# Reliability of Multi-Channel IEC 61850 Mission-Critical Substation Communication Networks based on Markov Process Incorporating Linear Dynamical Systems and Calculus Inferences

By

Vonani Clive Mathebula

971147593

A thesis submitted in fulfilment of the requirements for the degree

Of

Doctor of Philosophy in Electrical Engineering

College of Agriculture, Engineering and Science, University of KwaZulu-Natal

Durban, South Africa

UNIVERSITY OF
KWAZULU-NATAL

2021

# Reliability of Multi-Channel IEC 61850 Mission-Critical Substation Communication Networks based on Markov Process Incorporating Linear Dynamical Systems and Calculus Inferences

By

Vonani Clive Mathebula

971147593

A thesis submitted in fulfilment of the requirements for the degree

Of

Doctor of Philosophy in Electrical Engineering

College of Agriculture, Engineering and Science, University of KwaZulu-Natal

Durban, South Africa

April 2021

Vonani Clive Mathebula

_____

Supervisor:

Professor Akshay Kumar Saha

_____

# Reliability of Multi-Channel IEC 61850 Mission-Critical Substation Communication Networks based on Markov Process Incorporating Linear Dynamical Systems and Calculus Inferences

By

Vonani Clive Mathebula

971147593

A thesis submitted in fulfilment of the requirements for the degree

Of

Doctor of Philosophy in Electrical Engineering

College of Agriculture, Engineering and Science, University of KwaZulu-Natal

Durban, South Africa

April 2021

As the candidate's supervisor, I agree to the submission of this thesis.

Supervisor

Professor Akshay Kumar Saha

_____

# DECLARATION 1 - PLAGIARISM

I, Vonani Clive Mathebula, declare that

1. The research reported in this thesis, except where otherwise indicated, is my original research.
2. This thesis has not been submitted for any degree or examination at any other university.
3. This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.
4. This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
    a) Their words have been re-written but the general information attributed to them has been referenced
    b) Where their exact words have been used, then their writing has been placed in italics and inside quotation marks, and referenced.
5. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and the 'References' sections.

Vonani Clive Mathebula

_____

## DECLARATION 2 - PUBLICATIONS

**a) List of published journal articles:**

**Publication 1**
V. C. Mathebula and A. K. Saha, "Mission Critical Safety Functions in IEC-61850 Based Substation Automation System - A Reliability Review," Int. J. Eng. Res. Africa, vol. 48, pp. 149–161, 2020, doi: 10.4028/www.scientific.net/jera.48.149.

**Publication 2**
V. C. Mathebula and A. K. Saha, "Reliability and Availability of Multi-Channel IEC-61850 Substation Communication Networks for Mission-Critical Applications," Int. J. Eng. Res. Africa, vol. 51, pp. 199–216, 2020, doi: 10.4028/www.scientific.net/JERA.51.199.

**Publication 3**
V. C. Mathebula and A. K. Saha, "Responsiveness of Multi-Channel IEC-61850 Substation Communication Network Reliability Performance to Changes in Repair Factors," IEEE Access, vol. 9, pp. 789–800, 2021, doi: 10.1109/ACCESS.2020.3046950.

**Publication 4**
V. C. Mathebula and A. K. Saha, "Impact of Imperfect Repairs and Diagnostic Coverage on the Reliability of Multi-Channel IEC-61850 Substation Communication Network," IEEE Access, vol. 9, pp. 2758–2769, 2021, doi: 10.1109/ACCESS.2020.3047781.

**Publication 5**
V. C. Mathebula and A. K. Saha, "Sensitivity and elasticity of multi-channel IEC-61850 Substation Communication Networks to imperfect repairs," Sustain. Energy, Grids Networks, vol. 26, pp. 100443, 2021, doi: 10.1016/j.segan.2021.100443.

**Publication 6**
V. C. Mathebula and A. K. Saha, "Multi-state IEC-61850 Substation Communication Network based on Markov partitions and Symbolic Dynamics," Sustain. Energy, Grids Networks, vol. 26, pp. 100466, 2021, doi: 10.1016/j.segan.2021.100466.

**Publication 7**
V. C. Mathebula and A. K. Saha, "Impact of Quality of Repairs and Common Cause Failures on the Reliability Performance of Intra-Bay IEC 61850 Substation Communication Network Architecture based on Markov and Linear Dynamical Systems," IEEE Access, vol. 9, pp. 112805–112820, 2021, doi: 10.1109/ACCESS.2021.3104020.

**b) Submitted manuscript under review for publication**

V. C. Mathebula and A. K. Saha, "Reliability of IEC 61850 based Substation Communication Network for Synchronous Generator Intra-Bay Architecture Considering Quality of Repairs

and Common Cause Failures," Submitted to Protection and Control of Modern Power Systems on the 21st of May 2022.

**c) Research presentation:**

V.C. Mathebula and A.K. Saha, "Reliability of repairable IEC-61850 mission-critical communication networks in power distribution centres", Postgraduate Research and Innovation Symposium (PRIS), Durban, South Africa, December 2020 (on-line).

**d) Author contributions:**

Vonani Clive Mathebula: Conceptualization, Investigation, Methodology, Design, Software, Formal analysis, Visualisation, Original writing of draft manuscripts, Review & Editing, Critical revision and editing of the final manuscripts.

Akshay Kumar Saha: Supervision, Resources and the Review of manuscripts.

Vonani Clive Mathebula

_____

## PREFACE

Vonani Clive Mathebula researched under Professor Akshay Kumar Saha's supervision in the School of Engineering, discipline of Electrical, Electronic and Computer Engineering. The research investigates the IEC 61850 Substation Communication Network (SCN) reliability in power distribution centres within industrial facilities for safety-related mission-critical applications. The research focused on the digitalisation of power distribution centres that brings about many advantages due to advancements in electronics and communication systems, enabling the realisation of full substation automation that allows implementing digital-based protection systems, control, and monitoring substation equipment using Substation Automation Systems. The IEC 61850 is the latest substation communication standard that enables real-time mission-critical message exchange between Intelligent Electronic Devices using Generic Object-Oriented Substation Events messaging service.

The research is designed to specifically answer questions relating to the requirements of the IEC 61508 standard for safety-related systems to enable the interfacing of the IEC 61850 based SCNs and safety-related systems in power distribution centres within industrial facilities concerning the reliability of the system. The research's objectives investigate the methods and considerations of evaluating the reliability performance of IEC 61850 based SCN, the basis for parameter optimisation and stability analysis for executing safety-related mission-critical functions based on the IEC 61508 standard. The research also investigates the responsiveness of the SCN reliability performance to repair factors, diagnostic coverage and common causes of failure to enable parameter selection to attain the desired system performance. Insights are shared in the research outcomes about the impact of repairs quality on the SCN's reliability performance, stability and responsiveness to system parameters. The research findings ensure an improved, optimised system functional specification and operational regime to maintain its performance during its useful life.

The research work produced eight journal articles. Two of the eight journals have been published by Trans Tech Publications, also known as Scientific.net under the International Journal of Engineering Research in Africa, comprising one review journal article and one research journal article. Three other research journal articles have been published by IEEE under the IEEE Access journal. Elsevier published two research journal articles under the Sustainable Energy, Grids and Networks journal. The last journal article is currently under review for publication in Protection and Control of Modern Power Systems, a Springer Open publication.

In addition, the research work was awarded 3rd Prize in the 2020 Postgraduate Research, and Innovation Symposium (PRIS 2020) organised by the University of Kwazulu-Natal, College of Agriculture, Engineering and Science.

## ACKNOWLEDGEMENTS

Above all, I thank God, who made everything possible and enabled me to pursue the research. I am grateful to God for my health and the means to undertake further studies. To Him, all be the glory!

I express my sincere gratitude to my supervisor Professor Akshay Kumar Saha, for his guidance, encouragement and constructive criticism, without which the research would not have been successful. Through his guidance, I have "learned how to learn". Thank you, Sir.

To my friend Dr Marubini Manyage, you have unfailingly encouraged me from my master's through to doctoral studies. Thank you so much, Sir. Thank you for accepting to proofread the selected chapters of my thesis. Thank you for your concern about my health. May God bless your family.

To Ms Miranda Skaka, thank you for your encouragement, helping to source research articles, and accepting to proofread selected chapters of my thesis. Thank you for your friendship. Your concern for our family is greatly appreciated. May God bless your family.

Great appreciation also goes to Mr Thapelo Theledi for assisting me in sourcing research articles. You have always been there to celebrate even the smallest of the research successes. Thank you, Sir.

To my friend, Mr Remember Sigawuke and his family, thank you for checking on me when I was not feeling well during my studies. May God bless your family.

To my friend and brother, Mr Musatondwa Lalamani, thank you for reaching out to me during my studies. Our conversation gave me great courage and hope. Thank you, Sir. May God bless you and your family.

To my friend Mr Voquiline Shiluvana, with whom we have been pursuing further studies together, thank you for your encouragement along the way. May God bless your family, Sir.

To my friend Mr Baaresa Tjia, thank you for your encouragement along the way. May God bless you as you pursue further studies, Sir.

To my very close friend and wife, Dolly Mathebula, thank you so much for your love and unfailing support. You have always cared for the kids and me and remained patient, allowing me to pursue my studies. You have acted as a father to our kids on my behalf on many occasions; thank you so much. May God give you wisdom and bless you as you pursue your further studies. Thank you for accepting to proofread the selected chapters of my thesis.

To my kids, Nkateko and Makungu, thank you for enforcing study breaks by 'disturbing' me from time to time. You always knew when I needed to take a break. I thank God for you always. May God remain with you and guide you to fulfil your purposes according to His will.

