalling shall apply a safety brake in case of unrespected distance between trains.</p> <p>In case of degraded visibility due to train failure or environmental conditions, the driver shall reduce train's speed and withdrawn the train from revenue service.</p> <p>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.</p> <p>Failure rate of safety brake command from Signalling shall be lower or equal to <math>1 \times 10^{-9}</math> failure per hour. "</p>  | Operators<br>Rolling Stock subsystem<br>Signals | 1 | F |
|  |  |  | Stopping distance too long | Insufficient front / rear lighting in case of driving by line of sight (lighting failure)  | Presence of another train | <p>White lights shall be available to indicate to maintenance staff/personnal on the track approach of a train.</p> <p>White lights shall have a failure rate lower than <math>1 \times 10^{-6}</math> failure per hour per light.</p> <p>Failures leading to switch on white lights instead of red lights shall have a failure rate lower or equal to <math>1 \times 10^{-9}</math> failure per hour.</p> <p>In each cabin, marker (white and red) lights on both sides shall have a independant power supply and command from the other one.</p> <p>Red lights shall be available to indicate to driver that he is approaching a train.</p> <p>Red lights shall have a failure rate lower than <math>1 \times 10^{-6}</math> failure per hour per light.</p> <p>A dependable train detection system shall be implemented on the line to ensure a safe distance between trains.</p> <p>Signalling shall apply a safety brake in case of unrespected distance between trains.</p>  | Rolling Stock subsystem<br>Signals              | 1 | F |



|         |  |                   |                              |  |                           |   |                                      |   |   |
|---------|--|-------------------|------------------------------|--|---------------------------|---|--------------------------------------|---|---|
|         |  |                   |                              | (train driver's errors)  |                           | In case of degraded visibility due to train failure or environmental conditions, the driver shall reduce train's speed and withdrawn the train from revenue service.<br>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to 1 x 10 <sup>-9</sup> failure per hour. "<br><br>In case of degraded visibility due to train failure or environmental conditions, the driver shall reduce train's speed and withdrawn the train from revenue service.   | Operators                            |   |   |
|         |  |                   | Stopping distance too long   | Circulation of a train which does not comply with the minimum operation conditions' requirements | Presence of another train | Operator shall withdrawn trains from revenue service in the cases defined in the Operation Manual and/or according to Incorrect Operational Status display on Driver Display Unit.<br>"Driver shall respect the following by-pass activation rules:<br>- In case of activation of a single Low Main Reservoir Governor By-pass, the train shall be allow to finish the day.<br>- In case of activation of a both Low Main Reservoir Governor By-passes or any other By-pass, the train shall be withdrawn from revenue service."  | Operators                            | 1 | F |
|         |  |                   | Stopping distance too long   | Adhesion problem: errors design of the wheel / rail interface or presence of external elements   | Presence of another train | All rails (main-line, depot, workshop and stabling areas) shall be conform to track profile defined in contract.<br><br>A validation test shall be performed to confirm the correct operation of wheel slide protection of safety brake on tracks with low adhesion level.<br>Operation shall maintain the tracks in correct state of cleanness and prevent its excessive wearing<br>Train shall be equipped with sanding system.   | Operators<br>Rolling Stock subsystem | 1 | F |
|         |  |                   | Stopping distance too long   | Train driver error (distance with downstream train, trackside signalling not respected)          | Presence of another train | A dependable train detection system shall be implemented on the line to ensure a safe distance between trains.<br>Signalling shall apply a safety brake in case of unrespected distance between trains.<br>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to 1 x 10 <sup>-9</sup> failure per hour. "<br>The Driver shall be responsible to manage the train's speed and to respect lateral signalling.  | Operators<br>Signals                 | 1 | E |
| 1.1.2.1 |  | Side-on collision | Invisible vehicle            |  | Crossing of a train       | As same as 1.1.1.1  |                                      | 1 | F |
| 1.1.2.2 |  |                   | Disappearance of a vehicle   |  | Crossing of a train       | As same as 1.1.1.2  |                                      | 1 | F |
| 1.1.2.4 |  |                   | Stopping distance too long   |  | Crossing of a train       | As same as 1.1.1.3  |                                      | 1 | F |
| 1.1.2.5 |  |                   | Fouling of the dynamic gauge | Wrong calculation of the fouling point   | Crossing of a train       | A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).<br>A validation test shall be done to check train compliance to static and dynamic gauges.<br>A fatigue calculation note shall be done to validate wheel design.  | Rolling Stock subsystem              | 1 | F |
|         |  |                   |                              | Wheel failure  | Crossing of a train       | A fatigue calculation note shall be done to validate wheel design.<br>Wheels shall comply to EN 13262   | RS subsystem                         | 1 | F |
|         |  |                   |                              | Loss of carbody integrity  | Crossing of a train       | Pivot Bolster integrity shall be validated by a compression test and/or fatigue test if calculation note conclusions indicate that it is required.<br>Carbody integrity shall be validated by a fatigue test if calculation note conclusions indicate that it is required.<br>Headstock integrity shall be validated by a calculation note<br>Carbody integrity shall be validated by a calculation note for compression and fatigue<br>Carbody integrity shall be validated by a validation test in compression<br>Welding plan shall comply with EN 1011-4 standard.<br>Car-car clearance shall be validated during design<br>Car-car clearance shall be checked by validation test<br>"1 year inspection on carbody must include:<br>- Visual inspection of mounting brackets of the underframe equipment including good tightening of the fixings of the boxes fixed to the underframe"<br>"If an HFR nut is removed, it shall always be replaced by a new one. Where an assembly has already been tightened by the constructor, replacement of the fastener is compulsory if :<br>- a thread lock has been used<br>- a HFR nut has been used | Rolling Stock subsystem              | 1 | F |

|         |  |  |                              |   |                         |   |   |   |   |
|---------|--|--|------------------------------|---|-------------------------|---|---|---|---|
|         |  |  |                              |   |                         | - a Nordlock (NL) or CS washer has been used<br>- a non-reusable washer or nut has been used (according to the type of fastener)"<br>Bogie-car clearance shall be validated during design<br>Bogie-car clearance shall be checked by validation test  |   |   |   |
|         |  |  |                              | Failure of suspension, bogie, connection vehicle-bogie, gauge dynamics, not respected gauge, interfaces vehicle station | Crossing of a train     | A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).<br>A validation test shall be done to check train compliance to static and dynamic gauges.<br>Secondary suspension shall have mechanical vertical stop to limit the train movement in case of flat or over-pressured suspension.<br>Infrastructures shall be compliant with specified gauge in ICD  | Rolling stock subsystem                         | 1 | F |
|         |  |  |                              | Overspeed   | Crossing of a train     | As same as 2.1.1.2  |   |   |   |
| 1.1.3.1 |  | Frontal collision  | Invisible vehicle            |   | Presence of other train | As same as 1.1.1.1  |   |   |   |
| 1.1.3.2 |  |  | Disappearance of a vehicle   |   | Presence of other train | As same as 1.1.1.2  |   |   |   |
| 1.1.3.3 |  |  | Stopping distance too long   |   | Presence of other train | As same as 1.1.1.3  |   |   |   |
| 1.1.3.4 |  |  | Fouling of the dynamic gauge |   | Presence of other train | As same as 1.1.2.5  |   |   |   |
| 1.1.3.5 |  |  | Reverse movement             | Traction Control Unit failure   | Presence of other train | A dependable train detection system shall be implemented on the line to ensure a safe distance between trains.<br>Signalling shall apply a safety brake in case of unrespected distance between trains.<br>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to 1 x 10-9 failure per hour. "<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.<br>Failure of management of direction assumed by traction shall have a failure rate lower or equal to 1 x 10-5 failure per hour per traction equipment.<br>A validation test shall be done to validate the correct design of the direction management on the train. | Operators<br>Rolling Stock subsystem<br>Signals | 1 | F |
|         |  |  |                              | Driver mistake when selecting the driving direction"  | Presence of other train | "Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to 1 x 10-9 failure per hour. "<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.<br>Personnel presence close to a train under voltage is forbidden.   | Operators<br>Signals                            | 1 | F |
|         |  |  |                              | Rupture of a semi-automatic coupler   |                         | As same as 1.1.1.1  |   | 1 | F |
|         |  |  |                              | Untimely uncoupling   |                         | As same as 1.1.1.1  |   | 1 | F |
|         |  |  |                              | Rupture of semi-permanent coupler   |                         | As same as 1.1.1.1  |   | 1 | F |
|         |  |  |                              | Loss of integrity: bad operation during coupling  |                         | As same as 1.1.1.1  |   | 1 | F |
|         |  |  |                              | Failure of the parking brake  |                         | As same as 1.1.1.1  |   | 1 | F |
| 1.1.4.1 |  | Collision with train or part of a train (not operation), | Invisible vehicle            | Unexpected entrance of a train in the operating area  |                         | As same as 1.1.1.1  |   | 1 | F |
|         |  |  |                              | The maintainer isolates the parking brake when the main pipe is under low pressure                                      | Presence of other train | Maintainer shall apply brake shoes or wheel wedges before isolating train parking brakes.   |   | 1 | F |

|         |   |   |   |   |  |  |  |   |   |
|---------|---|---|---|---|--|--|--|---|---|
| 1.1.4.2 |   |   | Disappearing of a vehicle   |   |  | As same as 1.1.1.2   |  | 1 | F |
| 1.1.4.3 |   |   | Stopping distance too long  |   |  | As same as 1.1.1.3   |  | 1 | F |
| 1.1.4.4 |   |   | Fouling of the dynamic gauge  |   |  | As same as 1.1.3.4   |  | 1 | F |
| 1.1.4.5 |   |   | Reverse movement  |   |  | As same as 1.1.3.5   |  | 1 | F |
| 1.2.1.1 | COLLISION BETWEEN A TRAIN AND FIXED EQUIPMENT | Collision with a mechanical part of a train   | Fall of a mechanical part of a train on the track due to binding failure / due to break | Inadequate design or manufacturing  |  | <p>Before line opening, a train must travel the whole line to ensure its clearance</p> <p>Windscreen compliance to NF F 15818 and NF F 31250 shall be demonstrated by validation tests.</p> <p>Lateral windows compliance to NF F 31129 and NFF 01-492 shall be demonstrated by validation tests.</p> <p>The design of the vehicle shall ensure the integrity of the structure and assembly of the parts of the rolling stock in worst case foreseeable conditions.</p> <p>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.</p> <p>Carbody integrity shall be validated by a calculation note for compression and fatigue</p> <p>Carbody integrity shall be validated by a fatigue test if calculation note conclusions indicate that it is required.</p> <p>Carbody integrity shall be validated by a validation test in compression</p> <p>Validation test shall be done to demonstrate couplers compliance to EN15227</p> <p>Validation test shall be done to demonstrate anti-climber devices compliance to EN15227</p> <p>"1 year inspection on carbody must include:</p> <ul style="list-style-type: none"> <li>- Visual inspection of mounting brackets of the underframe equipment including good tightening of the fixings of the boxes fixed to the underframe"</li> <li>"If an HFR nut is removed, it shall always be replaced by a new one. Where an assembly has already been tightened by the constructor, replacement of the fastener is compulsory if :</li> <li>- a thread lock has been used</li> <li>- a HFR nut has been used</li> <li>- a Nordlock (NL) or CS washer has been used</li> <li>- a non-reusable washer or nut has been used (according to the type of fastener)"</li> </ul> <p>The train shall comply to IEC 61373 regarding mechanical resistance to vibrations.</p> | Operators Rolling Stock subsystem            | 2 | F |
| 1.2.1.2 |   |   |   | Inadequate maintenance of the train   |  | <p>Maintainer shall respect the Maintenance Plan and Maintenance procedures.</p> <p>After revenue service, maintenance shall repair each train that displays incorrect operation status before next mission.</p> <p>Driver shall start the operation only if no incorrect operation status is indicated on the driver display unit.</p> <p>Maintenance staff shall be trained to intervene on Hanoi Line 3 train.</p> <p>United Joint Venture (UJV) shall train maintenance staff to intervene on Hanoi Line 3 train.</p>  | Rolling Stock subsystem                      | 2 | F |
| 1.2.2.1 |   | Collision with fixed equipment (trackside equipment, Overhead Contact System, infrastructure) | Collision due to a lateral movement of the vehicle                                      | Failure of suspension, bogie, connection vehicle-bogie, gauge dynamics, not respected gauge, interfaces vehicle station |  | <p>Infrastructures shall be compliant with specified gauge in ICD</p> <p>Pivot Bolster integrity shall be validated by a compression test and/or fatigue test if calculation note conclusions indicate that it is required.</p> <p>calculation note shall check bogie stability, and identify which configuration is the most pessimistic, including degraded conditions.</p> <p>Bogie stability shall be checked by validation test.</p> <p>A calculation note shall check bogie unloading due to track cant gradient (dQ/Q)</p> <p>A validation test shall check bogie unloading due to track cant gradient (dQ/Q)</p> <p>Secondary suspension shall have mechanical vertical stop to limit the train movement in case of flat or over-pressured suspension.</p>   | Maintenance Operator Rolling stock subsystem | 2 | F |
|         |   |   |   | Wrong calculation of the gauge  |  | <p>A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).</p> <p>A validation test shall be done to check train compliance to static and dynamic gauges.</p>  | Rolling stock subsystem                      | 2 | F |
|         |   |   |   | Extreme operating configuration not considered in regard to the vehicle gauge calculation                               |  | <p>A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).</p> <p>A validation test shall be done to check train compliance to static and dynamic gauges.</p>  | Rolling stock subsystem                      | 2 | F |
|         |   |   |   | Overspeed of train  |  | As same as 2.1.1.2   | Rolling stock subsystem                      | 2 | F |