To my parents, Mr Stephen Mhlanganisi Mathebula and Mrs Tsakane Anna Mathebula, thank you for allowing me to conclude my high school studies at Orhovelani High School,

where the idea of pursuing doctoral studies was conceived. I greatly appreciate all the sacrifices you have made for me to attend university and your prayers for me. Thank you for checking on me when I was not feeling well during my studies. May God bless you. I hope that this achievement will be an excellent surprise for you.

To my mother, Mrs Gadihele Sophia Rulane, thank you for your love and support; and for checking on me when I was not feeling well during my studies. May God bless you.

To my brother Mr Nyiko Mathebula, thank you for encouraging me during my high school studies, especially at Orhovelani, where the idea of doctoral studies began, and for taking time to drive me through to my first graduation. Thank you, Sir. May God bless you.

To my sister, Mrs Lebogang Mathebula and family, thank you for your love for our family and for checking on me when I was not feeling well during my studies. I hope that this thesis will be an excellent surprise for you.

To my brother, Mr Fumani Mathebula, I remember very well you helping me with the registration process on my arrival in Durban to attend university, which is the foundation of this achievement. Thank you, Sir.

To my sister Mrs Phozisa Mathebula and the family, thank you for your concern when I was not feeling well during my studies. I hope that this thesis will be an excellent surprise for you.

To my cousin, Ms Tsheketi Augustina Ndhambi, thank you for the encouragement during my studies and your concern when I was not feeling well. Even though you are in another country, you walked the path with me; you knew every milestone, you celebrated even my small achievements, distance proved not to be an issue. May God bless you.

To my sister, Ms Mixo Hlungwani, we walked the academic journey together even though you left me to continue by myself. Thank you for all the support and encouragement. May God bless you as you begin another chapter of your life.

To my sister, Ms Boitumelo Rulane, thank you for always caring. May God bless you.

To my cousin, Ms Masingita Hlungwani, my brother Tsundzuka Bamuza and your families, thank you for your concern about my health during my studies. May God bless you.

To my cousin, Ms Mikateko Ndhambi, thank you for the inspiration to study while working. I hope that this achievement will be an excellent surprise for you.

To my cousin, Mr Cyreal Musa Sekatane and your family, thank you for your concern when I was not feeling well during my studies. Thank you also for checking on my parents whenever you are home. I hope that this achievement will be an excellent surprise for you.

To my sister, Ms Tsakani Fiona Mathebula, this one is for you! May God bless you.

Again, all the glory goes to God Almighty, who made all possible! To Him be the praise, forever and ever!

## ABSTRACT

IEC 61850 based Substation Communication Networks (SCN) enable substation processes to be digitalised to fulfil the most sought substation monitoring, protection and control of electrical systems. The standard enables peer-to-peer communication of mission-critical messages, aided by onboard diagnostic capabilities to ease the identification of system faults. The implementation of Safety-Related Systems in industrial facilities comprising sensors, logic solvers and final elements in power distribution centres necessitate compliance to IEC 61508 standard, where circuit breakers act as final elements to isolate electrical machines. In recent times, combinatorial methods such as the Reliability Block Diagram have been used to evaluate the architecture of IEC 61850 based SCN reliability and availability due to the simplicity of the approach. These methods, however, assume that all system faults are identified and fully repaired, which is not the case in practice. In this thesis, the reliability of a repairable multi-channel IEC 61850 based SCN architecture is modelled using a structure-function and the Markov process while Systems Thinking integrates imperfect repair factors into the model. Thereafter, a novel eigenvalue analysis method based on Markov partitions and symbolic dynamics in the context of linear dynamical systems is used to investigate the impact of imperfect repairs on the system's reliability based on the number of mean state transitions and dynamical behaviour. The eigenvalue method is then advanced by a complimentary analysis technique based on the absorbing Markov Chain process and matrix calculus methods to determine the system's responsiveness to repair factors. The case studies results demonstrate that imperfect repairs cannot be ignored for mission-critical applications because the simplifying assumptions of combinatorial analysis methods greatly over-state the system's reliability performance. The results also indicate that common causes of failure coupled with imperfect repairs significantly negatively impact the system's performance. Moreover, system performance is highly dependent on the diagnostic coverage of the individual subsystems than their repair efficiencies for high diagnostic coverages at 90% and 99% based on ISO 13849-1. Hence, the results demonstrate that emphasis should be more on the system diagnostic coverage for the fact that it is embedded in the system design itself that cannot easily be changed once the system is commissioned and operational.

## CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| CFF | Common Cause Failure |
| DC | Diagnostic Coverage |
| E/E/PE | Electrical/Electronic/Programable Electronic |
| ETE | End-To-End |
| EUC | Equipment Under Control |
| FMEDA | Failure Modes, Effects, and Diagnostic Analysis |
| FRGM | Funnel Risk Graph Method |
| FTA | Fault Tree Analysis |
| GGIO | Generic Logical Node Input/output |
| GOOSE | Generic Object-Oriented Substation Event |
| HMI | Human Machine Interface |
| HSR | Highly Available Seamless Redundancy |
| IEC | International Electrotechnical Commission |
| IED | Intelligent Electronic Device |
| IEEE | Institute of Electrical and Electronics Engineers |
| ISO | International Organization for Standardization |
| MC | Markov Chain |
| MMS | Manufacturing Message Specification |
| MTTF | Mean Time To Failure |
| MTTR | Mean Time To Repair |
| OSI | Open Systems Interconnection |
| PSRC | Power System Relaying Committee |
| PRP | Parallel Redundancy Protocol |
| PT | Proof Test |
| PTE | Proof Test Effectiveness |
| QoR | Quality of Repairs |
| RAMS | Reliability, Availability, Maintainability and Safety |
| RBD | Reliability Block Diagram |
| RSTP | Rapid Tree Spanning Protocol |
| RTU | Remote Terminal Unit |
| SAS | Substation Automation System |
| SCN | Substation Communication Network |
| SIF | Safety Instrumented Function |
| SV | Sampled Values |
| SIL | Safety Integrity Level |

| | |
|---|---|
| SIS | Safety Instrumented System |
| SoS | System of Systems |
| TCP/IP | Transmission Control Protocol/Internet Protocol |

## LIST OF SYMBOLS

| | |
|---|---|
| $A$ | Availability |
| $A_P$ | Availability of parallel systems |
| $A_s$ | Availability of series systems |
| $\beta$ | Common cause factor |
| Ɗ | Diagonal matrix operator |
| ε | Elasticity |
| $\lambda$ | Failure rate |
| ∀ | For all |
| $I$ | Identity matrix |
| $\otimes$ | Kronecker product |
| $PFD_{avg}$ | Probability of Failure on Demand |
| $r_{eff}$ | Repair efficiency |
| μ | Repair rate |
| $e_{dc}$ | System diagnostic coverage |
| $P$ | Transition probability matrix |
| $Q_{sys}$ | System unreliability |
| $R_P$ | Reliability of parallel systems |
| $R_s$ | Reliability of series systems |
| $R_{sys}$ | System reliability |
| vec | Vector operator |

# CHAPTER 1

# INTRODUCTION

## 1.1 Background

The digitalisation of power distribution centres increases as industries grow confidence in applying Substation Automation Systems (SAS). The system offers many advantages such as easy system diagnostics, reduced copper wires, less installation time, increased monitoring, and simplifies the process of effecting or implementing system design changes [1], [2]. IEC 61850 is the latest standard for Substation Communication Networks (SCN) that enables peer-to-peer communication between substation devices, allowing a faster communication platform between Intelligent Electronic Devices (IEDs) to share critical information such as interlocking and protection signals [3]. Moreover, the IEC 61850 standard also supports bay distributed functions, ensuring high reliability because the loss of communication resulting from a switch failure does not immediately render the system inoperable. However, industries are yet to be comfortable with the reliability of the IEC 61850 based SCN when applied within power distribution centres of industrial facilities to execute mission-critical functions [3], [4].

The GOOSE communication mechanism of IEC 61850 based SCN is suitable for substation protection scheme devices to share information than legacy communication protocols that only allow master-slave communication configurations, which does not support peer-to-peer communication required for distributed mission-critical signal exchange [1], [5]. The standard also solves the challenges resulting from multiple substation communication protocols, including propriety protocols that make the integration of substation devices even more challenging [1], [2]. The reliability of IEC 61850 based SCNs has been explored at both component and system levels using many approaches based on combinatorial analysis methods such as the reliability block diagrams and failure mode effect analysis in the form of state-space transition approach, respectively; to investigate composite reliability of the system. Nevertheless, these approaches fall short when interrogating some of the requirements of the safety-related standard IEC 61508 for Electrical, Electronic and Programmable Electronic (E/E/PE) devices. Complete digitalisation of power distribution centres in industrial facilities requires SCNs to interface to IEC 61508 based safety-related systems [6]–[8].

## 1.2 Research problem and motivation

A power distribution centre's primary function is to distribute power to various parts of the plant and supply power to medium voltage motors, where some of the medium voltage motors include draught fan systems in thermal plants. The Safety Integrity Level (SIL) of the draught systems' protection is based on the IEC 61508 and IEC 61511 safety-related standards.

The IEC 61508 and its associated standards emphasise the system's reliability and fail-safe design approach and focus on the probability of failure on demand for specific safety instrumented protection and control functions [6], [9]. The IEC 61508 and IEC 61511 standards complement each other, where the IEC 61508 is targeted to the designers of safety-related system components, whereas the IEC 61511 is aimed at the safety-related user's systems and components [10]. The IEC 61508 stipulates specific requirements to be satisfied for safety instrumented protection functions. The ever-growing digitalisation of power distribution centres within industrial facilities requires safety instrumented systems to be implemented through SCNs, wherein IEC 61850 is the most preferred communication protocol within industrial facilities' power distribution centres.