|         |  |  |   |   |                                   |  |                         |   |   |
|---------|--|--|---|---|-----------------------------------|--|-------------------------|---|---|
|         |  |  |   | Excessive load or badly distributed   |                                   | A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).<br>A validation test shall be done to check train compliance to static and dynamic gauges. | Rolling stock subsystem | 2 | F |
| 1.2.2.2 |  |  | Collision with feeding system equipment                                 | Bad compatibility between conductor rail and train collector shoe                         |                                   | A 3rd rail current collector gauge analysis shall be done.   | Rolling stock subsystem | 2 | F |
|         |  |  |   | Incompatible distance between conductor rail and train collector shoe                     |                                   | A 3rd rail current collector gauge analysis shall be done.   | Rolling stock subsystem | 2 | F |
| 1.2.3.1 |  | Non observance of system limits                      | Collision at system limits  | Rupture of a semi-automatic coupler   |                                   | As same as 1.1.1.1   |                         | 2 | F |
|         |  |  |   | Untimely uncoupling   |                                   | As same as 1.1.1.1   |                         | 2 | F |
|         |  |  |   | Rupture of semi-permanent coupler   |                                   | As same as 1.1.1.1   |                         | 2 | F |
|         |  |  |   | Loss of integrity: bad operation during coupling  |                                   | As same as 1.1.1.1   |                         | 2 | F |
|         |  |  |   | Failure of the parking brake  |                                   | As same as 1.1.1.1   |                         | 2 | F |
|         |  |  |   | Stopping distance too long  |                                   | As same as 1.1.1.3   |                         | 2 | F |
|         |  |  |   | Train driver error  |                                   | As same as 1.1.1.3   |                         | 2 | F |
| 1.3.1.1 | COLLISION WITH HUMAN BEINGS OR ANIMALS | Collision with a human being on the track or walkway | Collision with a person on the track in case of evacuation              | Protected evacuation zone not respected by train  | Presence of human on the track    | Prior to authorize door opening for on line evacuation, traction power supply shall be cut off in both directions and the trains in the area shall be immobilized with safety brake.   | Signal                  | 2 | F |
|         |  |  |   | Train motion during evacuation on the line, on the related track or on the adjacent track | Presence of human on the track    | Prior to authorize door opening for on line evacuation, traction power supply shall be cut off in both directions and the trains in the area shall be immobilized with safety brake.<br>During evacuation, train shall be immobilized with safety brake.                                     | Operator<br>Signal      | 2 | F |
| 1.3.1.2 |  |  | Collision with a person accessing the track during passengers' exchange | Door opening on the wrong side at station, commanded by Signalling                        |                                   | As same as 4.2.2.2   |                         | 2 | F |
|         |  |  |   | Door opening on the wrong side at station, commanded by Train Control                     |                                   | As same as 4.2.2.2   |                         | 2 | F |
|         |  |  |   | Door opening on the wrong side at station   |                                   | As same as 4.2.2.2   |                         | 2 | F |
|         |  |  |   | Doors opening on the wrong side: train driver error                                       |                                   | An ergonomic analysis of the cabin shall be realized to prevent driver error (wrong command).  |                         | 2 | E |
|         |  |  |   | Manual door opening (EED) allowed on the wrong side at stationnary                        | Emergency Egress Device activated | As same as 4.2.2.2   |                         | 2 | F |
|         |  |  |   | Manual door opening (EED) allowed while the train is in motion                            | Emergency Egress Device activated | As same as 4.2.2.2   |                         | 2 | F |
|         |  |  |   | Loss of door closing effort in case of manual door  | Emergency Egress Device activated | As same as 4.2.2.2   |                         | 2 | F |

|         |  |   |   |   |                                |  |  |   |   |
|---------|--|---|---|---|--------------------------------|--|--|---|---|
|         |  |   |   | opening (EED) while the train is in motion.                                       |                                |  |  |   |   |
|         |  |   |   | Door opening while vehicle is not in correct position, commanded by Signalling    |                                | As same as 4.2.2.2   |  | 2 | F |
|         |  |   |   | Door opening while vehicle is not in correct position, commanded by Train Control |                                | As same as 4.2.2.2   |  | 2 | F |
|         |  |   |   | Door opening while vehicle is not in correct position, on door failure            |                                | As same as 4.2.2.2   |  | 2 | F |
|         |  |   |   | Door opening status not communicated to Signalling                                |                                | The erroneous "Door closed and locked" status provided by doors shall have a failure rate lower or equal to 5 x 10 <sup>-11</sup> failure per hour per door.<br>After repairing a door failure which request door lock out, maintenance staff shall check the correct status of the "Doors closed and locked" trainline when only the repaired door is opened.<br>Prior to authorize door opening for on line evacuation, traction power supply shall be cut off in both directions and the trains in the area shall be immobilized with safety brake.   |  | 2 | F |
|         |  |   |   | Spurious traction due to TCU (Traction Control Unit)                              | Presence of human on the track | "Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to 1 x 10 <sup>-9</sup> failure per hour. "<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.<br>Personnel presence close to a train under voltage is forbidden.<br>While not actuated, master controller shall automatically return on coasting position if it is in traction position.<br>Untimely traction of a motor without authorization from train shall have a failure rate lower or equal to 5 x 10 <sup>-7</sup> failure per hour for each traction equipment.<br>"Train shall be immobilized with Safety Brake while in depot.<br>Safety Brake shall only be released for testing purpose or for train departure." |  | 2 | F |
| 1.3.1.3 |  |   | Collision with staff during coupling / uncoupling             | Bad respect of coupling / uncoupling procedure                                    | Human on the track             | Access to track shall be restricted and submitted to rules, to prevent access to people unaware about dangers and risk of collision with running trains.   |  | 2 | F |
| 1.3.2.1 |  | Collision with human being in a specific area | Collision with staff working on the track (in a working area) | Failure of the parking brake  | Human on the track             | As same as 1.1.1.1   |  | 2 | F |
|         |  |   |   | Inefficient service braking   | Human on the track             | As same as 1.1.1.3   |  | 2 | F |
|         |  |   |   | Safety Brake failure or inefficiency  | Human on the track             | As same as 1.1.1.3   |  | 2 | F |
|         |  |   |   | Rupture of a semi-automatic coupler   | Human on the track             | As same as 1.1.1.1   |  | 2 | F |
|         |  |   |   | Untimely uncoupling   | Human on the track             | As same as 1.1.1.1   |  | 2 | F |
|         |  |   |   | Rupture of semi-permanent coupler   | Human on the track             | As same as 1.1.1.1   |  | 2 | F |
|         |  |   |   | Loss of integrity: bad operation during coupling                                  | Human on the track             | As same as 1.1.1.1   |  | 2 | F |
|         |  |   |   | Failure of the parking brake  | Human on the track             | As same as 1.1.1.3   |  | 2 | F |
|         |  |   |   | Overspeed in a working area   | Human on the track             | As same as 1.1.1.3   |  | 2 | F |

|         |  |  |  |  |                    |  |                      |   |   |
|---------|--|--|--|--|--------------------|--|----------------------|---|---|
|         |  |  |  | Train warning devices (horn, lights) not activated               | Human on the track | Driver shall use horn to warn human being or vehicle on the track.<br>Horn shall be available to warn maintenance staff/personnel on the track.<br>Horn shall have a failure rate lower than 5 x 10 <sup>-6</sup> failure per hour per horn.<br>Access to track shall be restricted and submitted to rules, to prevent access to people unaware about dangers and risk of collision with running trains.<br>Operator shall prevent access to tracks, depot and maintenance workshop to unauthorized people<br>White lights shall be available to indicate to maintenance staff/personnel on the track approach of a train.<br>White lights shall have a failure rate lower than 1 x 10 <sup>-6</sup> failure per hour per light.                               | Maintenance Operator | 2 | F |
|         |  |  |  | Staff in transfer area and unexpected movement of train          | Human on the track | "Train shall be immobilized with Safety Brake while in workshop.<br>If safety brake is released for maintenance purpose, wedges shall be used to immobilize it. "<br>Operator shall prevent access to tracks, depot and maintenance workshop to unauthorized people<br>Access to track shall be restricted and submitted to rules, to prevent access to people unaware about dangers and risk of collision with running trains.  | Maintenance Operator | 2 | F |
| 1.3.2.2 |  |  | Collision with a human being in a specific area                  | Failure of the parking brake                                     |                    | As same as 1.1.1.1   |                      | 2 | F |
|         |  |  |  | Inefficient service braking                                      |                    | As same as 1.1.1.3   |                      | 2 | F |
|         |  |  |  | Safety Brake failure or inefficiency                             |                    | As same as 1.1.1.3   |                      | 2 | F |
|         |  |  |  | Train driver error (spurious handling of the master controller)  | Human on the track | "Train shall be immobilized with Safety Brake while in depot.<br>Safety Brake shall only be released for testing purpose or for train departure."  | Operator             | 2 | F |
|         |  |  |  | Overspeed of train   |                    |  |                      | 2 | F |
|         |  |  |  | No detection of the loss of integrity of a train                 | Human on the track | Safety brake shall be activated in case of integrity loss of a train detected by electrical cut between two cars.  | Maintenance          | 2 | F |
|         |  |  |  | Train warning devices (horn, lights) not activated               |                    |  |                      | 2 | F |
|         |  |  |  | TCU failure  | Human on the track | "Train shall be immobilized with Safety Brake while in workshop.<br>If safety brake is released for maintenance purpose, wedges shall be used to immobilize it. "<br>Low power test shall be done on a single traction case at the time.   | Maintenance          | 2 | F |
| 1.3.2.3 |  | Collision with human on the platform           | Passenger standing on the side of the platform                   | Train warning devices (horn, lights) not activated               | Human on platform  | As same as 1.3.2.1   |                      | 2 | F |
|         |  |  | Fouling of the dynamic gauge                                     | Fouling of the dynamic gauge                                     | Human on platform  | As same as 1.1.2.5   |                      | 2 | F |
| 1.3.2.4 |  | Collision with an external object on the track | Presence of external object (out of railway system) on the track | Presence of external object (out of railway system) on the track |                    | Before line opening, a train must travel the whole line to ensure its clearance<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.<br>Carbody integrity shall be validated by a calculation note for compression and fatigue<br>Carbody integrity shall be validated by a fatigue test if calculation note conclusions indicate that it is required.<br>Carbody integrity shall be validated by a validation test in compression<br>Validation test shall be done to demonstrate couplers compliance to EN15227<br>Validation test shall be done to demonstrate anti-climber devices compliance to EN15227 | Maintenance          | 1 | F |
|         |  |  | Collision with objects from another train                        | Collision with objects from another train                        |                    | Underframe equipments shall have positive mounting.<br>"1 year inspection on carbody must include:<br>- Visual inspection of mounting brackets of the underframe equipment including good tightening of the fixings of the boxes fixed to the underframe"<br>"If an HFR nut is removed, it shall always be replaced by a new one. Where an assembly has already been tightened by the constructor, replacement of the fastener is compulsory if :<br>- a thread lock has been used<br>- a HFR nut has been used<br>- a Nordlock (NL) or CS washer has been used<br>- a non-reusable washer or nut has been used (according to the type of fastener)"   | Maintenance          | 1 | F |

| 2       | DERAILMENT / OVERTURN – Lack of vehicle stability – Loss of guidance during train movement |   |                    |   |  |   |                                     |        |        |
|---------|--|---|--------------------|---|--|---|-------------------------------------|--------|--------|
| 2.1.1.1 | LACK OF VEHICLE STABILITY  | Lack of vehicle stability during train movement | Load of vehicle    | Empty vehicle (incorrect design)  |  | A calculation note shall check bogie stability, and identify which configuration is the most pessimistic, including degraded conditions.<br>Bogie stability shall be checked by validation test.<br>A calculation note shall check bogie unloading due to track cant gradient (dQ/Q)<br>A validation test shall check bogie unloading due to track cant gradient (dQ/Q)   | Rolling stock subsystem             | 1      | F      |
|         |  |   |                    | Overloaded vehicle / Freight load badly distribute  |  | A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).<br>A validation test shall be done to check train compliance to static and dynamic gauges.  |                                     | 1      | F      |
|         |  |   |                    | Natural frequency appearing for a critical load   |  | The train shall comply to IEC 61373 regarding mechanical resistance to vibrations.<br>A calculation note shall check bogie stability, and identify which configuration is the most pessimistic, including degraded conditions.<br>Bogie stability shall be checked by validation test.<br>The train shall comply to IEC 61373 regarding mechanical resistance to vibrations.  |                                     | 1      | F      |
| 2.1.1.2 |  |   | Overspeed of train | Inefficient of safety braking due to automatic isolation of a service brake   |  | As same as 1.1.1.3  |                                     | 1      | F      |
|         |  |   |                    | Inefficient service braking   |  | As same as 1.1.1.3  |                                     | 1      | F      |
|         |  |   |                    | Safety Brake failure or inefficiency  |  | As same as 1.1.1.3  |                                     | 1      | E      |
|         |  |   |                    | Air production failure  |  | As same as 1.1.1.3  |                                     | 1      | F      |
|         |  |   |                    | Car load compensation failure   |  | As same as 1.1.1.3  |                                     | 1      | F      |
|         |  |   |                    | Overspeed due to traction system failure  |  | Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.<br>Failure of traction leading to overspeed shall have a failure rate lower or equal to $3,33 \times 10^{-5}$ failure per hour per traction unit.<br>The Driver shall be responsible to manage the train's speed and to respect lateral signalling.<br>The failure leading to the loss of speed indication on Driver Display Unit shall be lower or equal to $6 \times 10^{-5}$ failure per hour per display unit.<br>In case of inconsistency between speed indication on Tachometer and on Driver Display Unit, Driver shall signal it to OCC and train shall be send in maintenance at the end of the day to repair it.<br>In case of inconsistency between speed indication on Tachometer and on Driver Display unit, driver shall use the highest speed indicated as reference.<br>Tachometer failure rate shall be lower or equal to $1 \times 10^{-5}$ failure per hour. | Operator<br>Rolling Stock subsystem | 1      | F      |
|         |  |   |                    | Undue manual isolation of a brake panel due to human error  |  | As same as 1.1.1.3  |                                     | 1      | F      |
|         |  |   |                    | Deterioration / Cracking of the brake discs due to a parking brake still applied<br>Or due to remaining / spurious pressure in brake cylinder |  | As same as 1.1.1.3  |                                     | 1<br>1 | F<br>F |
|         |  |   |                    | Low wheel/rail adhesion factor - Safety brake   |  | All rails (main-line, depot, workshop and stabling areas) shall be conform to track profile defined in contract.<br>Wheel profile shall comply with NFF-03-402.<br>A validation test shall be performed to confirm the correct operation of wheel slide protection of safety brake on tracks with low adhesion level.<br>Operation shall maintain the tracks in correct state of cleanness and prevent its excessive wearing<br>Train shall be equipped with sanding system.  | Operator<br>Rolling Stock subsystem | 1      | F      |

|         |  |  |   |  |   |                         |   |   |
|---------|--|--|---|--|---|-------------------------|---|---|
|         |  |  |   |  | Signalling shall ensure that there is always adequate safety distance between two RSK in operation to prevent collision in case of Safety Brake (assuming the minimum guaranteed deceleration rate)   |                         |   |   |
|         |  |  |   | Loss of control command (TCMS)   | As same as 1.1.1.3  |                         | 1 | F |
|         |  |  |   | Speed higher than expected, driver error   | As same as 1.1.1.3  |                         | 1 | F |
|         |  |  |   | Loss of vigilance of the driver  | As same as 1.1.1.3  |                         | 1 | F |
|         |  |  |   | Erroneous display of the speed   | As same as 1.1.1.3  |                         | 1 | F |
| 2.1.1.3 |  |  | Failure of the train guidance equipment | Failure of the bogie or carbody / bogie link   | Pivot Bolster integrity shall be validated by a compression test and/or fatigue test if calculation note conclusions indicate that it is required.  | Rolling stock subsystem | 1 | F |
|         |  |  |   | Failure of the suspension bogie  | A calculation note shall check bogie stability, and identify which configuration is the most pessimistic, including degraded conditions.<br>Bogie stability shall be checked by validation test.<br>A calculation note shall check bogie unloading due to track cant gradient (dQ/Q)<br>A validation test shall check bogie unloading due to track cant gradient (dQ/Q)<br>Secondary suspension shall have mechanical vertical stop to limit the train movement in case of flat or over-pressured suspension.   | Rolling stock subsystem | 1 | F |
|         |  |  |   | No release of parking brake leading to overheating of breaking equipment.  | Mechanical Brake failure leading to non parking brake release at bogie level shall be lower than 5 x 10 <sup>-7</sup> failure per hour.<br>Parking brake monitoring failure leading to non detection of parking brake applied at bogie level shall be lower than 5 x 10 <sup>-8</sup> failure per hour.<br>Train monitoring system shall made coherency check between brakes status train lines and local brakes status with an integrity level at least equal to SIL-0<br>Traction inhibition failure while parking brake is detected applied shall be lower than 1 x 10 <sup>-7</sup> failure per hour.   | Rolling stock subsystem | 1 | E |
|         |  |  |   | No release of pneumatic brake leading to overheating of breaking equipment.                                      | Mechanical Brake failure leading to non service brake release at bogie level shall be lower than 1 x 10 <sup>-7</sup> failure per hour.<br>Service brake monitoring failure leading to non detection of service brake applied at bogie level shall be lower than 5 x 10 <sup>-8</sup> failure per hour.<br>Train monitoring system shall made coherency check between brakes status train lines and local brakes status with an integrity level at least equal to SIL-0<br>Brake's wheel slide protection function shall also ensure a axle blocked detection function.<br>Traction inhibition failure while pneumatic brake is detected applied shall be lower than 1 x 10 <sup>-7</sup> failure per hour. | Rolling stock subsystem | 1 | F |
|         |  |  |   | Failure of mechanical part of the roller bearing system.   | A calculation note shall check bogie stability, and identify which configuration is the most pessimistic, including degraded conditions.<br>Bogie stability shall be checked by validation test.<br>A calculation note shall check bogie unloading due to track cant gradient (dQ/Q)<br>A validation test shall check bogie unloading due to track cant gradient (dQ/Q)<br>All rails (main-line, depot, workshop and stabling areas) shall be conform to track profile defined in contract.<br>Wheel profile shall comply with NFF-03-402.<br>Gearbox (bearing and gears) and axle box bearings shall be properly sized.<br>A finite element analysis shall be performed to ensure axle box resistance.     | Rolling stock subsystem | 1 | F |
|         |  |  |   | Mechanical blocking of an axle except axle bearing failure: seizing of a traction motor / failure of the gearbox | Gearbox (bearing and gears) and axle box bearings shall be properly sized.<br>Endurance validation test shall be done on gearbox.<br>Lubrication validation test shall be done on gearbox.<br>Brake's wheel slide protection function shall also ensure a axle blocked detection function.  |                         | 1 | F |
|         |  |  |   | Failure of the axle bogie  | The axles shall comply with EN 13261<br>Trailer axles shall comply to EN 13103<br>Powered axles shall comply to EN 13104<br>Brake's wheel slide protection function shall also ensure a axle blocked detection function.  | Rolling stock subsystem | 1 | F |



|          |   |  |   |   |  |  |  |   |   |
|----------|---|--|---|---|--|--|--|---|---|
|          |   |  |   | Unexpected opening of one or several detrainment doors of vehicle in motion   |  | As same as 7.2.1.2   |  | 1 | F |
| 2.1.2.1  |   | Lack of stability stopped in curve     | Load of vehicle                             |   |  | As same as 2.1.1.1   |  | 1 | F |
| 2.2.1.1  | LOSS OF GUIDANCE                                    | Due to rolling stock failure           | Overspeed of train                          | Too high traction effort or inefficient braking   |  | As same as 2.1.1.2   |  | 1 | F |
|          |   |  |   | Adhesion problem  |  |  |  | 1 | F |
| 2.2.1.2  |   |  | Failure of train guidance                   | Failure of the train guidance equipment   |  | As same as 2.1.1.3   |  | 1 | F |
| 2.2.1.3  |   |  | Failure of a mechanical part                | Inadequate design or manufacturing  |  | As same as 2.1.1.3   |  | 1 | F |
|          |   |  |   | Inadequate maintenance  |  | As same as 2.1.1.3   |  | 1 | F |
| 2.2.2.1  |   | Due to external conditions             | Presence of external objects                | Presence of external object (out of railway system) on the track  |  | As same as 2.1.1.3   |  | 1 | F |
|          |   |  |   | Derailment due to objects from another train  |  | As same as 2.1.1.3   |  | 1 | F |
| 2.2.2.2  |   | Driver errors                          | Driver errors                               | Loss of guidance due to train driver error  |  | As same as 2.1.1.3   |  | 1 | F |
| <b>3</b> | <b>GAS EMISSION – TOXIC SMOKE – AIR VENTILATION</b> |  |   |   |  |  |  |   |   |
| 3.1.1.1  | GAS EMISSION  | Presence of polluting materials /fluid |   | Contact between two different products or fluids<br>Use of toxic Products /materials"   |  | The selection of material shall be in line with EC 1907/2006: REACH regulation for Registration, Evaluation and Authorization of chemical substances<br>Cleaning staff and maintenance staff shall only use product(s) complying with list provided by carbuilder  | Rolling stock subsystem<br>Maintenance | 3 | F |
| 3.2.1.1  | TOXIC SMOKE   | Emission due to on-board fire          | Fire  | - Ignition due to electrical failure<br>- Ignition due to overheating of electromechanic equipment's onboard the train (following intrinsic failure, loss of cooling,...) |  | Train shall comply with EN 45545.<br>Surge arrestor shall comply with IEC 61287-1.<br>The train shall comply with the requirements of EN 50153 regarding protective provision relating to electrical hazards<br>Each door shall be equipped with an Emergency Egress Device to allow evacuation.<br>Ventilation shall be automatically stopped in the saloon areas where smoke is detected.<br>Power supply shall be automatically stopped in the underframe areas where fire is detected. | Rolling stock subsystem                | 2 | F |
|          |   |  |   | Ignition due to overheating HVAC heating unit   |  | Heaters activation shall be prevented in case of loss of ventilation.<br>Heaters shall be protected by thermal breaker to prevent excessive heating.<br>HVAC unit shall be equipped with air filters.<br>Appropriate maintenance of the train filters shall be done regularly to limit the accumulation of waste liable to ignite (fire risk).   | Rolling stock subsystem                | 2 | F |
|          |   |  |   | Presence of smoke due to a maintenance intervention   |  | Maintenance regulations as in 1.2.1.2  | Maintenance                            | 2 | F |
| 3.2.1.2  |   |  | Explosion                                   | Explosive liquids or gas giving off toxic smoke   |  | Train shall comply with EN 45545   | RS subsystem                           | 2 | F |
| 3.2.2.1  |   | Emission due to chemical reaction      | Contact between two incompatible substances | Liquids or gas used during a maintenance intervention   |  | The selection of material shall be in line with EC 1907/2006: REACH regulation for Registration, Evaluation and Authorization of chemical substances<br>Cleaning staff and maintenance staff shall only use product(s) complying with list provided by carbuilder  | Rolling stock subsystem                | 2 | F |
|          |   |  |   | Incompatibility between materials used and the conditions of use  |  | The selection of material shall be in line with EC 1907/2006: REACH regulation for Registration, Evaluation and Authorization of chemical substances<br>Cleaning staff and maintenance staff shall only use product(s) complying with list provided by carbuilder  | Maintenance                            | 2 | F |
| 3.2.2.3  |   | Emission due to fire in                | Presence of smoke in a                      | Natural entrance of smoke in the train  |  | "In case of smoke or fire detection outside the train, the operator/OCC shall<br>- Not allow a train to enter in a fire or smoked area   | Rolling stock subsystem                | 2 | F |

|          |  |                                       |  |  |  |  |   |   |   |
|----------|--|---------------------------------------|--|--|--|--|---|---|---|
|          |  | a station / in depot                  | station and entrance of toxic smoke in the train |  |  | - Evacuate all trains to safe area (away of smoke)"<br>In case of smoke or fire detection outside the train, the fresh air dampers of ventilation shall be closed to avoid the entrance of smoke inside the train<br>Ventilation shall be automatically stopped in the saloon areas where smoke is detected.<br>In case of smoke detection in the train, passengers shall be evacuated , if possible at next station.  |   |   |   |
|          |  |                                       |  | Entrance of smoke in the train caused by the ventilation |  | Ventilation shall be automatically stopped in the saloon areas where smoke is detected.  | Rolling stock subsystem                 | 2 | E |
| 3.3.1.1  | LACK OF AIR RENEWAL  | Due to on-board ventilation           | Insufficient ventilation                         | Obstruction of air ducts                                 |  | HVAC unit shall be equipped with air filters.<br>Appropriate maintenance of the train filters shall be done regularly to limit the accumulation of waste liable to ignite (fire risk).   | RS system Maintenance                   | 3 | E |
|          |  |                                       |  | Failure of ventilation                                   |  | A calculation note shall be done to check the compliance of ventilation unit to minimal air flow required in the contract in emergency ventilation.<br>Validation test shall demonstrate compliance of ventilation unit to minimal air flow required in the contract in emergency ventilation.<br>When the automatic ventilation fails during revenue service, the emergency ventilation shall be maintained<br>In case of smoke detection in the train, passengers shall be evacuated , if possible at next station.  | Rolling stock subsystem Operator        | 3 | E |
|          |  |                                       |  | Failure of ventilation power supply                      |  | Auxiliary converters shall be design to supply minimal ventilation rate according to relevant standards in case of failure a single converter.<br>A validation test shall be done to check that emergency ventilation is ensured when a single auxiliary converter fails.<br>A calculation note shall be done to check that battery dimensioning complies with contract requirement.<br>A validation test shall be done to check that battery dimensioning complies with contract requirement.<br>The failure leading to the loss of both auxiliary converters shall have a failure rate lower or equal to $1 \times 10^{-5}$ failure per hour.<br>The failure leading to the loss of the battery shall have a failure rate lower or equal to $3,76 \times 10^{-7}$ failure per hour per battery.  | Rolling stock subsystem                 | 3 | E |
| <b>4</b> | <b>FALLS – inside a vehicle and from the train on to the track</b> |                                       |  |  |  |  |   |   |   |
| 4.1.1.1  | FALL INSIDE A VEHICLE  | Lack of balance during train movement | Slipping   | Slippery flooring material                               |  | "Floor covering shall be made to be slip resistant. The determination of the anti-slip property shall be made following :<br>- EN 14041:2005 - Resilient, textile and laminate floor coverings Essential characteristics clause 4.5 or<br>- DIN 51130; Testing of floor coverings - Determination of the anti-slip property - Workrooms and fields of activities with slip danger, walking method - Ramp test<br>Or following another equivalent standard<br>A validation report shall be provided by supplier."   | Rolling stock subsystem                 | 3 | E |
|          |  |                                       |  | Humid or polluted flooring (inadequate cleaning product) |  | Operator shall clean the floor with products that comply with the requirements manufacturer defined in the maintenance manual.   | Maintenance                             | 3 | E |
| 4.1.1.2  |  |                                       | Obstacles  | Obstacles set by the design                              |  | With the exception of platforms tripod bars, no obstacle shall be in the middle of the train.<br>Interior arrangements shall allow free feet movement and prevent passengers to trip on it.  | Rolling stock subsystem                 | 3 | F |
|          |  |                                       |  | Obstacles due to a passenger                             |  | The operator shall not allow the presence of animals which can disturb the movement of passengers in that train or in station. Exceptions like guiding dogs for blind people can be considered.  | Operator                                | 3 | E |
|          |  |                                       |  | Abnormal acceleration                                    |  | "A calculation note shall be done to ensure traction acceleration performances:<br>- acceleration from 0 to 35km/h is equal 1.00 m/s <sup>2</sup> in EL6.6 including jerk of 0.8m/s <sup>3</sup><br>-acceleration from 0 to 70 km/h remains superior to 0.75 m/s <sup>2</sup> in EL6.6 including jerk of 0.8m/s <sup>3</sup><br>- residual acceleration at 80 km/h remains superior to 0.1 m/s <sup>2</sup> in EL6.6<br>- starting acceleration remains inferior to 1.2m/s <sup>2</sup> in ELE<br><br>The calculation note shall also determine how equipment failures are acceptable to respect the performances in degraded mode."<br>"A validation test shall be done to ensure traction acceleration performances:<br>- acceleration from 0 to 35km/h is equal 1.00 m/s <sup>2</sup> in EL6.6 including jerk of 0.8m/s <sup>3</sup><br>-acceleration from 0 to 70 km/h remains superior to 0.75 m/s <sup>2</sup> in EL6.6 including jerk of 0.8m/s <sup>3</sup><br>- residual acceleration at 80 km/h remains superior to 0.1 m/s <sup>2</sup> in EL6.6<br>- starting acceleration remains inferior to 1.2m/s <sup>2</sup> in ELE" | Rolling stock subsystem<br><br>Operator | 3 | F |
|          |  |                                       |  | Abnormal deceleration                                    |  | "A calculation note shall be done to confirm that service brake is designed to reach the following performances:<br>- under EL6.6 in nominal conditions, the deceleration shall be at least 1,1 m/s <sup>2</sup> .   | Rolling stock subsystem                 | 3 | F |