Legacy substation communication protocols such as Modbus RTU, Ethernet TCP/IP and DNP3 do not support real-time communication required for protection and interlocking within a substation. However, IEC 61850 based SCN enables automated functions for protection, control, and monitoring within a substation by taking advantage of the much-improved electronics and digital systems that enhance information exchange and communication technologies in general [6], [11]. The IEC 61850 standard enables real-time interoperability between substation devices [11], a significant accomplishment of the substation communication standard in enabling substation design integration and optimisation.

According to K. Kaneda et al. [11], the design of an IEC 61850 based SCN should consider the functional requirements of the communication network as the first and most important input in the design process of formulating the design criteria to allow proper selection of SCN components such as switches and IEDs. The criteria should also consider the criticality level of the substation and the required safety-related protection applications.

Even though not all substation functions have been modelled in the IEC 61850 standard [11], using Generic Input/Output logical node (GGIO) allows modelling functionalities that are not standard in IEC 61850. Therefore, the appropriate application of logical nodes is necessary to achieve interoperability and satisfy the substation automation system's required functionalities. Moreover, careful consideration is required not to compromise the interoperability of the substation devices. Hence, generic logical nodes such as GGIO in the IEC 61850 based SAS should only be used to implement functions that are not defined in the standard. Thus, generic nodes can be considered for implementing safety-related functions initiated outside the power distribution centre.

IEC 61850 based SCN protocol uses Generic Object-Oriented Substation Events (GOOSE) messages to transmit information that changes sporadically to deliver such messages to multiple devices using multicast/broadcast frames. These messages include tripping commands and interlocking information [4]. The IEC 61783 standard identifies several SCN possible digital communication errors that may lead to packets' corruption; the

standard also makes recommendations for how each can be mitigated or avoided. The recommended measures outlined in the standard are not mandatory; this is because alternate measures can be implemented in a system to mitigate the same possible errors. Since the protection and interlocking functions are implemented using the GOOSE messages in the IEC 61850 based SCN [11], SCN for transmitting GOOSE message must satisfy the IEC 61508 requirements to execute safety-related functions initiated outside the power distribution centre. Hence, the research investigates the reliability of the IEC 61850 based SCN in the context of the safety-related standard IEC 61508 and seeks to determine the impact of the quality of repairs on the SCN's reliability performance. The research also seeks to determine the basis of performance optimisation and its stability under various parameter levels. The following section presents the research questions.

### 1.3 Research questions

The research seeks to answer the following questions concerning the reliability of IEC 61850 based SCN in industrial facilities' power distribution centres.

a) Whether combinatorial reliability analysis methods are suitable for evaluating IEC 61850 based Substation Communication Networks (SCNs) for mission-critical applications, with specific reference to IEC 61508, the standards for safety-related systems?
b) What would be considered a safety-related mission-critical SCN architecture's desired characteristics considering reliability in a power distribution centre within industrial facilities?
c) Whether the quality of repairs can be optimised for best performance, and; what would be the basis for optimisation?
d) What would be considered the most critical factor to consider for achieving high-reliability performance, and at what system level?

### 1.4 Aims and objectives

The research aims to investigate the IEC 61850 based power distribution centre SCN architecture's functional reliability performance from the IEC 61508 perspective, particularly the impact of imperfect repairs and system fault coverage, as applied in industrial facilities. The objectives of the research are as follows:

a) Determine methods and considerations to evaluate IEC 61850 based SCN performance, optimisation and stability when the system is used to execute safety-related mission-critical functions.
b) Investigate the responsiveness of SCN reliability performance to repair factors and system fault coverage to enable parameter selection.

Hence, the objective of the research is to develop reliability modelling techniques of IEC 61850 based SCN architecture to evaluate the impact of imperfect repairs and diagnostic coverage on its performance, aimed at proposing a basis for system design and operational optimisation. In addition, the research aims to evaluate the system performance sensitivity to the repair factors and its diagnostic coverage. The effectiveness of the mathematical models is evaluated considering a "one-out-of-two" system commonly applied in protection schemes within industrial facilities.

## 1.5 Scope of the research

The research work investigates the reliability of a multi-channel IEC 61850 based SCN using the Markov process. Specific to this research, a 'one-out-of-two' system is investigated to determine the impact of repairs on the system's useful life, considering repair efficiency and system diagnostic coverage. Moreover, the research investigates the impact of common causes of failures on the system characterised by the low quality of repairs. In-depth investigations of system stability and convergence rate are studied using linear dynamical systems and matrix similarity concepts to determine the system's asymptotic behaviour, while sensitivity studies are utilised to study the system's transient response to parameter changes. All programming is done on MATLAB software. The following section presents the contributions to knowledge.

## 1.6 Contribution to knowledge

The reliability of SCN is mainly evaluated using combinatorial analysis methods because they are easy to comprehend and apply. However, the methods do not consider system states interactions resulting from the complexity of the systems. Modern digital communication systems are considered complex due to their state evolution resulting from subsystems' state changes, the physical environment and the required human intervention level during the design and operational stages. These aspects are highlighted in Chapter 2 and summarised in a published review journal article [2], whose main contributions are:

a) Highlight the capability of IEC 61850 based SAS functional features to execute mission-critical safety protection applications.
b) Highlight factors to be incorporated in evaluating IEC 61850 based SAS dependability for mission-critical safety functions.
c) Review of analysis methods used to evaluate the reliability and availability of IEC 61850 SAS.

The research work uses the Markov process and mathematical expectation incorporating Systems Thinking to integrate quality of repairs in the evaluation of SCN's reliability performance in Chapter 4 and Chapter 5 as a result of the system's level of diagnostic coverage, repair efficiency based on the completeness and correctness of repairs, and the

impact of common causes of failures on the system at different levels of quality of repairs. The contributions of Chapter 4 are summarised in a published research journal article [8], whose main contributions are:

a) Highlight SAS's reliability and availability performance evaluation necessities when IEC 61850 digital-based SCN interfaces to IEC 61508 systems in a future power distribution centre.
b) Integration of system diagnostic capability and repair efficiency factors in evaluating the system reliability and availability performance in IEC 61850 digital SCN based on Systems Thinking.
c) Highlight the criticality and impact of diagnostic capability and repair efficiency factors on the mean system state transitions of a multi-state IEC 61850 SCN.

The contributions of Chapter 5 concerning the impact of common causes of failure on the reliability performance of IEC 61850 based SCN are summarised in a published research journal article [12], whose main contributions are:

a) Analysis of IEC 61850 SCN architecture reliability based on Markov process and Linear Dynamical Systems, considering the quality of repairs and common causes of failure; where the concept of architecture reliability focuses on the reliability of the physical SCN.
b) Impact of CCF on the system architectural state transitions' dynamics and stability, considering the quality of repairs.

The research work also investigated the impact of the quality of repairs on the system's reliability performance and stability using the Markov process and linear dynamical systems in Chapter 6, where the transition probability matrix's eigenvalues are used to characterise the behaviour of the system. The system's performance level is based on the spectral gap between the eigenvalue magnitude one and the second largest eigenvalue(s). Moreover, it is shown in the chapter that the response of the eigenvalue magnitudes can be used as a basis for parameter optimisation and dynamical analysis. The main contributions of Chapter 6 are summarised in two published research journal articles [13], [14], whose main contributions are:

a) Determining the repair efficiency's effectiveness on the system's reliability performance and its dynamics at any given system diagnostic coverage level.
b) Analysis of the Markov chain process dynamics using the eigenvalues' magnitude and layout formation. The spectral gap magnitude between the eigenvalue magnitude one and the second-largest eigenvalue is used to determine the rate of system convergence based on mean state transitions and philosophical operating changes resulting from changes in repair efficiency and or diagnostic coverage.

The impact of system parameter changes on the reliability performance is investigated in Chapter 7, wherein the absorbing Markov chain process and matrix calculus methods are used to determine the system's responsiveness. This approach enhances the eigenvalue method as a complementary technique to determine the effectiveness of various factors at the subsystem level. The main contributions of Chapter 7 are summarised in two published research journal articles [15], [16], whose main contributions are:

a) Demonstrate the significance of accurate and comprehensive system fault diagnostics and repairs to achieve high system reliability performance for mission-critical systems in power distribution centres.
b) Provide complimentary analysis technique that advances the asymptotic eigenvalue analysis method based on absorbing Markov chain and matrix calculus to focus on the system's transient states.
c) Analysis of system responsiveness to imperfect repairs (viz. repair efficiency and system diagnostic coverage factors) to enable objective optimisation of the system Mean Time To Failure (MTTF) based on the mean system state transitions at the subsystem level of multi-channel IEC 61850 SCNs.

The research outcome shares insights into understanding the requirements for SCNs to execute mission-critical safety-related functions and the basis for system optimisation for high-reliability performance.

## 1.7 List of novelties

This section presents a summarised list of novelties:

a) The research models the quality of repairs (viz. repair efficiency and diagnostic coverage) impacting the reliability performance of IEC 61850 based SCN architecture using the Markov process and symbolic dynamics in the context of Linear Dynamical Systems. The focus is on the spectral gap between the magnitude '1' and the second-largest eigenvalue magnitudes that determine the average mean system state transitions before failure, whereas a change in the layout formation of the eigenvalues determines the change in system dynamics. This approach enables the determination of system parameter optimisation basis.
b) Sensitivity and elasticity analysis of IEC 61850 based SCN architecture to the quality of repairs (viz. repair efficiency and diagnostic coverage) is modelled using the Markov process and Matrix Calculus methods to enable effective system parameter adjustment for optimisation purposes.

## 1.8 Thesis outline

Chapter 2: This chapter presents the literature review and focuses on the IEC 61850 communication network standard. Safety-related mission-critical systems concerning industrial power distribution centres are also reviewed in this chapter, wherein an overview of the functional safety standard IEC61508 is presented. The dependability, rating of safety instrumented systems and their reliability evaluation methods are reviewed. In addition, reliability evaluation studies of IEC 61850 based SCN are comparatively analysed. The chapter concludes by summarising the review findings.