|         |  |  |  |                                     |   |  |   |   |
|---------|--|--|--|-------------------------------------|---|--|---|---|
|         |  |  |  |                                     | <p>- under EL6.6 with one car isolated, the deceleration shall be at least 1,1 m/s<sup>2</sup>.<br/>- Jerk for deceleration shall be limited to 0,8 m/s<sup>3</sup>.</p> <p>The calculation note shall also determine how many actuator failures are acceptable to respect the degraded performance."<br/>A validation test shall be performed to confirm the service brake performances (in nominal and degraded mode).<br/>"A calculation note shall be done to confirm that safety brake is designed to reach the following performances:<br/>- under EL6.6 in nominal conditions, the deceleration shall be at least 1,35 m/s<sup>2</sup>.<br/>- under EL6.6 with one car isolated, the deceleration shall be at least 0,72 m/s<sup>2</sup>.<br/>- Maximum tolerable jerk for deceleration from 80km/h to 0 km/h shall less than 4 m/s<sup>3</sup>, according to EN 13452-1.</p> <p>The calculation note shall also determine how many actuator failures are acceptable to respect the degraded performance."<br/>A validation test shall be performed to confirm the safety brake performances (in nominal and degraded mode).</p>   | Operator                               |   |   |
| 4.1.1.3 |  |  | Insufficient lighting                              | Incorrect design of lighting system | <p>The train shall comply with standard EN 13272 §5.3 which requires two independent architectures for: nominal lighting and emergency lighting<br/>The lighting architecture must be designed in order to be compliant with table 2 of EN 13272.</p>   | Rolling stock subsystem                | 3 | F |
|         |  |  |  | Failure of lighting system          | <p>Train control failure leading to the lighting level reduction below 50 lux shall have a failure rate lower or equal to 1 x 10<sup>-9</sup> failure per hour.<br/>Saloon lighting system failure leading to the lighting level reduction below 50 lux shall have a failure rate lower or equal to 1 x 10<sup>-9</sup> failure per hour per car.<br/>"1 year inspection on train must include:<br/>- Visually check the floor coverings for any signs of damages and ensure they are properly intact (pay special attention on all joints).<br/>- Check all signage for any signs of damaged.<br/>- Check the presence of the fire extinguisher and the date of validity<br/>- Visually examine each body side door panel, body side windows glazed panel, door leaf windows glazed panel and door seals for any signs of damages.<br/>- Visually check windows and windscreens for any signs of damages.<br/>- Visually check passengers doors lighting are working properly<br/>- Visually check and ensure that all passengers' seats and under seat covers and are not damaged.<br/>- Visually check all saloon lighting is functioning. Check the lighting diffuser panels for any signs of damages and ensure they are properly secured, replace any faulty lights if required.<br/>- Check all grab poles and handrails for any signs of damaged and ensure they are properly fixed.<br/>- Check for signs of water ingress."</p> | Rolling stock subsystem                | 3 | F |
| 4.1.1.4 |  |  | Absence or failure of support equipment of persons | Absence or failure of a support bar | <p>Prehension points shall be available for passengers from any point of the saloon.<br/>1 year inspection on train must include:<br/>- Visually check the floor coverings for any signs of damages and ensure they are properly intact (pay special attention on all joints).<br/>- Check all signage for any signs of damaged.<br/>- Check the presence of the fire extinguisher and the date of validity<br/>- Visually examine each body side door panel, body side windows glazed panel, door leaf windows glazed panel and door seals for any signs of damages.<br/>- Visually check windows and windscreens for any signs of damages.<br/>- Visually check passengers doors lighting are working properly<br/>- Visually check and ensure that all passengers' seats and under seat covers and are not damaged.<br/>- Visually check all saloon lighting is functioning. Check the lighting diffuser panels for any signs of damages and ensure they are properly secured, replace any faulty lights if required.<br/>- Check all grab poles and handrails for any signs of damaged and ensure they are properly fixed.<br/>- Check for signs of water ingress."</p>   | Rolling stock subsystem<br>Maintenance | 3 | F |
|         |  |  |  | Failure of a seat binding           | <p>A calculation note shall demonstrate seats robustness.<br/>A validation test shall be done to demonstrate seats robustness.<br/>A calculation note shall demonstrate that train structure can hold seats.<br/>"1 year inspection on train must include contents as in <b>Absence or failure of a support bar</b></p>   | RS subsystem<br>Maintenance            | 3 | F |

|         |  |                                   |   |  |  |   |   |   |   |
|---------|--|-----------------------------------|---|--|--|---|---|---|---|
| 4.1.1.5 |  |                                   | Instability of passengers during coupling | Speed approach during coupling not limited               |  | As same as 1.1.1.1  |   |   |   |
|         |  |                                   |   | Bad coupling / uncoupling                                |  | The Driver is responsible to manage the coupling speed of the train that shall be limited to 3 km/h to prevent irreversible deformations of coupling and shock absorber devices.<br>The supplier of semi-automatic coupler shall demonstrate that the unexpected uncoupling of semi-automatic coupler reaches the target of $1 \times 10^{-9}$ failure per hour.<br>The uncoupling shall be prevented when the train is not at standstill   | Rolling stock subsystem                       | 3 | F |
| 4.1.2.1 |  | Lack of balance during evacuation | Slipping                                  | Slippery flooring material                               |  | As same as 4.1.1.1  | RS system Maintenance                         | 3 | F |
|         |  |                                   |   | Humid or polluted flooring (inadequate cleaning product) |  | As same as 4.1.1.1  | RS subsystem Maintenance                      | 3 | F |
| 4.1.2.2 |  |                                   | Unexpected train motion                   | Unexpected operation from train driver                   |  | Prior to authorize door opening for on line evacuation, traction power supply shall be cut off in both directions and the trains in the area shall be immobilized with safety brake.<br>During evacuation, train shall be immobilized with safety brake.<br>In case emergency evacuation, if ATC failure prevents doors opening, driver shall switch to protected mode to open the doors.<br>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to $1 \times 10^{-9}$ failure per hour. "<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.<br>Before allowing doors opening for evacuation, the operator shall ensure that the 3rd rail is de-energized.                           | Operator<br>Signal                            | 3 | F |
|         |  |                                   |   | Untimely traction order from Signalling                  |  | The loss of Holding brake command / untimely traction authorization from Signalling to train shall have a failure rate lower or equal to $1 \times 10^{-7}$ failure per hour.<br>The untimely force signal provided by Signalling via Ethernet shall have a failure rate lower or equal to $1 \times 10^{-5}$ failure per hour.<br>The erroneous "All doors closed and locked" status provided by train to Signalling and traction authorization shall have a failure rate lower or equal to $1 \times 10^{-9}$ failure per hour.<br>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to $1 \times 10^{-9}$ failure per hour. "<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake. | Operator<br>Signal                            | 3 | F |
|         |  |                                   |   | Untimely traction order from Train control               |  | The untimely Traction Enabled authorization from train to traction shall have a failure rate lower or equal to $1 \times 10^{-8}$ failure per hour.<br>The untimely force signal provided by Train Control System via Ethernet shall have a failure rate lower or equal to $1 \times 10^{-5}$ failure per hour.<br>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to $1 \times 10^{-9}$ failure per hour. "<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.   | Rolling stock subsystem<br>Operator<br>Signal | 3 | F |
|         |  |                                   |   | Untimely traction during passenger exchange              |  | The untimely traction without "traction and electrical brake Enable" authorization shall have a failure rate lower or equal to $5 \times 10^{-7}$ failure per hour.<br>The untimely application of traction force signal by Traction electronic while no traction force signal is received via Ethernet shall have a failure rate lower or equal to $1 \times 10^{-5}$ failure per hour.<br>The failures of holding brake control equipment causing the movement of the train shall have a failure rate lower or equal to $1 \times 10^{-7}$ failure per hour.<br>The failures of bogie brake equipment causing the movement of the train while in holding brake shall have a failure rate lower or equal to $1 \times 10^{-7}$ failure per hour.<br>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.  | Rolling stock subsystem<br>Operator<br>Signal | 3 | F |

|         |                                |  |                                    |  |  |  |   |   |   |
|---------|--------------------------------|--|------------------------------------|--|--|--|---|---|---|
|         |                                |  |                                    |  |  | Failure rate of safety brake command from Signalling shall be lower or equal to 1 x 10 <sup>-9</sup> failure per hour. " Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.   |   |   |   |
|         |                                |  |                                    | Inefficient safety braking                               |  | During evacuation, train shall be immobilized with safety brake.<br>Failure rate of safety brake order transmission to brakes shall lower or equal to 1 x 10 <sup>-9</sup> failure per hour.<br>Non respect of safety brake performances, including failures of load compensation and wheel slide protection, shall not have a failure rate lower or equal to 1 x 10 <sup>-9</sup> failure per hour.<br>"A calculation note shall be done to confirm that safety brake is designed to reach the following performances:<br>- under EL6.6 in nominal conditions, the deceleration shall be at least 1,35 m/s <sup>2</sup> .<br>- under EL6.6 with one car isolated, the deceleration shall be at least 0,72 m/s <sup>2</sup> .<br>- Maximum tolerable jerk for deceleration from 80km/h to 0 km/h shall less than 4 m/s <sup>3</sup> , according to EN 13452-1.<br><br>The calculation note shall also determine how many actuator failures are acceptable to respect the degraded performance."<br>A validation test shall be performed to confirm the safety brake performances (in nominal and degraded mode). | Rolling stock subsystem<br><br>Operator<br><br>Signal | 3 | F |
| 4.1.2.3 |                                |  | Insufficient lighting              | Incorrect design of lighting system                      |  | As same as 4.1.1.3   | RS subsystem  | 3 | F |
|         |                                |  |                                    | Failure of lighting system                               |  | As same as 4.1.1.3   | RS subsystem  | 3 | F |
| 4.1.3.1 |                                | Lack of balance during passengers' exchange            | Slipping                           | Slippery flooring material                               |  | As same as 4.1.1.1   | Rolling stock subsystem<br><br>Maintenance            | 3 | F |
|         |                                |  |                                    | Humid or polluted flooring (inadequate cleaning product) |  | As same as 4.1.1.1   | RS subsystem<br>Maintenance                           | 3 | F |
| 4.1.3.2 |                                |  | Obstacles                          | Obstacles set by the design                              |  | As same as 4.1.1.2   | RS subsystem  | 3 | F |
|         |                                |  |                                    | Obstacles due to a passenger                             |  | As same as 4.1.1.2   | Operator  | 3 | E |
|         |                                |  |                                    | Abnormal acceleration                                    |  | As same as 4.1.1.2   | RS subsystem<br>Operator                              | 3 | F |
|         |                                |  |                                    | Abnormal deceleration                                    |  | As same as 4.1.1.2   | RS subsystem<br>Operator                              | 3 | F |
| 4.1.3.3 |                                |  | Unexpected train motion            | Unexpected operation from train driver                   |  | As same as 4.1.1.3   | Operator<br>Signal                                    | 3 | F |
|         |                                |  |                                    | Untimely traction order from Signalling                  |  | As same as 4.1.1.3   | Operator<br>Signal                                    | 3 | F |
|         |                                |  |                                    | Untimely traction order from Train control               |  | As same as 4.1.1.3   | RS subsystem<br>Operator                              | 3 | F |
|         |                                |  |                                    | Untimely traction during passenger exchange              |  | As same as 4.1.1.3   | RS subsystem<br>Operator                              | 3 | F |
|         |                                |  |                                    | Inefficient safety braking                               |  | As same as 4.1.1.3   | RS subsystem<br>Operator                              | 3 | F |
| 4.2.1.1 | FALL FROM TRAIN ONTO THE TRACK | Opening or breach in the vehicle during train movement | Break of a fixed part of a vehicle | Break of the window                                      |  | Lateral windows compliance to NF F 31129 and NFF 01-492 shall be demonstrated by validation tests.<br>1 year inspection on train must include:<br>- Visually check the floor coverings for any signs of damages and ensure they are properly intact (pay special attention on all joints).<br>- Check all signage for any signs of damaged.<br>- Check the presence of the fire extinguisher and the date of validity<br>- Visually examine each body side door panel, body side windows glazed panel, door leaf windows glazed panel and door seals for any signs of damages.   | Maintenance   | 1 | F |