Chapter 3: This chapter presents the followed methodology to investigate the reliability of IEC 61850 mission-critical SCN based on a stochastic model using the Markov process and discusses reliability and availability evaluation concepts. The derivation of the reliability function and essential reliability and availability formulae is presented and discussed. System dynamics analysis, as well as preliminaries and notation of matrix calculus, are presented, and the research work's boundaries and limitations.

Chapter 4: This chapter focuses on integrating imperfect repairs and system diagnostic coverage as factors that should be considered in determining the reliability and availability of a mission-critical system based on IEC 61850 and IEC 61508. An overview of an industrial power distribution centre and the case studies basis are discussed. Modelling imperfect repairs and system diagnostic coverage using structure-function, Systems Thinking, and the Markov process is presented. The estimation of the system's mean state transitions based on mathematical expectation is presented in this chapter. The overview of system diagnostic coverage levels is discussed and forms the basis of the research case studies. Subsequently, the results and discussions are presented, as well as the case studies findings and conclusions.

Chapter 5: This chapter investigates the impact of common causes of failures in SCN characterised by low quality of repairs. The β-factor model is used in this research work and is discussed in this chapter. Modelling CCFs in systems with imperfect repairs and limited diagnostic coverage based on the Markov process is also discussed. Case studies results and discussions are presented. Subsequently, findings and conclusions resulting from the studies are discussed.

Chapter 6: This chapter presents an overview of dynamical systems and the Markov partitions. Thereafter, the Markov process in the context of linear dynamical systems is presented and used to study the dynamics of the system and its performance based on eigenvalues using the concept of matrix similarity. The chapter ends by presenting case studies and discussing the findings and the conclusions and recommendations.

Chapter 7: This chapter presents the context of the sensitivity and elasticity analysis of the mean system state transitions to the repair and diagnostic coverage factors used to analyse

its responsiveness. Thereafter, the derivation of the absorbing Markov Chain fundamental matrix's sensitivity and elasticity is discussed. Next, the modelling of sensitivity and elasticity of a 'one-out-of-two' system to imperfect repair factors is presented. The results and discussions of the case studies are summarised. Observations and the findings of the case studies are highlighted in the chapter conclusion.

Chapter 8: This chapter summarises the research findings and conclusions. The future recommended research work is also presented in this chapter.

# CHAPTER 2

# LITERATURE REVIEW

## 2.1 Introduction

IEC 61850 is the latest standard for communication networks in substations comprising multi-vendor systems. However, the introduction of digital communication-based networks brings about new challenges to the substation environment, which among others, results from incorrect specification, stochastic or systematic hardware failures of substation devices, systematic software failures, environmental influences or supply voltage disturbances that can result in many different errors and or failures during communication between substation devices [2], [4], [17]. According to the IEC 61508 standard for safety-related systems, the implementation of functional safety systems comprising sensors, logic solvers, and final elements require the entire system to be reliable and available on-demand from the sensors to the final elements. The system's performance should also be real-time and deterministic to act on the onset demand of protection functions. Substation Communication Networks (SCNs) interface with circuit breakers through microprocessor based Intelligent Electronic Devices (IEDs) in power distribution centres. Circuit breakers, therefore, act as final elements of the Safety Instrumented Systems (SIS) to isolate electrical machines when it becomes necessary [18], [19]. Therefore, the SCN and circuit breakers' dependability should satisfy the applicable safety standards' requirements in power distribution centres.

Legacy safety-related control systems such as PROFsafe, Ethernet Powerlink safety, SERCOS III safety and EtherCAT implement an additional layer over and above the seven layers of the Open System Interconnection (OSI) model in order to satisfy the requirements of the IEC 61508 standard; whereas IEC 61850 based SCN is based only on the seven layers of the OSI model. IEC 61850 incorporates error detection capabilities within the seven layers of the OSI. Legacy safety control systems do not support peer-to-peer communication between substantiation devices, while IEC 61850 based system supports peer-to-peer communication and interoperability between multi-vendor devices as the main objective of the standard. Multi-vendor devices are often configured to execute critical protection functions in order to eliminate Common Cause Failures (CCF) [20]–[22].

Safety-related systems can be implemented using any technology, including software-based technologies; however, the Safety Integrity Level (SIL) of the technology employed should satisfy the required level of specified safety integrity [4] based on the IEC 61508 standard. Hence, IEC 61850 based SCN system can be considered for implementing safety-related functions since it supports interoperability between multi-vendor devices, which is most suited for a substation environment where tripping of circuits is needed during plant

abnormalities. IEC 61850 based automation system support real-time information exchange in the form of Generic Object Oriented Substation Events (GOOSE), legacy substation communication protocols such as Modbus RTU, Ethernet TCP/IP and DNP3 do not support real-time communication that is needed for protection, bus transfer schemes and interlocking information exchange between substation devices [1], [4], [23]–[25].

Substation Communication Network (SCN) failures are the leading cause of Substation Automation System (SAS) failures, with the physical layer of the OSI model being the area where they mainly occur [26], [27]. Incorrect network configuration and settings are also concerns following the physical layer, which can be minimised or even avoided by testing the SCN during its commissioning. According to [26], firmware upgrades of Intelligent Electronic Devices (IED) as well as code and database failures may also cause SCN to malfunction, since upgrades of IEDs often include additional parameters as part of improvements, which will impact the current addressing functions of the IED, while code simplification eliminates code errors. It is, therefore, necessary to re-commission the system following firmware upgrades of network devices.

The design of the IEC 61850 based SCN should consider the required functional specification of the automation system as the first and most important input in the design process in order to formulate design criteria to allow proper selection of SCN devices such as switches and IEDs based on the criticality level of the substation, as well as any implemented safety protection functions. This approach is acceptable since different substations will have different criticality levels. It follows, therefore, that IEC 61850 does not guarantee any level of reliability. However, the standard's flexibility allows the designer of the SCN to determine and configure the network topology to meet the required level of reliability according to the communication system's functional requirements. Moreover, IEC 61850 also supports bay distributed functions, ensuring high reliability because the loss of communication as a result of a switch failure will not immediately render the system inoperable [1], [27], [28].

Although not all substation functions have been modelled in IEC 61850 according to [11], using generic logical node GGIO allows modelling functions that are not standard in IEC 61850. Nevertheless, careful consideration is required in order not to compromise the interoperability of the substation devices. Therefore, the appropriate application of logical nodes is necessary to achieve interoperability to satisfy the SCN's required functionalities. Generic logical nodes such as GGIO in IEC 61850 based system should be used only to implement functionalities that are not defined in the IEC 61850 standard. Hence, they can be considered for implementing safety-related functions since IEC 61850 based SCN uses GOOSE messages to transmit information that changes sporadically to provide real-time deterministic delivery of such messages to multiple devices using multicast/broadcast frames,

and these messages include tripping commands and interlocking information signals [4], [11], [24].

Section 2.2 presents a review of the IEC 61850 communication network. Safety-related mission-critical systems are discussed in section 2.3 concerning industrial power distribution centres. An overview of the functional safety standard IEC61508 is presented in section 2.4. Sections 2.5 and 2.6 present the dependability and rating of safety instrumented systems, respectively. Reliability evaluation of safety instrumented systems is presented in section 2.7, whereas section 2.8 presents reliability evaluation studies of IEC 61850 based SCN. Section 2.9 presents the review findings and the conclusion of the review.

## 2.2 Digital Substation: IEC 61850 based Substation Communication Network

The reliability of the IEC 61850 based SCN has been explored at both component and system levels using many methods such as the Reliability Block Diagrams (RBD) and failure mode effect analysis in the form of state-space transition approach, respectively. The objective has always been intending to investigate the composite reliability of the system ultimately. These methods seem to offer some comfort level to the system's designers and the plant owners to encourage full implementation of the standard within power distribution centres to realise its full benefits.

### 2.2.1 Overview of the IEC 61850 Substation Communication Networks standard

The evolution of SCNs saw the replacement of propriety protocols with open and standardised Transport Control Protocol/ Internet Protocol (TCP/IP) based Ethernet networks, enabling more straightforward and cost-effective integration of various industrial protection and control substation devices using modern microprocessor-based Electronic Intelligent Devices (IEDs) to integrate protection, monitoring, automation, control, as well as digital fault recording capability in one device [18], [29]–[31]. IEC 61850 standard, being the latest substation automation system standard that enables peer-to-peer communication between substation devices, was developed between 2002 and 2005 to enable interoperability between multiple vendor-supplied devices. The standard comprises ten parts, wherein the general and specific functional requirements in the substation are defined in parts 3, 4 and 5 of the standard [18], [27], [31], [32]. The IEC 61850 standard is intended explicitly for electrical substations or power distribution centres to solve interconnectivity challenges resulting from the use of multi-vendor devices by adopting an abstracting architectural construct in the form of data objects and services that are independent of any underlying protocols [18], [19], [33]. Some of the benefits or functional features of the IEC 61850 standard include [18], [19], [33]–[35]:

- Fast data transmission of Generic Substation Events (GSE) messages using a peer-to-peer mechanism

- Data definition based on object-oriented modelling
- Standardised data modelling
- Communication extendibility and data integrity
- Non-vendor dependent system scalability
- Increased reliability by application of appropriate bus topology
- Simplicity, cost-effective substation architecture and Future proof standard
- Standardised high-level communication services based on switched Ethernet technology

Accordingly, the IEC 61850 standard enables project design simplification due to standardised tools and design platform, easy deployment, construction, installation and commissioning, and project documentation thereof [34]. In modern SCNs, IEDs are connected to an Ethernet network, and their abstract models are mapped to Manufacturing Message Services (MMS), Generic Object-Oriented Substation Events (GOOSE) and Sampled Values (SV) messages according to IEC 61850. Hence, the reliability and security of SCNs should be of high integrity, as well as able to tolerate faults [27], [29], [35], [36]. Advanced Ethernet communication networking protocols offer deterministic transmission of messages needed for real-time and mission-critical tasks such as protection and interlocking applications in power distribution centres, wherein GOOSE message is employed according to IEC 61850 standard [18], [19]. Figure 2-1 depicts the mapping of GOOSE, SV & MMS messages to the OSI model communication stack's Ethernet layer.