|         |  |  |   |   |                                   |  |              |   |   |
|---------|--|--|---|---|-----------------------------------|--|--------------|---|---|
|         |  |  |   |   |                                   | <ul style="list-style-type: none"> <li>- Visually check windows and windscreens for any signs of damages.</li> <li>- Visually check passengers doors lighting are working properly</li> <li>- Visually check and ensure that all passengers' seats and under seat covers and are not damaged.</li> <li>- Visually check all saloon lighting is functioning. Check the lighting diffuser panels for any signs of damages and ensure they are properly secured, replace any faulty lights if required.</li> <li>- Check all grab poles and handrails for any signs of damaged and ensure they are properly fixed.</li> <li>- Check for signs of water ingress."</li> </ul>   |              |   |   |
|         |  |  |   | Break of the windshield   |                                   | <p>Windscreen compliance to NF F 15818 and NF F 31250 shall be demonstrated by validation tests.</p> <p>1 year inspection on train must include contents as in risk reduction means for Break of the window above</p>  | Maintenance  | 1 | F |
|         |  |  |   | Break of the gangway  |                                   | <p>A calculation note shall be done to demonstrate that gangway design can sustain AW3 load</p> <p>A validation test shall check that gangway do not collapse under ELE8 load and is not damaged.</p> <p>A calculation note shall be done to demonstrate that gangway can be used in the worst conditions defined in the line plan.</p> <p>A validation test shall check that gangway is not damaged in worst conditions defined in the line plan.</p> <p>The car-car clearance shall be defined by calculation note or by simulation.</p> <p>Car-car clearance shall be checked by validation test</p>  | Maintenance  | 1 | F |
| 4.2.1.2 |  |  | Unexpected operation of the vehicle doors | Door opening while vehicle is in motion, commanded by Signalling    |                                   | <p>Untimely door enable command provided by Signalling shall have a failure rate lower or equal to <math>3 \times 10^{-8}</math> failure per hour.</p> <p>Zero Velocity information provided by Signalling while train is running shall have a failure rate lower or equal to <math>1 \times 10^{-6}</math> failure per hour.</p> <p>Untimely door opening command provided by Signalling via Ethernet shall have a failure rate lower or equal to <math>1 \times 10^{-5}</math> failure per hour.</p>   | RS subsystem | 1 | F |
|         |  |  |   | Door opening while vehicle is in motion, commanded by Train control |                                   | <p>Untimely door enable command provided by train control shall have a failure rate lower or equal to <math>3 \times 10^{-8}</math> failure per hour.</p> <p>Zero Velocity information provided by train control while train is running shall have a failure rate lower or equal to <math>1 \times 10^{-6}</math> failure per hour.</p> <p>Zero Velocity information provided by Traction electronic while train is running shall have a failure rate lower or equal to <math>1 \times 10^{-5}</math> failure per hour.</p> <p>Zero Velocity information provided by Braking electronic while train is running shall have a failure rate lower or equal to <math>1 \times 10^{-6}</math> failure per hour.</p> <p>Untimely door opening command provided by train control via Ethernet shall have a failure rate lower or equal to <math>1 \times 10^{-5}</math> failure per hour.</p> <p>Door failures leading to electrical supply of doors enable trainline shall have a failure rate lower or equal to <math>1 \times 10^{-9}</math> failure per hour per door.</p> <p>Door failures leading to electrical supply of doors zero velocity trainline shall have a failure rate lower or equal to <math>5 \times 10^{-8}</math> failure per hour per door.</p> <p>A validation test shall be done at train level to check the correct operation of door opening function: Doors shall only open if all conditions specified in technical specification are present.</p> | RS subsystem | 1 | F |
|         |  |  |   | Door opening while vehicle is in motion, on door failure            |                                   | <p>The untimely opening of a door when train is in movement, with no authorisation from train shall have a failure rate lower or equal to <math>1 \times 10^{-9}</math> failure per hour.</p>  | RS subsystem | 1 | F |
|         |  |  |   | Manual door opening (EED) allowed while the train is in motion      | Emergency Egress Device activated | <p>Loss of Hold Door Closed signal from signalling while the train is in motion and an Emergency Egress Demand is activated shall be less than <math>1 \times 10^{-7}</math> failure per hour.</p> <p>Zero Velocity information provided by train control while train is running shall have a failure rate lower <math>1 \times 10^{-6}</math> failure per hour.</p> <p>Loss of Hold Door Closed signal from train control while the train is in motion shall be less than <math>1 \times 10^{-7}</math> failure per hour.</p> <p>Zero Velocity information provided by Traction electronic while train is running shall have a failure rate lower or equal to <math>1 \times 10^{-5}</math> failure per hour.</p> <p>Zero Velocity information provided by Braking electronic while train is running shall have a failure rate lower or equal to <math>1 \times 10^{-6}</math> failure per hour.</p> <p>Warning shall be set to inform passenger about their responsibility and possible prosecution while using the EED.</p> <p>A validation test shall be done at train level to check the correct operation of emergency egress devices.</p> <p>Emergency Egress Device shall either include a cover or have a design that prevent the handle of Emergency Egress Device from accidental operation.</p>  | RS subsystem | 1 | F |

|         |  |  |  |  |  |  |                       |   |   |
|---------|--|--|--|--|--|--|-----------------------|---|---|
|         |  |  |  | Loss of door closing effort in case of manual door opening (EED) while the train is in motion. |  | Untimely door opening on Emergency Egress Device activation, with no train authorization, shall have a failure rate lower or equal to $2 \times 10^{-7}$ failure per hour per door.<br>Warning shall be set to inform passenger about their responsibility and possible prosecution while using the Emergency Egress Device.<br>Emergency Egress Device shall either include a cover or have a design that prevent the handle of Emergency Egress Device from accidental operation.  | RS subsystem          | 1 | F |
|         |  |  |  | Non detection of the opening of one or more doors  |  | The erroneous "Door closed and locked" status provided by doors shall have a failure rate lower or equal to $5 \times 10^{-11}$ failure per hour per door.<br>The erroneous "All doors closed and locked" status provided by train to Signalling and traction authorization shall have a failure rate lower or equal to $1 \times 10^{-9}$ failure per hour.   | RS subsystem          | 1 | F |
| 4.2.1.2 |  |  | Departure with open doors or doors closed but not locked | Erroneous doors closed and locked status allowing traction                                     |  | The erroneous "Door closed and locked" status provided by doors shall have a failure rate lower or equal to $5 \times 10^{-11}$ failure per hour per door.<br>The erroneous "All doors closed and locked" status provided by train to Signalling and traction authorization shall have a failure rate lower or equal to $1 \times 10^{-9}$ failure per hour.<br>All door failures resulting in a door not closed and locked, despite closing order, shall have a failure rate lower or equal to $1 \times 10^{-4}$ failure per hour at train level.<br>All train failures resulting in a door not closed and locked, despite closing order, shall have a failure rate lower or equal to $1 \times 10^{-4}$ failure per hour.<br>Door failures leading to electrical supply of doors closed and locked trainline shall have a failure rate lower or equal to $1 \times 10^{-9}$ failure per hour per door.<br>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to $1 \times 10^{-9}$ failure per hour."<br>A validation test shall be done at train level to check the correct operation of doors closed and locked safety loop.<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.  | RS subsystem          | 1 | E |
|         |  |  |  | Unexpected operation from train driver   |  | An ergonomic analysis of the cabin shall be realized to prevent driver error (wrong command).  |                       |   |   |
|         |  |  |  | Untimely traction order from Signalling  |  | As same as 4.1.1.3   | Operator Signal       | 1 | F |
|         |  |  |  | Untimely traction order from Train control   |  | As same as 4.1.1.3   | Operator Signal       | 1 | F |
|         |  |  |  | Untimely traction during passenger exchange  |  | As same as 4.1.1.3   | RS subsystem Operator | 1 | F |
|         |  |  |  | Inefficient train immobilization during passengers exchange                                    |  | "A calculation note shall be done to confirm that holding brake is designed to reach the following performances:<br>- under EL8 with one car isolated and in slope of 4%, the train shall not move.<br><br>The calculation note shall also determine how many actuator failures are acceptable to respect the degraded performance."<br>A validation test shall be performed to confirm the holding brake performances (in degraded mode).<br>The loss of Holding brake command / untimely traction authorization from Signalling to train shall have a failure rate lower or equal to $1 \times 10^{-7}$ failure per hour.<br>The untimely Traction Enabled authorization from train to traction shall have a failure rate lower or equal to $1 \times 10^{-8}$ failure per hour.<br>The failures of holding brake control equipment causing the movement of the train shall have a failure rate lower or equal to $1 \times 10^{-7}$ failure per hour.<br>The failures of bogie brake equipment causing the movement of the train while in holding brake shall have a failure rate lower or equal to $1 \times 10^{-7}$ failure per hour.<br>"Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to $1 \times 10^{-9}$ failure per hour."<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake. | RS subsystem          | 1 | F |
| 4.2.1.3 |  |  | Break of a fixed part of a vehicle                       | Break of a fixed part of a vehicle   |  | As same as 4.2.1.1   | Maintenance           | 1 | F |

|         |                      |   |   |   |  |  |                       |   |   |
|---------|----------------------|---|---|---|--|--|-----------------------|---|---|
| 4.2.1.4 |                      |   | Unexpected operation of the vehicle doors | Door opening on the wrong side at station, commanded by Signalling    |  | Untimely door enable command provided by Signalling shall have a failure rate lower or equal to $3 \times 10^{-8}$ failure per hour.<br>Untimely door opening command provided by Signalling via Ethernet shall have a failure rate lower or equal to $1 \times 10^{-5}$ failure per hour.   | Signal                | 1 | E |
|         |                      |   |   | Door opening on the wrong side at station, commanded by Train Control |  | Untimely door enable command provided by train control shall have a failure rate lower or equal to $3 \times 10^{-8}$ failure per hour.<br>Untimely door opening command provided by train control via Ethernet shall have a failure rate lower or equal to $1 \times 10^{-5}$ failure per hour.<br>Door failures leading to electrical supply of doors enable trainline shall have a failure rate lower or equal to $1 \times 10^{-9}$ failure per hour per door.   | RS subsystem          | 1 | E |
|         |                      |   |   | Door opening on the wrong side at station                             |  | The untimely opening of a door when train is stopped, with no authorisation from train shall have a failure rate lower or equal to $1 \times 10^{-9}$ failure per hour.  | RS subsystem Operator | 1 | F |
|         |                      |   |   | Manual door opening (EED) allowed on the wrong side at station        |  | Warning shall be set to inform passenger about their responsibility and possible prosecution while using the Emergency Egress Device.<br>In case of door opening on the opposite side of platform, Driver shall inform OCC that evacuation is on-going.<br>In case of door opening on the opposite side of platform, trains in the area shall be stopped in Safety brake, and traction power supply shall be cut off by OCC.<br>Emergency Egress Device shall either include a cover or have a design that prevent the handle of Emergency Egress Device from accidental operation.  | RS subsystem Operator | 1 | F |
| 4.2.2.1 |                      | Interface between vehicle and walkway during evacuation                       | Inadequate vehicle / walkway interfacing  | Too large gap between the vehicle and the walkway                     |  | A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).<br>A validation test shall be done to check train compliance to static and dynamic gauges.<br>Infrastructures shall be compliant with specified gauge in ICD<br>Train System shall prevent the access to gangway area to passengers.   | RS subsystem          | 1 | F |
|         |                      |   |   | Too large height difference between the train floor and the walkway   |  | A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).<br>A validation test shall be done to check train compliance to static and dynamic gauges.<br>Infrastructures shall be compliant with specified gauge in ICD<br>Train System shall prevent the access to gangway area to passengers.   | RS subsystem          | 1 | F |
| 4.2.3.1 |                      | Train movement during the evacuation  | Unexpected train motion                   |   |  | As same as 4.1.2.2   | RS subsystem          | 1 | F |
| 4.2.4.1 |                      | Opening or breach in the vehicle when a train is stopped between two stations | Unexpected operation of the vehicle doors | Unexpected operation from train driver                                |  | Door closing shall be announced by visual signal and audio signal to passengers.<br>A validation test shall be done to validated visual signal and audio signal to passengers during doors closing sequence.<br>A validation test shall be done to validated that door is not be able to reach closed and locked position if an obstacle of $40 \times 60$ mm (according to EN14752) is present.<br>The non detection of obstacle by door sensitive edge shall have a failure rate lower or equal to $2 \times 10^{-7}$ failure per hour per door.<br>A validation test shall be done to validated that door closing force is limited according to EN14752.<br>The door obstacle detection shall have a failure rate lower or equal to $1 \times 10^{-7}$ failure per hour per door. | RS subsystem          | 1 | E |
|         |                      |   |   | Opening command from a passenger                                      |  | As same as 4.2.1.4   | RS subsystem          | 1 | F |
|         |                      |   |   | Non detection of the opening of one or more doors                     |  | As same as 4.2.1.2   | RS subsystem          | 1 | F |
| 4.2.4.2 |                      |   | Break of a fixed part of a vehicle        | Break of a fixed part of a vehicle                                    |  | As same as 4.2.1.1   | RS subsystem          | 2 | F |
| 4.3.1.1 | FALL BETWEEN VEHICLE | Lack of balance during  | Bad train positioning                     | Failure of the suspension   |  | Bogie's secondary suspension shall have lateral dampers to limit lateral jerk sustained by passengers.<br>A validation test shall be done to define train riding comfort on the main line.<br>A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).  | RS subsystem          | 1 | F |