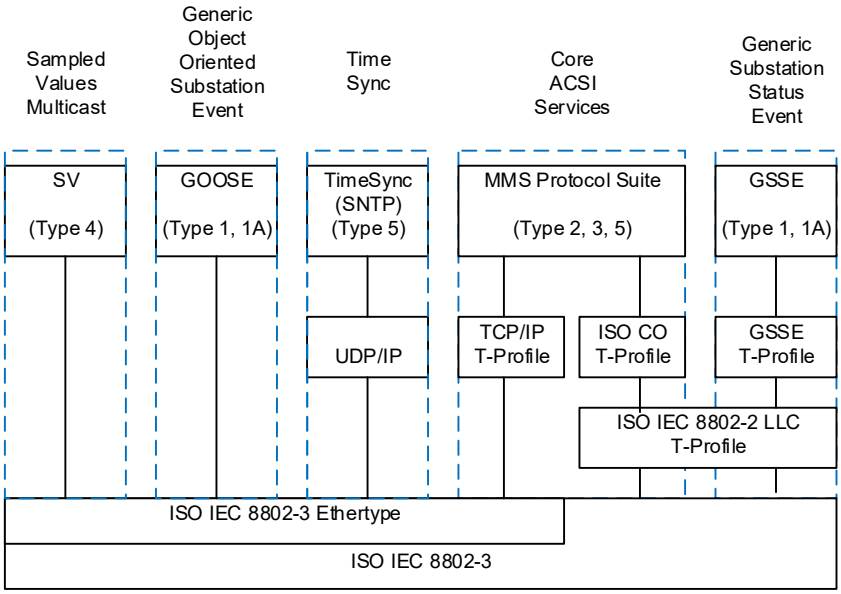


Figure 2-1: Mapping of GOOSE, SV & MMS to OSI model communication stack [27], [33], [35], [37]

Mapping of GOOSE and SV messages directly to the Ethernet layer allows fast communication of messages in real-time using peer-to-peer communication between devices

without going through the TCP/IP layer, thereby enabling the development of sophisticated, time-critical, deterministic protection functions. IEC 61850 standard defines time-critical peer-to-peer or horizontal communication (device to device) messages as GOOSE and SV. Accordingly, protection functions can be configured to be deterministic and, therefore, highly reliable [18], [19], [29], [35].

GOOSE and SV messages are transmitted using the multicast mode and delivered to multiple devices recipient IEDs. In particular, GOOSE messages are event-driven, with built-in retransmission mechanism capability to increase dependability, as depicted in Figure 2-2. A similar concept is used for SV [18], [34] [38].

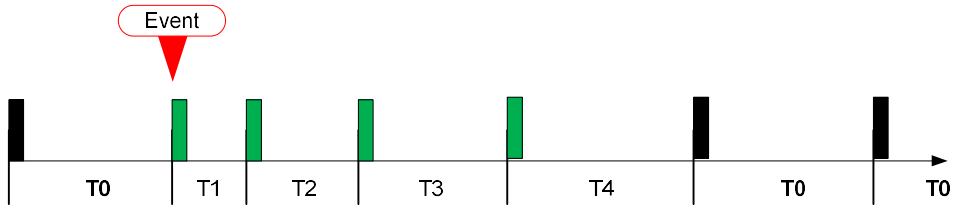


Figure 2-2: GOOSE message retransmission mechanism [3], [4], [34]

The IEC 61850 standard defines performance classification of message transmission to which the data signals can be managed in order to satisfy specific design requirements in substations as depicted in Table 2-1 [18], [29]:

Table 2-1: IEC 61850 message types and performance classes [29], [30], [38]

| Message Type | Application | Performance Class | Transmission Time (ms) |
|---|---|---|---|
| 1A | Fast messages (Trip) | P1 | 10 |
| | | P2/P3 | 3 |
| 1B | Fast messages (Other) | P1 | 100 |
| 3 | | P2/P3 | 20 |
| 2 | Medium speed | | 100 |
| 3 | Low speed | | 500 |
| 4 | Raw data | P1 | 10 |
| | | P2/P3 | 3 |
| 5 | File transfer | | >1000 |
| 6 | Time synchronisation | | (Accuracy) |

According to [18], [38], the message transmission time in SCNs is dependent on the communication devices' processing time and the substation architecture, as illustrated in Figure 2-3; where the time $t_b$ is dependent on the network communication architecture including all latency accumulated from message queuing and processing time at each substation communication device along the message path. Hence, the SCN's architecture determines the End-to-End (ETE) performance of the communication network. Thus, the performance of a SCN is highly dependent on the overall performance of the SCN. Even

though the IEC 61850 standard offers many benefits according to [18], [19], [33]–[35], in [34], [39], the authors highlight reliability, availability and performance of the system as some of the challenges brought by digital Substation Automation System (SAS) technology.

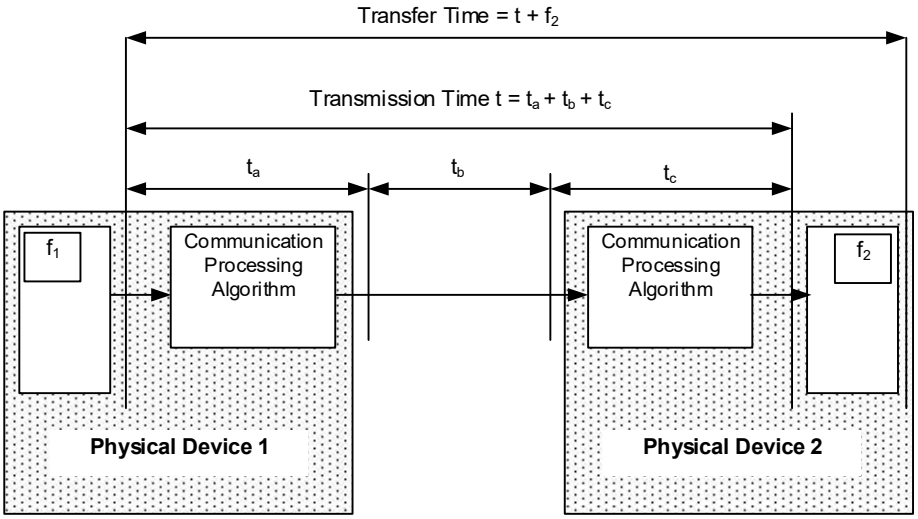


Figure 2-3: GOOSE Message transmission time between IEDs [18]

IEC 61850 based SCN architecture determines the speed and deterministic characteristic transmission of protection function messages [35]. Data flow management associated with protection applications is assigned to have the highest priority in the SCN, followed by operational data; the least priority is assigned to non-operational data, including disturbance records, to achieve real-time deterministic message transmission in IEC 61850 based SCNs. Therefore, the definition of message transmission performance classification in the IEC 61850 standard is well suited for stringent mission-critical real-time applications such as protection functions [30].

The IEC 61850 standard does not standardise SCN architectures and leaves it to the system designer. However, the Institute of Electrical and Electronics Engineers' Power System Relaying Committee (IEEE/PSRC) consider cascade, star, ring, star-ring, and redundant ring as typical SCN architectures [28], [40]. Figure 2-4 depicts the star and ring communication network architectures. In [30]–[32], [35], [40], IEC 61850 based SCN architectures have been studied, as well as implemented in some cases. According to [30]–[32], [35], [39], [40], the star architecture offers the least reliability with no redundancy and has a single point of failure since it has one backbone switch. Hence, the star architecture is only suitable for monitoring, even though it offers the lowest network latency and is easy to maintain. On the other hand, ring architecture provides redundancy through an alternative path using Rapid Spanning Tree Protocol (RSTP) or propriety protocols. However, network reconfiguration is required when one link or switch failure occurs [30], [35].

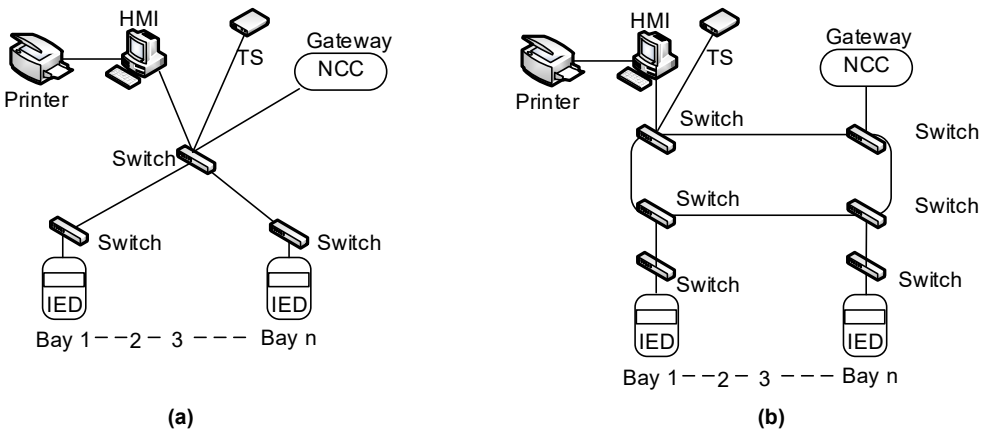


Figure 2-4: Star and ring Substation Communication Network (SCN) architectures [31], [35], [39]

In [30]–[32], the hybrid SCN architectures are considered, where the SCN architecture combines two or more types of SCN architectures and can offer the best performance and benefits such as the highest level of redundancy and low network latency if it is optimally configured. Figure 2-5 depicts ring-star hybrid SCN architecture.

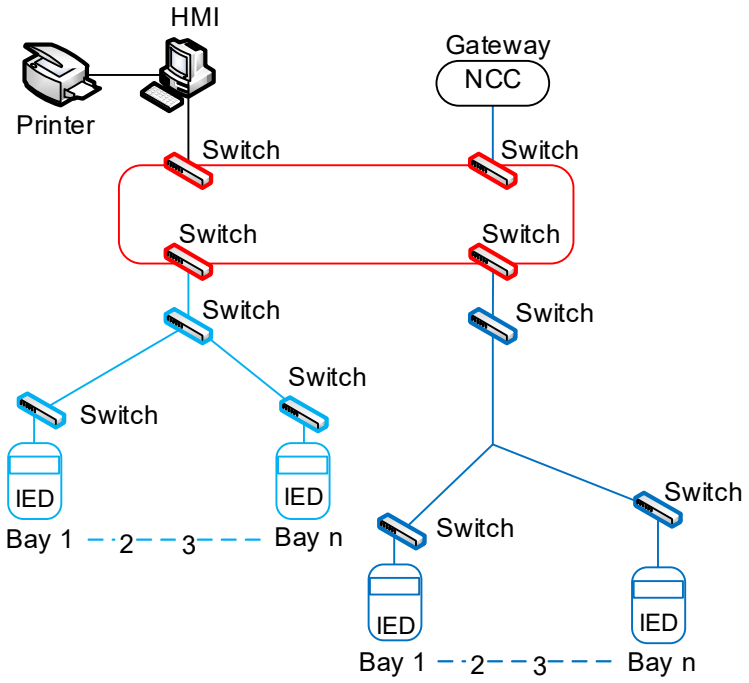


Figure 2-5: Ring-star SCN architecture [31], [35], [39], [41]

According to the IEC 61850 standard, following the IEC 61870-4 concerning the reliability of a SCN, no single point of failure should cause the system to be inoperable [28], [30], [32]. Therefore, to satisfy substation protection and control objectives, the SCN design should consider the following [30], [35]:

- Dependability

- Bandwidth
- Redundancy design approach
- Latency delays
- Network convergence
- Network segmentation
- Scalability and expandability
- Maintainability
- Interoperability

IEC 61850 based SCN architecture comprises three levels: process, bay, and station levels, as depicted in Figure 2-6 [19], [42]. The process level is involved with the measurements instruments or sensors that interface to the bay level comprising IEDs, whereas the station level is the control application layer [19], [30], [32], [39], [42].

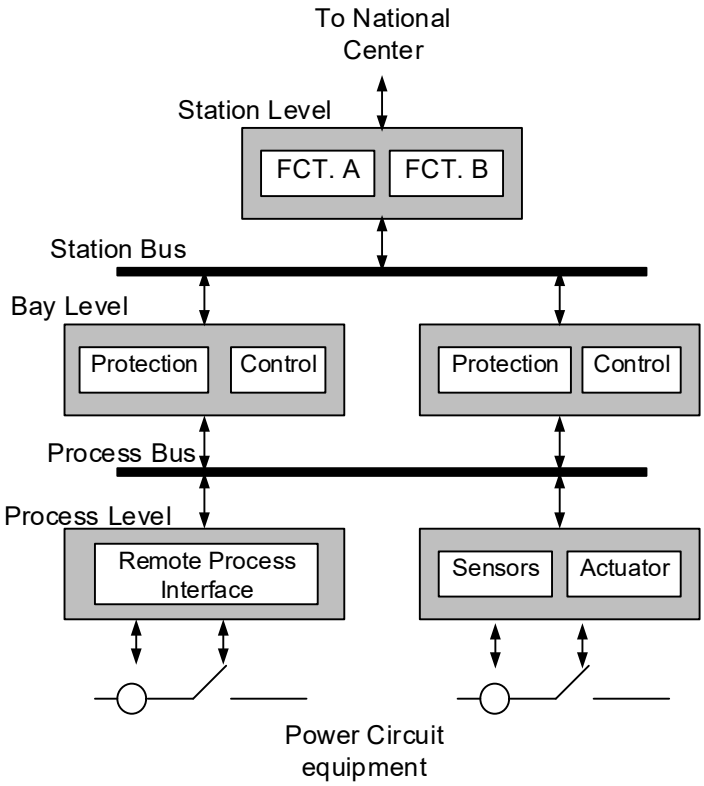


Figure 2-6: Levels of IEC 61850 Substation Communication Network [1]

The configuration of Figure 2-6 enables optimal communication between devices and communication to the substation control and monitoring centre through server/client configuration, resulting in shorter transmission times of substation messages on events occurring on request. In addition, IEC 61850 SCN aided SAS's functional configuration is suited for time-critical applications such as protection functions that require messages to be

transmitted immediately on an event occurring between substation devices [34]. The most complicated part of the SCN is the process bus comprising many hardware devices, software routers, firmware modules, and user-defined settings, making it challenging to fulfil the availability and performance requirements of the SCN according to [39]; this view is right mainly for purely transmission and distribution substations. However, in industrial plants where the primary plant interface is hardwired, the same view is not applicable since power distributions centres utilise metal-clad switchgear to distribute power to various parts of the plant and large motors. The following section discusses highly available SCNs protocols.

### 2.2.2 Active Redundancy in Substation Communication Networks

The application of Rapid Spanning Time Protocol (RSTP), according to IEEE 802.1w, prevents message flooding in SCNs by blocking messages in specific paths to prevent message circulation where ring architectures are used. However, the RSTP requires some time in milliseconds to seconds to reconfigure the network to use an alternative path to route messages in case of a link failure [30], [35]. The time required to reconfigure the network is dependent on the complexity of the SCN. Advancements in networking technology offer highly available industrial network communication protocols according to IEC 62439-3 with reliable data communication and deterministic recovery times. Even so, only the Parallel Redundancy Protocol (PRP) and Highly Available Seamless Redundancy (HSR) protocol offer seamless redundancy with zero network reconfiguration time.

The two protocols are based on the active redundancy principle, achieved by duplicating the information exchange according to IEC 62439-3, and therefore enabling the protocol to achieve zero network reconfiguration time in case of a link or switch failure, provided that both networks are operating successfully before the failure of one of the Local Area Networks (LANs). Parallel Redundancy Protocol (PRP) and Highly Available Seamless Redundancy (HSR) protocol are recommended in IEC 61850 Edition 2 in order to achieve seamless redundancy and zero recovery time in case of failure in a substation automation system [30], [35]–[37], [43], [44]. Figure 2-7 depicts generalized architectures of PRP and HSR SCNs.

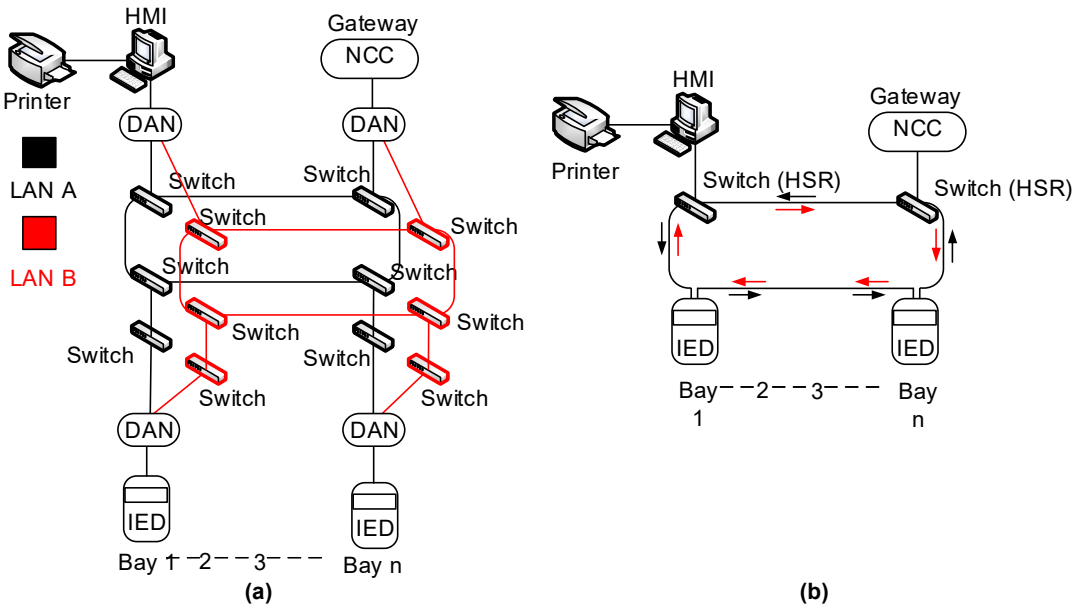


Figure 2-7: Parallel Redundancy Protocol and Highly Available Seamless Redundancy SCNs architectures [30]

The Parallel Redundancy Protocol (PRP) and HSR operate transparently in layer 2 of the OSI model. The protocols append a Redundancy Control Trailer (RCT) and Highly Available Redundancy tag (HSR Tag), respectively, to the pre-existing Ethernet frame as depicted in Figure 2-8 and Figure 2-9 [36], [39], [43].