|          |   |                              |   |   |  |  |              |   |   |
|----------|---|------------------------------|---|---|--|--|--------------|---|---|
|          | AND PLATFORM                                  | passengers' exchange         |   |   |  |  |              |   |   |
|          |   |                              |   | Unsteady load of the vehicle not absorbed by train suspensions              |  | A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).<br>A validation test shall be done to check train compliance to static and dynamic gauges.   | RS subsystem | 1 | F |
|          |   |                              |   | Wrong calculation of the gauge  |  | A calculation note shall be done to demonstrate that the static and dynamic gauges are compliant with contractual requirement, even in worst conditions (suspensions failures, wind, track cant).<br>A validation test shall be done to check train compliance to static and dynamic gauges.   | RS subsystem | 1 | F |
|          |   |                              |   | Flat wheel  |  | A fatigue calculation note shall be done to validate wheel design.<br>Wheels shall comply to EN 13262<br>Brake's wheel slide protection function shall also ensure a axle blocked detection function.<br>Wheel profile shall comply with NFF-03-402.<br>Non respect of safety brake performances, including failures of load compensation and wheel slide protection, shall not have a failure rate lower or equal to 1 x 10-9 failure per hour.   | RS subsystem | 1 | F |
|          |   |                              |   | Inefficient service braking   |  | "Signalling shall protect the train against overspeed, reverse movement, undemanded movement, train departure with opened door and signal trespassing by activating a safety brake.<br>Failure rate of safety brake command from Signalling shall be lower or equal to 1 x 10-9 failure per hour. "<br>Whatever the driving mode, in case of overspeed, reverse movement, undemanded movement, departure with opened door, obstacle on the track or signal trespassing, driver shall apply a safety brake.<br>Signalling shall ensure that there is always adequate safety distance between two RSK in operation to prevent collision in case of Safety Brake (assuming the minimum guaranteed deceleration rate)  | RS subsystem | 1 | F |
|          |   |                              |   | Train driver error  |  | To facilitate evacuation, train shall be stopped in a straight line and not in a curve.  | Operator     | 1 | F |
| 4.3.1.2  |   |                              | Unexpected train motion                       |   |  | As same as 4.1.2.2   | RS subsystem | 1 | F |
|          |   | Lack of balance in the depot | Staff injury while boarding / alighting train | Too large gap between the vehicle and the walkway                           |  | As same as 4.2.2.1   | RS subsystem | 3 | F |
|          |   |                              |   | Too large height difference between the train floor and the walkway         |  | As same as 4.2.2.1   | RS subsystem | 3 | F |
| <b>5</b> | <b>FIRE AND EXPLOSION / LEAKAGE</b>           |                              |   |   |  |  |              |   |   |
| 5.1.1.1  | STAFF OR PASSENGER NEAR PRESSURISED EQUIPMENT | On the train                 | Inadequate design                             | Inadequate design / settings of pressure regulation                         |  | "Each air production units shall be equipped with a safety valve triggering if the pressure in the main pipe is higher than 10 bars.<br>Failure rate of the safety valve preventing air pressure reduction shall be lower than 5 x 10-7 failure per hour per safety valve."<br>A validation test shall be done on Air production units to ensures safety valves trigger when pressure is higher than 10 bars.<br>"Each Heating, Ventilation and Air Conditionning unit shall be equipped with safety valves triggering in case of over-pressure and releasing pressure.<br>Explosion of pressurized circuit shall have a failure rate lower or equal to 1 x 10-9 failure per hour per pressurized circuit."<br>A validation test shall be done on Heating, Ventilation and Air Conditionning units to ensures safety valves trigger when pressure is too high. | RS subsystem | 1 | E |
|          |   |                              |   | Inadequate design of tanks  |  | Each Air production tank shall be designed to handle a pressure of 11 bars.<br>A validation test shall be done on Air production tanks to ensure they can handle a pressure of 11 bars.<br>HVAC units shall integrate a system to retain liquid leakage, like a bath system.   | RS subsystem | 1 | E |
|          |   |                              |   | Inadequate design of the installation related to the rechargeable batteries |  | "Vicinity of batteries shall be kept clear from any ignition source :<br>- open flames or fire,<br>- smoke,<br>- glowing embers,<br>- flying sparks while doing grinding work,<br>- electrical sparks caused by switches or fuses,<br>- hot surfaces with temperature above 300°C,<br>- electrostatic discharges.<br>Work shall be done with electrically insulated tools that do not strike sparks. "   | RS subsystem | 1 | F |

|         |   |              |                                     |   |  |  |                             |   |   |
|---------|---|--------------|-------------------------------------|---|--|--|-----------------------------|---|---|
|         |   |              |                                     |   |  | A calculation shall be done to dimension the battery box events to evacuate the hydrogen produced during operation. Safety Warning shall be applied on battery box to inform maintenance staff about risks of explosive atmosphere, electrocution, corrosive liquid and hot surfaces.<br>The size of battery case events shall comply with the results of dimensioning calculation.  |                             |   |   |
| 5.1.1.2 |   |              | Inadequate maintenance intervention | Safety Brake isolation done only by switch inside saloon area |  | Prior any brake system maintenance intervention, the main pipe shall be at atmospheric pressure and air production unit operation isolated (LOTO procedure applies)  | Maintenance                 | 2 | E |
| 5.2.1.1 | STAFF OR PASSENGER NEAR EXPLOSIVE MATERIALS | On the train | Presence of explosive materials     | Use of explosive substances (liquids, solids...)              |  | Train shall comply with EN 45545.  | RS subsystem                | 1 | F |
|         |   |              |                                     | Battery failure, including regulation                         |  | "Vicinity of batteries shall be kept clear from any ignition source :<br>- open flames or fire,<br>- smoke,<br>- glowing embers,<br>- flying sparks while doing grinding work,<br>- electrical sparks caused by switches or fuses,<br>- hot surfaces with temperature above 300°C,<br>- electrostatic discharges.<br>Work shall be done with electrically insulated tools that do not strike sparks."<br>A calculation shall be done to dimension the battery box events to evacuate the hydrogen produced in operation. The size of battery case events shall comply with the results of dimensioning calculation.<br>Batteries shall be equipped with heating sensor.<br>Safety Warning shall be applied on battery box to inform maintenance staff about risks of explosive atmosphere, electrocution, corrosive liquid and hot surfaces.<br>If the temperature value provided by battery is out of range, the battery charging shall be stopped. | RS subsystem<br>Maintenance | 1 | F |
| 5.2.1.2 |   |              | Presence of explosive materials     | Power capacitor failure, including regulation                 |  | Traction supplier shall demonstrate using qualitative or quantitative analysis that explosion risk of power capacitors, HSCB and IES are negligible.<br>Auxiliary converter supplier shall demonstrate using qualitative or quantitative analysis that explosion risk of power capacitors is negligible.   | RS subsystem                | 1 | F |
| 5.3.1.1 | FIRE  | On the train | Fire ignition inside the train      | Design using highly flammable materials                       |  | Train shall comply with EN 45545.  | RS subsystem                | 2 | F |
|         |   |              |                                     | Overheating of electromechanical devices                      |  | Train shall comply with EN 45545.<br>Surge arrester shall comply with IEC 61287-1.<br>The train shall comply with the requirements of EN 50153 regarding protective provision relating to electrical hazards<br>Each door shall be equipped with an Emergency Egress Device to allow evacuation.<br>Ventilation shall be automatically stopped in the saloon areas where smoke is detected.<br>Power supply shall be automatically stopped in the underframe areas where fire is detected.   |                             |   |   |
|         |   |              |                                     | Short circuit leading to conductors or connections ignition   |  | As the same as Overheating of electromechanical devices  | RS subsystem                | 2 | F |
|         |   |              |                                     | Ignition of accumulated dust, waste or filters                |  | Heaters activation shall be prevented in case of loss of ventilation.<br>Heaters shall be protected by thermal breaker to prevent excessive heating.<br>HVAC unit shall be equipped with air filters.<br>Appropriate maintenance of the train filters shall be done regularly to limit the accumulation of waste liable to ignite (fire risk).   | RS subsystem                | 2 | F |
|         |   |              |                                     | Incorrect maintenance operation (loose connections...)        |  | Maintainer shall respect the Maintenance Plan and Maintenance procedures.<br>After revenue service, maintenance shall repair each train that displays incorrect operation status before next mission.<br>Driver shall start the operation only if no incorrect operation status is indicated on the driver display unit.<br>Maintenance staff shall be trained to intervene on Hanoi Line 3 train.<br>United Joint Venture (UJV) shall train maintenance staff to intervene on Hanoi Line 3 train.   | Maintenance<br>Operators    | 2 | F |
| 5.3.1.2 |   |              | Fire ignition outside the           | Design using highly flammable materials                       |  | As same as 5.3.1.1   | RS subsystem                | 2 | F |

|         |  |                     |                       |  |  |   |              |   |   |
|---------|--|---------------------|-----------------------|--|--|---|--------------|---|---|
|         |  |                     | passenger compartment |  |  |   |              |   |   |
|         |  |                     |                       | Overheating of electromechanical devices                             |  | As same as 5.3.1.1  | RS subsystem | 2 | F |
|         |  |                     |                       | Short circuit leading to conductors or connections ignition          |  | As same as 5.3.1.1  | RS subsystem | 2 | F |
|         |  |                     |                       | Ignition of accumulated dust, waste or filters                       |  | As same as 5.3.1.1  | RS subsystem | 2 | F |
|         |  |                     |                       | Axle blocking or permanent mechanical braking in case of tire wheels |  | As same as 2.1.1.3  | RS subsystem | 2 | F |
| 5.3.2.1 |  | Fire in the station | Propagation of fire   | Train entrance in a fire area not prohibited or late prohibited      |  | In case of smoke or fire detection outside the train, the operator/OCC shall<br>Not allow a train to enter in a fire or smoked area<br>Evacuate all trains to safe area (away of smoke) | Operator     | 3 | F |
|         |  |                     |                       | Inadequate smoke exhaust means, the smoke penetrating another train  |  | In case of smoke or fire detection outside the train, the fresh air dampers of ventilation shall be closed to avoid the entrance of smoke inside the train                              | Operator     | 3 | F |

## Appendix 3: Checklist of Railway Vehicle Mobilisation

### VEHICLE PRE-MOBILISATION CHECKLIST

#### 1. Vehicle Information

Registration No.

Date of Service

Hours/Km operated

Next Service due (Hours/Km)

#### 2. Minimum Requirements for Vehicle (Yes/No)

- Interlocking system to ensure that only one wheelset can be raised or lowered at any time for friction drive and hydrostatic systems.
- Park brake system fails safe and able to hold a minimum 1/30 grade.
- Fire extinguisher minimum 4.5kg, tested and tagged within 6 months.
- Flashing amber beacon visible from front and rear of vehicle.
- Emergency stop (with decal) – inside or outside machine as appropriate
- Guarding (lockable door and/or limit switch and/or guarding over parts).
- Safety signage in place for pinch points, warnings, overhead wires etc.
- Are service brakes fail safe and/or backed up with secondary brake
- Braking capability on all four wheels that are in contact with rail.
- Does the emergency off tracking system have interlocking to both front and rear protection from being operated at the same time to prevent a runaway?
- Applicable signage in cabin to inform operator of the height of the rolling stock in travel mode and; the maximum allowable speed on track (forward and reverse).
- Horn appropriate for the working conditions (i.e. loud enough to be heard out on the track or other working area)
- The controls for the engagement of the rolling stock are operated from the cabin.
- Vehicle module ID plate fitted to front and rear hi-rail.
- Reversing Camera (colour) fitted (where the operator does not have a direct vision behind the vehicle)

#### 3. Condition of Vehicle and Equipment (Yes/No)

- The general cleanliness of the property, both inside and outside, is satisfactory.
- Damage-free.
- Visible oil / water leaks are not present.
- Hydraulic and fuel system hoses and fittings should be inspected for wear or damage.
- Assess the serviceability and proper operation of all brakes, tyres, rail wheels, drive spigots, interlocks, sensors, alarms, and indicators.

#### 4. Compliance documentation (Yes/No)

- Operators Manual is specific published for vehicles and available in the driver cabins.
- Risk assessment: Part of Railway vehicle are established and specific updated based on real-time working conditions.
- A pre-start book is supplied for the vehicle, which includes crucial rail components.
- Rolling stock registration sticker, certificate or equivalent for the urban railway.
- Log of maintenance (minimum of 3 months records).
- Annual inspection report for railway vehicles.
- If necessary, change management documentation are provided for any revisions.
- Wheel checks are performed every 500 hours or six months, whichever occurs first.

#### 5. Comments and declarations

Notes on minimum requirements exceptions; list additional included asset or serial numbers; any further information.

Declares that this machine is in a safe condition, is free from defect and is fit for purpose.

Signature of assessors.

### Pre-START CHECKLIST (for vehicle checking)

#### 1. Vehicle Information

Registration No.

Date of Service

Hours/Km operated

Next Service due (Hours/Km)

#### 2. Vehicle Checklist prior to operating on site

- Check if any existing damage (list in comments if any damage found)

- Free of visible oil leaks and excess grease. Check hydraulic system hoses and fittings for deterioration, wear or damage.
- Fire extinguisher in date.
- Rail network registration in date.
- Pre-start book.
- Operators Manual is available in the driver cabins.
- Risk assessment: Part of Railway vehicle present with machine.
- Maintenance records in cab or available.

### 3. Comments and declarations

Notes on minimum requirements exceptions; list additional included asset or serial numbers; any further information.

Declares that this machine is in a safe condition, is free from defect and is fit for purpose.

Signature of assessors.

### Pre-WORK BRIEFING CHECKLIST (for staffs/workers)

#### 1. Working site detail

|                    |                              |                   |
|--------------------|------------------------------|-------------------|
| Scope of Work      | Responsible staff            |                   |
| Date of Work       | Location                     | First aid locaton |
| Weather conditions | Emergency controller/contact |                   |

#### 2. Hazard identification of working task (Yes/No)

- Is everyone qualified to perform the responsibilities assigned?
- Are all employees wearing in very visible clothing?
- Is there a secure area on the workplace?
- Is communication with other workgroups required?
- Have any environmental effects been identified?
- Is the work going to have an impact on track circuits, turnouts, points, or signals?