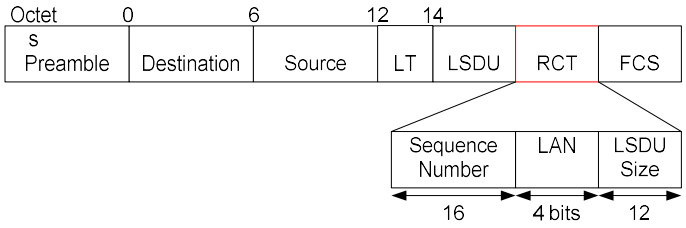


Figure 2-8: Redundancy Control Trailer (RCT) [43]

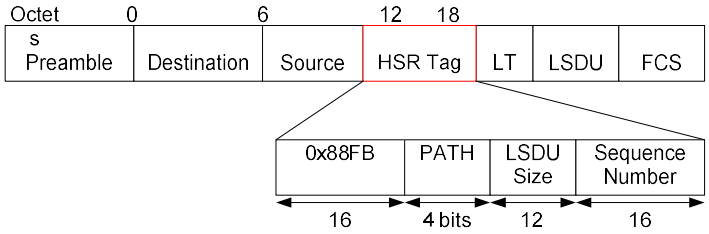


Figure 2-9: Highly Seamless Redundancy (HSR) tag [43]

The RCT is made up of sequence number, LAN identifier, frame size and PRP suffix, while the HSR Tag is made up of the Ethernet header, path, frame size and a sequence number [36], [39], [43]. However, implementing SCN architectures to achieve functional redundancy often results in sophisticated architectures, repercussions on development, operating and

maintenance cost, and should therefore be only considered for safety-related mission-critical functions such as critical protection applications [45], [46]. The following section presents safety-related systems in thermal plants.

## 2.3 Safety-related mission-critical systems

In thermal plants, auxiliary boiler loads such as fans, pumps and mills are supplied from medium voltage switchboards, where some of the fan motors are draught fan system motors protected by IEC 61508 and IEC 61511 safety-related and Safety Instrumented Systems (SIS) protection function loops in a boiler furnace [24]. The objective of SIS in a thermal plant is to protect against furnace explosion or implosion due to high or low pressure in case of process instability, where the most critical Safety Instrumented Function (SIF) is a Master Fuel Trip (MFT) [24], [47]–[49]. Legacy Safety Integrity Level (SIL) Safety Instrumented Systems (SIS) employed hardwired fail-safe circuits to implement SIFs in order to actuate final elements such as circuit breakers in medium voltage switchboards [39], [47], [50]. According to [49], [51], low demand SIFs are often sufficient for furnace pressure protection systems in the process industry in general, where the SIF is anticipated to operate once or less per annum.

The emphasis of IEC 61508 and its associated standards, such as IEC 61511, are both fail-safe design approaches and the reliability of safety-related systems, particularly safety instrumented protection functions [6]. IEC 61508 stipulates specific requirements and verification methods to satisfy safety instrumented protection functions concerning their reliability level. Even though IEC 61850 based SCN is the industry's preferred way of implementing protection, control, and monitoring substation equipment within power distribution centres, the industry is yet to be comfortable with the reliability of the system to fully apply it within industrial facilities, particularly for mission-critical applications [3], [6], [7], [27], [30], [31], [35]. Hence, IEC 61850 is expected to satisfy the IEC 61508 safety-related standard requirements as far as reliability is concerned with implementing Safety Instrumented Functions (SIFs).

## 2.4 Overview of the functional safety standard: IEC 61508

IEC 61508 is a standard for functional Safety of Electrical, Electronic and Programmable Electronic (E/E/PE) safety-related systems, and it has been in existence for over two decades. The safety lifecycle and Safety Integrity Level (SIL) of SISs are key concepts presented in the IEC 61508 standard [52]. The first publication of the standard was in 1998, following its original draft as IEC 1508 in 1995 [52], [53]. IEC 61508 Edition 2 was published in 2010 and is used as a global standard for the functional safety of safety-related systems [52], [53]. IEC 61508 is a standalone standard, and also a core standard from which IEC 62061 (machinery), IEC 61511 (process), IEC 61513 (nuclear) and IEC 61800-5-2 (power drives) are developed

[53], [54]. IEC 61511 addresses the sensor's dependability requirements and final element subsystems of a SIS irrespective of the technology used in the logic solver [54]. In the IEC 61508 standard, Parts 1 - 3 of the standard are normative, while the rest are informative [53]. Part-1 addresses general requirements for safety-related systems, Part-2 specifically deals with E/E/PE safety-related systems, and Part-3 focuses on software requirements [52], [53]. Normative means that the requirements should be complied with; therefore, emphasis should be placed on these parts of the standard to ensure compliance [53]. The standard ensures rationality and brings about consistency in the implementation of safety-related systems, of which their failure could impact life and damage to plant/property or environment. The standard also aims to standardise the approach to critical safety-related systems and provide verification guidelines regarding the compliance of SIFs to the standard [53], [55]. The IEC 61508 standard's approach to achieving functional safety requirements is through a safety lifecycle framework, as discussed in [9], [52]–[54]. The respective authors [9], [52]–[54] also discussed a detailed E/E/PE realisation lifecycle comprising both the requirements of safety functions and safety integrity according to the IEC 61508 standard. The overall safety life cycle covers the hazard and risks analysis, formulation of safety specifications and design requirements, overall planning and safety system realisation, installation and commissioning, and validation. Moreover, the scope covers operating and maintenance requirements and decommissioning of the safety system at the end of its life.

S. Kim et al. [56] states that software-based systems' low reliability and software integrity have resulted in many recalls by manufacturers in the past. In certain instances, recalls followed life-threatening incidences and damage to property. As a result, the development of highly reliable software-based systems is of high interest to developers and users. Hence, the realisation of the E/E/PE safety lifecycle is embedded in the overall system's safety lifecycle as depicted in Figure 2-10, which depicts a holistic overview of a process SIS that comprises the E/E/PE subsystem.

Phases 1 and 2 of the safety life cycle focus on the Equipment Under Control (EUC) system-level and its associated control system, wherein legislative, political, social, and physical implications resulting from unsafe state of the EUC to the surrounding environment are established. Analysis of potential risks and hazards associated with the EUC and or its control system is performed in phase 3 of the safety lifecycle. Phase 4 is concerned with the specification of safety requirements to avoid risks and hazards identified in phase 3. In phase 5, the safety system's transformation to design and performance requirements is performed [52], [53].

Phases 6, 7 and 8 are concerned with the safety life cycle's framework planning activities and installation, commissioning, validation, operating, and maintenance activities. Phase 6 focuses on the planning of operation and maintenance requirements of the safety system during

its lifespan. Therefore, this phase's outcome includes detailed operating and maintenance philosophies to ensure the safety system's effectiveness. Phase 7 addresses the planning of validation requirements, where the technical operating procedures are formulated to ensure the effectiveness and integrity of the test methods and inspections. Planning of the installation and commissioning activities concerning the safety-related system are addressed in phase 8 [52], [53], [57].

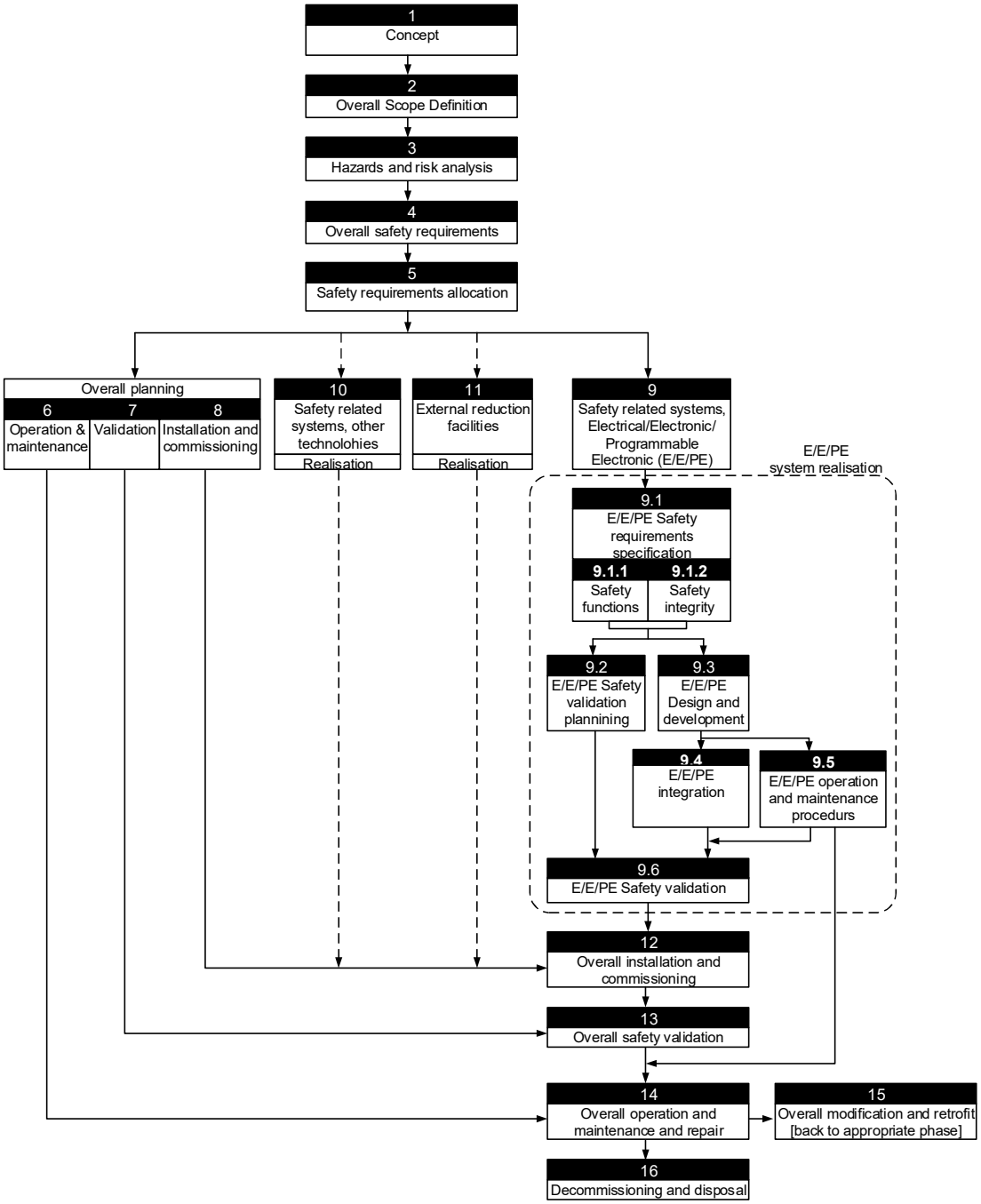


Figure 2-10: IEC 61508 Overall safety lifecycle [52], [53]

Phases 9 and 10 of the process focus on designing, analysing, and implementing safety-related systems. Phase 9 deals with E/E/PE based technologies, while phase 10 addresses other

technologies' realisation. In phase 11, the safety life cycle acknowledges that measures other than E/E/PE based technology safety systems can reduce risk. Since the IEC 61508 standard focuses on E/E/PE based technology systems, the lifecycle addresses the realisation of E/E/PE based system technologies as depicted in Figure 2-10 in phase 9. The realisation of E/E/PE based systems involves safety requirements specification, comprising safety functions and the associated integrity requirements. The realisation phase also includes safety validation planning, as well as design and development. All design and development activities are then integrated and validated together with the system operating and maintenance procedures to realise a complete functional E/E/PE based technology safety system [52], [53], [57].