#### 3. Does this task involve High-risk work? (Yes/No)

- Working in the surroundings of a mobile vehicle
- Restricted Areas
- Utilization of a lifting device
- Conducting work on or near electrified electrical systems
- Working at a high position.
- Work on or beside opearating railroad
- Hazardous Substances

#### 4. Description of hazard controls

- List of identified hazards
- Determine the corresponding solutions to control hazards.

#### 5. Verification and Declaration

I am free of the effects of alcohol and/or drugs. I am free from the effects of fatigue or illness and fit for work. I have informed the supervisor of the worksite of any prescription or non-prescription drugs that may impair my ability to execute job activities safely.

I have had the opportunity to identify new hazards and question the safety controls. I am aware of my responsibilities and obligations regarding the implementation of nominated controls.

I have been given the relevant work task programme and the site's Worksite Protection procedures.

I have received training in or have the knowledge of the Safe Work Method Statements.

## Appendix 5: Typical accident reaction plans

### Procedure for the accident of People falling on track

General response procedures and departmental responsibilities have been provided in section 7.3. The contents of this appendix provide site-specific operating instructions in the event of an accident

#### Station

- On the contact rail line, if the station detects the following situations, the first time to press the emergency stop button (PEP) and the emergency power off button (EPB) in the respective area:
  - Detect or receive a report of someone climbing through the security gate into the track area (including the station A/B driver station).
  - When detecting or receiving reports of people (including passengers or staff) entering or mistakenly entering the track area.
  - Other emergencies approved by OCC.
- Outage extent at contact rail power supply route or EPB emergency switch off
  - When pressing the EPB emergency power-off button, the power-off button should be pressed in the corresponding area.
  - If entering the railway station area illegally, causing the employee's position to change (entering a different power supply area), you must continue to press the next corresponding zone power-off button.
  - If an employee enters illegally at the same time as the train is going up and down, the power switch must be pressed with the corresponding up and down route.
- Detecting people entering the station track area illegally, Press the PEP emergency train stop button (press the EPB emergency power off button at the same time as the contact rail power supply line), immediately take advice to unauthorised persons, and report to the station operator, the police and try to get through the safe area to guide them back to the platform.
- If an unauthorised person becomes trapped on ancillary equipment of the platform (such as structural steel railings and station roof) and has a tendency to commit suicide, immediately notify the police and actively cooperate with external units such as fire protection, police to solve the case.
- Politely prevent passengers from taking photos, evacuate onlookers, and establish effective isolation areas.
  - Establish a field command in the appropriate area of the platform and report it to the train dispatcher;
  - At first, the field commander should actively discuss with the OCC leader and conduct an assessment of the events;
  - The station will take measures to control passenger traffic and evacuate customers at the platform when incidents occur.
- In case people stay inside the steel structure protection fence outside the station rail area or climb onto the station roof:
  - Arrange staff to closely monitor employees who illegally enter the track area;
  - Carry out safety monitoring of the route to maintain operation;
  - If there is contact on the railway line, when there are people on the station, according to the orders of the power dispatcher and train dispatcher, the station will restore the power. Trains have a speed limit of 10km/h when entering the station, when an abnormal situation occurs, immediately press the emergency stop button and the emergency power off button.
- According to OCC, organising trains in the emergency stop area:
  - Immediately do a good job of preparing the corresponding instructions;
  - When performing an evacuation in the area, hurry to the scene to assist the train driver in guiding the evacuation of passengers;
  - Arrange staff to guide personnel in potentially hazardous areas such as : where people fall or fall in rail areas and rail lifts, as well as beware of secondary incidents.
- When an incident (electric shock) occurs to people entering the track area
  - When electric shock occurs, on the contact rail power supply route must immediately stop the contact rail power supply in the corresponding area;
  - Report to the OCC, the police and the hospital, do well in the prevention of the incident scene, and cooperate with the police to investigate, collect evidence and rescue personnel;
  - After the event is finished processing, clean up the route so that operations can resume as soon as possible.

#### Train driver

- When a train driver entering the station has an incident, when he detects that there are people entering or stuck in the platform rail area, he must:
  - Immediately press the emergency train stop button;
  - Notify train dispatchers;
  - Do a good job of reassuring passengers.

- When a train receives information from the station train dispatcher about unauthorised entry, it must:
  - Listen to and obey the instructions of the train dispatcher;
  - When stopping the train in the area, must do a good job of reassuring passengers (on the contact rail power supply route, the train loses power on the contact rail must start the emergency power source), pay attention to check see if any passengers unlock the door and promptly notify OCC of the situation on the scene;
  - If the passengers on the train are agitated, and criticise or make it difficult for the driver, the driver must keep calm, do a good job of explaining and especially strengthen the reassurance and guide the passengers.
- If the train stops for a long time, pay attention to check the train's condition (status of using the reserve battery power of the train, the air volume of the wind cylinder, check if the train door is open) airlock, etc.), promptly report the status to the station dispatcher and comply with the train dispatcher's instructions.
- In the process of carrying out an area evacuation, the train driver must in principle apply the only door unlock method to unlock the first passenger door of the station near the direction of evacuation through the track area to organise evacuation and strengthen guidance work.
- After the incident, the train driver must promptly notify the main line staff to quickly go to the nearest station to assist the drivers of the affected train to do well in the service. customer care and security card control.
- When the driver of the train at the stopped area is required to carry out the order to reverse, in principle, the train driver will reverse with the towing vehicle.

#### **Dispatching centre**

- After receiving the report, the first time to confirm the area where the incident occurred is to press the emergency train stop button (confirm whether the emergency power off button is pressed at the next rail feed line) air contact) and check the condition of trains in the affected area.
- Maintain close communication with the field command, capture the entire situation at the scene and make decisions to adjust train operation;
  - Maintain to the maximum extent the normal operation of trains in the affected area in a safe state, (without interruption of operation) and organise the operation of small traffic when appropriate;
  - Organise the adjustment of train operations in the unaffected area.
- For train organisation during the forced stop period, based on the station's field situation, the passenger status of the train in the forced stop area, the train stop position and other factors, to flexibly apply the following measures and notify relevant units:
  - When the conditions for reversing the train are satisfied, and safety protection measures are well taken, OCC will organise for trains in the stopping area to return to the station to evacuate passengers;
  - When the train part cabin is forced to stop at the station, all passengers must be evacuated at the station;
  - When the train in the area is forced to stop can not move forward or backward, when the train is stopped and must stop for more than 15 minutes, please notify the relevant units to do well to prepare for the evacuation of passengers. When the mandatory stoppage period exceeds 20 minutes, immediately announce the evacuation of area passengers. When the convoy in the area of the mandatory stop is expected to exceed 20 minutes, immediately notify the evacuation of area passengers.
  - In case of inclement weather, in principle, passengers will not be evacuated in the forced evacuation stopping area due to staff entering the station tracks illegally. The station will try to organise the train back to the station for processing.

## Appendix 4: Example of Inspection plan

### Monthly Inspection plan

|           | May |     |     |     |     |     |   |   |     |     |     |     |     |    |    |     |     |     |     |     |     |    |     |     |     |     |     |     |    |     |    |     |   |
|-----------|-----|-----|-----|-----|-----|-----|---|---|-----|-----|-----|-----|-----|----|----|-----|-----|-----|-----|-----|-----|----|-----|-----|-----|-----|-----|-----|----|-----|----|-----|---|
|           | 1   | 2   | 3   | 4   | 5   | 6   | 7 | 8 | 9   | 10  | 11  | 12  | 13  | 14 | 15 | 16  | 17  | 18  | 19  | 20  | 21  | 22 | 23  | 24  | 25  | 26  | 27  | 28  | 29 | 30  | 31 |     |   |
| Train No. | S   | M   | T   | W   | T   | F   | S | S | M   | T   | W   | T   | F   | S  | S  | M   | T   | W   | T   | F   | S   | S  | M   | T   | W   | T   | F   | S   | S  | M   | T  |     |   |
| 1         |     |     |     |     |     |     |   |   |     |     |     |     |     |    |    |     |     |     |     |     |     |    |     |     |     |     |     |     |    |     |    |     |   |
| 2         | A   | (M) | A   | A   | K   | A   | K | A | (L) | A   | A   | A   | A   |    | A  | A   | (M) | A   | A   | A   | A   |    | A   | (L) | A   | A   | A   | A   | A  | A   | A  | A   |   |
| 3         | B   | A   | B   | B   | B   | K   |   |   | (M) | B   | B   | B   | B   | M  | B  | (L) | A   | B   | B   | B   | B   | A  | K   | (M) | B   | A   | B   | B   | B  | B   | B  | (L) | A |
| 4         |     |     |     |     |     |     | A | B | A   | C   | C   | C   | C   | L  | M  | (M) | B   | C   | C   | C   | C   | B  | (L) | K   | C   | C   | C   | C   | C  | C   | C  | (M) |   |
| 5         | C   | (L) | C   | C   | C   | B   | L | C |     |     |     |     |     | A  | C  | B   | C   | D   | K   | D   | D   | C  | (M) | A   | D   | D   | D   | L   |    | (L) | B  |     |   |
| 6         | D   | B   | (M) | D   | D   | C   | E | M | B   | (M) | D   | D   | D   | K  | L  |     |     |     |     |     | e   | D  | B   | B   | E   | E   | E   | M   | D  | (M) | C  |     |   |
| 7         | E   | C   | (L) | E   | E   | D   | B | E | K   | (L) | E   | E   | E   | B  | E  | C   | (L) | K   | D   | E   | F   | E  |     |     |     |     |     |     |    | E   | D  | D   |   |
| 8         | F   | D   | D   | (M) | F   | E   | C | F | C   | K   | (M) | F   | F   | C  | F  | D   | K   | (M) | E   | F   | G   | F  | C   | C   | (M) | F   | K   | D   | F  |     |    |     |   |
| 9         | G   | E   | E   | (L) | G   | F   | D | L | D   | D   | (L) | G   | G   | D  | G  | K   | D   | (L) | F   | G   | H   | G  | D   | D   | (L) | K   | F   | E   | G  | E   | E  |     |   |
| 10        | H   | F   | F   | F   | (M) | G   | M | G | E   | E   | F   | (M) | H   | E  |    | E   | E   | E   | (M) | H   | L   | H  | E   | E   | K   | (M) | G   | F   | H  | F   | F  |     |   |
| 11        | K   | G   | G   | K   | (L) | H   | F | H | F   | F   | G   | (L) | K   | F  | L  | F   | F   | F   | (L) | K   | K   | M  | F   | F   | F   | (L) | H   | G   | M  | G   | K  |     |   |
| 12        | L   | H   | K   | G   | H   | (M) | G | D | G   | G   | H   | K   | (M) | G  | d  | G   | H   | G   | G   | G   | (M) | M  | L   | G   | G   | G   | G   | (M) | H  | L   | K  | G   |   |
| 13        | M   | K   | H   | H   | A   | (L) | H | K | H   | H   | K   | H   | (L) | H  | H  | H   | H   | H   | H   | (M) |     | K  | H   | H   | H   | H   | (L) | K   | K  | H   | H  |     |   |

Kinds of maintenance

5-year inspection

3-month inspection

( ) 10-day inspection

Creaning

Wheel grinding

### Daily Inspection Plan

|                 |        |
|-----------------|--------|
| Date            | 02/May |
| Day of the week | Mon    |

| operation No.<br>(11) | train No. | departure<br>track No. | departure<br>time | temp-<br>arrival<br>track No. | temp-<br>arrival<br>time | re-<br>departure<br>track No. | re-<br>departure<br>time | final<br>arrival<br>track No. | final<br>arrival<br>time |
|-----------------------|-----------|------------------------|-------------------|-------------------------------|--------------------------|-------------------------------|--------------------------|-------------------------------|--------------------------|
| A                     | 03        | #01                    | 5:00              | -                             | -                        | -                             | -                        | #01                           | 21:00                    |
| B                     | 06        | #02                    | 5:10              | -                             | -                        | -                             | -                        | #02                           | 21:15                    |
| C                     | 07        | #03                    | 5:20              | -                             | -                        | -                             | -                        | #03                           | 21:30                    |
| D                     | 08        | #04                    | 5:30              | -                             | -                        | -                             | -                        | #04                           | 21:45                    |
| E                     | 09        | #05                    | 5:40              | -                             | -                        | -                             | -                        | #05                           | 22:00                    |
| F                     | 10        | #06                    | 5:50              | -                             | -                        | -                             | -                        | #06                           | 22:15                    |
| G                     | 11        | #07                    | 6:00              | -                             | -                        | -                             | -                        | #07                           | 22:30                    |
| H                     | 12        | #08                    | 6:10              | -                             | -                        | -                             | -                        | #25                           | 22:45                    |
| K                     | 13        | #09                    | 6:40              | #25                           | 10:00                    | #25                           | 16:00                    | #08                           | 23:30                    |
| L                     | 05        | #10                    | 7:00              | #21                           | 9:45                     | #21                           | 16:15                    | #09                           | 23:50                    |
| M                     | 02        | #11                    | 7:10              | #22                           | 9:30                     | #22                           | 17:00                    | #10                           | 23:40                    |

| under inspection | train No. |
|------------------|-----------|
| 8-year           | -         |
| 4-year           | 01        |
| 3-month          | 04        |
| 10-days          | 02, 05    |
| cleaning         | 13        |
| wheel grinding   | -         |



## Daily staff arrangements

| Date            |            |                    |
|-----------------|------------|--------------------|
| Day of the week |            |                    |
| Day-time shift  |            |                    |
| Position        | Staff Name | Today's assignment |
| Head of IY      |            |                    |
| Supervisor      |            |                    |
|                 |            |                    |
|                 |            |                    |
|                 |            |                    |
| Sub Supervisor  |            |                    |
|                 |            |                    |
|                 |            |                    |
|                 |            |                    |
| Staff           |            |                    |
|                 |            |                    |
|                 |            |                    |
|                 |            |                    |
|                 |            |                    |
|                 |            |                    |
|                 |            |                    |
|                 |            |                    |

## All-day shift

| All-day shift                         |                |            |                    |
|---------------------------------------|----------------|------------|--------------------|
| Group A                               | Position       | Staff name | Today's assignment |
| Responsible for the day               | Supervisor     |            |                    |
| Driving and daily inspection          | Sub Supervisor |            |                    |
| Dealing with failure during operation | Sub Supervisor |            |                    |
| Driving                               | Staff          |            |                    |
|                                       | Staff          |            |                    |
|                                       | Staff          |            |                    |
|                                       | Staff          |            |                    |
| Daily&other maintenance               | staff          |            |                    |
|                                       | staff          |            |                    |
| Group B                               | Position       | Staff name | Today's assignment |
| Responsible for the day               | Supervisor     |            |                    |
| Driving and daily inspection          | Sub Supervisor |            |                    |
| Dealing with failure during operation | Sub Supervisor |            |                    |
| Driving                               | Staff          |            |                    |
|                                       | Staff          |            |                    |
|                                       | Staff          |            |                    |
|                                       | Staff          |            |                    |
| Daily&other maintenance               | staff          |            |                    |
|                                       | staff          |            |                    |
| Group C                               | Position       | Staff name | Today's assignment |
| Responsible for the day               | Supervisor     |            |                    |
| Driving and daily inspection          | Sub Supervisor |            |                    |
| Dealing with failure during operation | Sub Supervisor |            |                    |
| Driving                               | Staff          |            |                    |
|                                       | Staff          |            |                    |
|                                       | Staff          |            |                    |
|                                       | Staff          |            |                    |
| Daily&other maintenance               | staff          |            |                    |
|                                       | staff          |            |                    |
| Group D                               | Position       | Staff name | Today's assignment |
| Responsible for the day               | Supervisor     |            |                    |
| Driving and daily inspection          | Sub Supervisor |            |                    |
| Dealing with failure during operation | Sub Supervisor |            |                    |
| Driving                               | Staff          |            |                    |
|                                       | Staff          |            |                    |
|                                       | Staff          |            |                    |
|                                       | Staff          |            |                    |
| Daily&other maintenance               | staff          |            |                    |
|                                       | staff          |            |                    |

## Form of Situation report

## Situation Report

|  |  |  |                         |                      |          |                      |                  |                  |          |
|--|--|--|-------------------------|----------------------|----------|----------------------|------------------|------------------|----------|
| 1. Creation Date                                   | Year:                                    |  | Month:                  |                      | Date:    |                      |                  |                  |          |
| 2. Document No.                                    |  |  |                         |                      |          |                      |                  |                  |          |
| 3. Work place name                                 |  |  |                         |                      |          |                      |                  |                  |          |
| 4. Type  | A  | 1. failure 2. accident 3. disaster 4. other      |                         |                      |          |                      |                  |                  |          |
|  | B  | 1. rolling stock 2. facility 3. driving 4. other |                         |                      |          |                      |                  |                  |          |
| 5. Date and time of occurrence                     | Year:                                    |  | Month:                  |                      | Date:    |                      | Day of the week: |                  | Weather: |
| 6. Place of occurrence                             | Line:                                    |  |                         | –                    | Line:    |                      |                  | Time             |          |
|  | Station:                                 |  |                         |                      | Station: |                      |                  |                  |          |
| 7. Operation No.                                   | No.:                                     |  | Line:                   |                      | –        | Line:                |                  |                  |          |
|  | Train set:                               |  |                         | Starting station:    |          | Destination station: |                  |                  |          |
| 8. Train No.                                       |  |  |                         |                      |          |                      |                  |                  |          |
| 9. Delay time                                      | Delay: (min)                             |  | Stop operation:         |                      | –        |                      | Number:          |                  |          |
|  |  |  | Deadhead train:         |                      | –        |                      | Number:          |                  |          |
| 10. Specific date information of the train         | Start operation                          | Recent improvement                               |                         | Workshop improvement |          | Monthly inspection   |                  | Daily inspection |          |
|  |  |  |                         |                      |          |                      |                  |                  |          |
| 11. Occurance situation                            |  |  |                         |                      |          |                      |                  |                  |          |
| 12. Contents of investigation                      |  |  |                         |                      |          |                      |                  |                  |          |
| 13. Treatment for the time being                   |  |  |                         |                      |          |                      |                  |                  |          |
| 14. Cause and analysis                             |  |  |                         |                      |          |                      |                  |                  |          |
| 15. Measures to prevent recurrence                 | Preventive measures against recurrences: |  |                         |                      |          |                      |                  |                  |          |
|  | Confirmation method of the effect:       |  |                         |                      |          |                      |                  |                  |          |
|  | Date of effect confirmation:             |  |                         |                      |          |                      |                  |                  |          |
| 16. Application of same measures to similar trains | Necessity: (Y or N)                      |  | Responsible work place: |                      |          | Performed date:      |                  |                  |          |

## Appendix 6: Contents of Internal Assessment and Safety Audit

### **Inspection for Safety Standard compliance.**

#### ***Responsibilities***

Departments/centers are staffed with full-time safety management, with clear safety management responsibilities.

Assign staff to be responsible for safety during all working shifts.

100% staff signs on the Statement of Safety Responsibilities.

100% staff are given a secure card and have a safety handbook.

#### ***Identify and control critical hazard sources***

Staff know the major hazard sources as well as the controls for this location

Develop a complete back-up plan for emergency response to hazard source items large of the company

#### ***Safety signs***

Install indicators, signs or warning signs at the source of danger, emergency exits, etc., without errors, without damage.

#### ***Safety training***

Organise safety training at departmental level.

Study the legal regulations on production safety, the company's safety regulations and charter

Employees in special work positions must have a verified certificate to work.

#### ***Working safety***

Standard working clothes, good working attitude.

Staffs need to have relevant certificates of skill, and must not commit unsafe acts.

Strictly implement the delivery mechanism to determine responsibility when there is an incident.

PPE should be used correctly. If the item is out of date or shows signs of damage, it should be replaced or sent for inspection and repair.

Comply with labor discipline, do not play loudly, do not do things that are not related to work.

It is strictly forbidden to make copies of keys or lend keys of production rooms and equipment in contravention of regulations

For incidents of equipment and facilities that affect safety, it is necessary to promptly implement good isolation or protection.

Working log need to be records, timely confirm and restore fault information.

Check regularly as prescribed to ensure the condition of equipment, facilities and infrastructure.

Timely handling of safety problems.

Clean in equipment room or public area, do not arrange prohibited items.

Fully prepared and ready spare parts and supplies for operation. Fully equipped with rescue equipment and supplies, have records and record the status of inspection and maintenance.

Arrange production safety meeting before working shift.

Developing and perfecting a classification management system for hazardous chemicals, supplies and materials;

Manage the procurement, storage and use of hazardous, hazardous, flammable and corrosive materials and corrosive products in accordance with regulations.

#### ***Construction safety management***

Construction activities must strictly comply with the mechanism of applying for permission to start construction and ask for permission to end construction, regulations on record keeping.

Outsourced personnel entering the construction must have employees of the operation management department at the site.

Employees must wear PPE as required.

Take necessary precautions and protective measures before starting construction

Scaffolding, operating platforms, ladders, etc. used for construction must meet safety requirements

Take proper precautions and safety protection for edge and hole positions.

Materials and components must be stacked neatly and firmly, and when stacking large components, measures must be taken to ensure that the components are stacked firmly.

Take preventive and protective measures for hazardous activities (such as high climbing, ignition, temporary use of electricity, etc.), and approved by the Safety Department.

When the construction activity is over, clean up and clean out of the site.

#### ***Accident responding and rescue.***

A complete backup plan for emergency response.

There is a plan to rehearse at the department level, the rehearsal items are carried out according to the plan.

Rehearsal records are in line with the company's regulations, timely updated.

Actively implement and respond to company-level drill requirements.

Master the work and professional knowledge related to emergency response.

Fully record documents and records of the incident.

**Inspection of fire protection regulations compliance.*****Responsibility and training for fire prevention***

The regulations of fire prevention and fighting responsibility for important production positions is implemented for each employee (warehouse, spare parts room, station control room, AFC room, OCC room, signal, power supplies). Based on the requirements of the operating company, build a volunteer fire prevention team.

Members of the volunteer fire prevention and fighting team master the methods and master the plan of fire prevention and rescue in the first stage.

Status of training and mastering fire prevention knowledge.

***Safety signs and emergency exits.***

Fire safety route and safe evacuation route are not blocked, safe exits are not locked.

The function of the evacuation indicator sign, the emergency light is in good condition.

***Fire protection equipment and facilities***

Periodically check fire extinguishers and fire hydrants.

Fire extinguishers, fire hydrants and tools and equipment of the volunteer fire prevention and fighting team are fully equipped and function well and effectively.

Fire protection equipment and facilities are not defective, inoperative, damaged.

The use of fire and electricity complies with the requirements in the relevant regulations of the company, without violating regulations.

***Status of potential fire remediation as well as the status of taking precautions***

Timely detection of potential fire hazards, develop effective preventive measures, and implement timely remedial actions.

Do not place flammable and explosive materials in the aisles and exits.

Do not violate regulations on the use of large-capacity electrical equipment.

**Inspection of production facilities*****Management documents.***

There are staff in charge of document management at department level.

System equipment, special equipment must have emergency rescue records, record results of rescue practices.

Safety procedures for equipment operation.

Equipment maintenance manual (including maintenance instructions, maintenance of all points, inspection levels).

All specialised divisions have a record of inspecting equipment and correcting potential hazards. All specialised divisions have records and reports of equipment breakdowns, troubleshooting.

The center/team/working shift builds a document system to manage assets and equipment, which must be updated monthly.

Each device sets up a device management card, and timely updates the content of the manageable.

Inspect the equipment as required by the device management record and record it in the test log. For equipment that requires lubrication, keep a lubrication log of the equipment.

In the delivery book, there are delivery and receipt contents about the equipment operating status.

***Safety training***

Personnel operating equipment must successfully complete training and acquire a working certificate.

Must establish a culture of lifelong learning and the purpose of educating all workers, perform regular production education training for operators in their assigned jobs, and keep knowledge current.

***Working site inspection***

The door of the room where important equipment is located must be kept closed.

Important equipment with equipment responsibility tags, usage notes, maintenance personnel and contact phone numbers

Equipment, facilities, tools, accessories (safety valves, pressure gauges, thermometers, water level gauges, oil level gauges) are completely problem-free. The items that come with the machine are complete and properly preserved.

Tool cabinet (box) for equipment maintenance: The tools are neatly lined up, quickly and conveniently placing tools; In the cabinet door (box lid) there is a list of tools in the cabinet, and the number of tools is the same as in the books.

The protective devices, insurance, interlocks, indicator signals, etc. of the machinery and equipment are not defective.

High-speed moving parts that are exposed to the outside such as gears and shafts, drive chains and belts at a height of less than 2m are required to have protective caps.

The device does not have the following phenomena: gas leakage, water overflow, dripping solution, solution leakage.

Equipment is well lubricated and maintained as required. The oil pipe is clear without clogging, the oil door is clearly not dirty. Lubricants are well maintained.

Whether the equipment is operating in a problem or overloaded condition. Operation without abnormal phenomena: Slow running, abnormal noise, abnormal smell, abnormal temperature rise, abnormal vibration, etc.

Tripod bolts and fixings are in good condition, not loose, not cracked. The device hoisting tool is not deformed, not worn, and the cable is not broken.

When carrying out maintenance (repair) of equipment, safety precautions must be taken and followed.

The AC switches, relays and contactors are intact and show no signs of spark burn. The cooling fan works well, the dust net is not clogged.

The wiring in the electrical control cabinet (box) is neatly arranged, the code of the wire is clear, the terminal of the wire is firmly fixed and not loose.

Whether the circuit is aging or not, the wire is overheated or not.

Electrical equipment, switches and sockets must not be installed on flammable materials.

Do not stack combustible materials under the mains switch box and mains power line.

In the warehouse is not allowed to use other equipment, except for fixed lighting equipment. In the warehouse of flammable hazardous materials, it is not allowed to use iodine and incandescent lamps that burn more than 60W, light switches are located outside the warehouse.

The voltage of the lathe's local lamp and the lamp operating in the session should not exceed 36V.

#### ***Special equipment inspection***

The person in charge of the department must take full responsibility for the safety of the department's special equipment.

The department must arrange full-time or part-time staff to manage the safety of special equipment.

Based on the requirements of the company's special equipment management records to make a special equipment logbook, when there is a change, it must be promptly updated, at least once a month.

Design documents: General drawings, drawings of main bearing structures, mechanical transmission diagrams, lubrication instruction diagrams, control principle diagrams of electrical and hydraulic systems (pneumatics)

Product quality certificate (The original is kept at the administrative office, copies t in the departments)

Instructions for use, maintenance and servicing; Documentation and installation technical documents.

Periodically self-check and record results (at least once a month)

Record the status of daily use (Note on the daily check sheet, shift handover schedule)

Record daily maintenance and servicing of safety accessories, safety protection devices, measuring and control devices and related accompanying tools.

Potential safety checks and remediation logs

Incidents and handling logs

Special equipment in the event of an incident and a backup plan for emergency rescue in the event of an incident

Certificate of operation of special equipment (departments must keep a copy)

Registration form for personnel operating special equipment (the table must include the type of work, the validity period), this table must be updated at least once a month.