Phase 12 focuses on the overall installation and commissioning of the safety system. It follows directly after the realisation of the safety system, where the installation and commissioning plan comes from phase 8 of the safety lifecycle on the overall planning stage of the lifecycle. In phase 13, the safety system's overall validation is performed after the system has been commissioned, where validation plans come from phase 7 of the overall planning phase of the safety life cycle. Phase 14 focuses on the overall operation, maintenance and repairs of the safety system during its lifespan. Similarly to phases 12 and 13, the overall operation and maintenance plan come from phase 6 of the lifecycle planning stage [52], [53], [57].

Phase 15 of the safety life cycle acknowledges that some form of system modification or retrofit may be required during the safety system's lifespan. Last is phase 16, which addresses the decommissioning and disposal requirements of the safety system hardware equipment at the end of its life [52], [53], [57]. R. Bell [53] presents a case study summary results looking into the causes of safety systems failures on their overall lifecycle. Although the study had low statistical significance according to the author, the results support the IEC 61508 standard in considering the overall safety lifecycle of safety-related systems since the cause of failures appears to be in all the lifecycle phases of the systems under study. However, more than 90% of Safety Instrumented System (SIS) failures can be attributed to sensors and final elements, where the incorrect specification of the SIS is the primary cause of functional safety failures [51], [53]; and therefore requires special attention during the requirements specification of safety systems. The following section reviews the dependability of a SIS.

## 2.5 Dependability of safety instrument systems

M. Magro et al. [4] defines safety as a concept of reducing the risk of physical injury or damage to a plant to an acceptable level. In [53], safety is defined as freedom from the unacceptance risk of physical injury or damage to people's health due to property damage or the environment. It is clear from the definitions of [4], [53] that physical injury and damage to property or environment are critical issues of interest, as stated in [45], [50], [51]. In [17], a

safety-related system is defined as any system that carries out the necessary function(s) to maintain a safe state of an Equipment Under Control (EUC). Moreover, [17] state that safety-related functions require real-time processing of commands to execute tripping of electrical circuits, as well as interlocking and closing circuits for changing-over supplies [23], [24], which can be achieved by deterministic characteristics of an Ethernet-based communication protocol where modern SCNs are used.

F. Redmill defines [52] safety integrity as a likelihood of a safety system to satisfactorily perform its intended function within a specified time, where the determination of acceptable levels of safety integrity for a specific plant risk profile is defined in IEC 61508. Functional safety is considered a sub-function of the overall safety concept; it depends on a system or equipment operating correctly according to [18], which defines a safety-related system as a system that carries out safety functions within a determined time. In addition, any system designed to provide a safety function necessary to achieve the safe state of the Equipment Under Control' (EUC) is classified as a safety-related system [52]; such systems are typically applied in high integrity pressure protection systems, such as boiler furnace system according to [9], [24].

In [48], [51], [54], Safety Instrumented System (SIS) is defined as a safety system comprising one or more SIF. A Safety Instrumented System (SIS) comprises three subsystems, as depicted in Figure 2-11, presenting a typical SIS reliability block diagram. Safety Instrumented System (SIS) is used in many industries to reduce risk to human life, plants, and the environment. In order to achieve this, E/E/PE based SIS technologies are used to detect process abnormalities and respond to the onset of hazardous events [9], [50], [58].

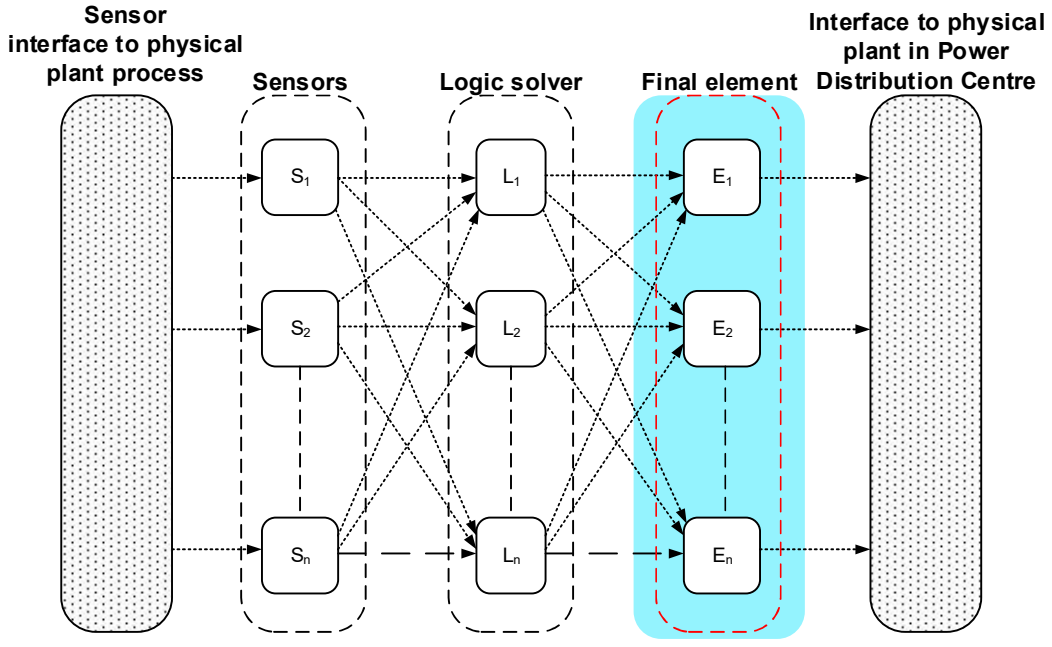


Figure 2-11: IEC 61508 safety instrumented system [51]

According to [9], [51], the lack of detail in the IEC 61508 safety lifecycle necessitates the use of Reliability, Availability, Maintainability and Safety (RAMS) studies in order to augment the safety lifecycle framework. Each SIF is performed by a SIS and is classified by SIL rating according to the IEC 61508 standard. Safety Instrumented Function (SIS) should be able to execute an emergency plant shutdown, as well as be able to fail-safe [48], [51]. In [54], Safety Integrity Level (SIL) is defined as a concept of measuring the level of dependability of a SIF to perform its intended function and therefore indicates the required level of reliability of a SIF.

In [56], a time factor is introduced in the SIF definition, where it is defined as the probability of a safety-related system to satisfactorily perform its intended function on demand within a specified time [56]. In the IEC 61508 standard, SIL is defined as a discrete measure for specifying an integrity level of an E/E/PE Safety Instrumented Function (SIF), where SIL 4 is the highest integrity level, and SIL 1 is the lowest integrity level [56], [59]. Each safety requirement should consist of a safety function of appropriate integrity level [6], wherein SIL rating can either be specified as low demand (PFD) or high demand (PFH). The difference between the two modes is that continuous mode continuously acts to keep the EUC in a safe state, while demand mode brings about the EUC to a safe state in case of process abnormality [9], [51]. Table 2-2 depicts the SIL rating classification based on PFDavg according to the IEC 61508 standard.

Table 2-2: Safety integrity levels ratings for safety functions [56], [60]

| Safety Integrity Level | Demand Mode of Operation | Continuous / High Demand |
|---|---|---|
| 1 | $10^{-5} \leq PFD_{avg} \leq 10^{-4}$ | $10^{-9} \leq PFD_{avg} \leq 10^{-8}$ |
| 2 | $10^{-4} \leq PFD_{avg} \leq 10^{-3}$ | $10^{-8} \leq PFD_{avg} \leq 10^{-7}$ |
| 3 | $10^{-3} \leq PFD_{avg} \leq 10^{-2}$ | $10^{-7} \leq PFD_{avg} \leq 10^{-6}$ |
| 4 | $10^{-2} \leq PFD_{avg} \leq 10^{-1}$ | $10^{-6} \leq PFD_{avg} \leq 10^{-5}$ |

The ever-increasing complexity of industrial control and protection systems and associated SIS necessitates diagnostic tools to ensure the plant's safety, reliability, availability, and performance. The diagnostic system detects SIS failure or errors in the system, allowing corrections and repairs to be carried out in time to improve the system's availability. The diagnostic system can either be passive or active, depending on the process's criticality. Passive diagnostic means that the system only executes on demand, while active diagnostic system continuously executes to check for errors on the system; the latter is most recommended for high rated SIL SIFs [28], [39], [51], [58].

In [58], [60], the authors highlighted that the Probability of Failure on Demand (PFD), according to the IEC 61508 standard, allows various reliability models to be used. However,

the approach taken by the standard assumes that a SIS is fully functional at time $t = 0$ and that its functionality is fully restored after every maintenance activity. Therefore, this assumption implies that all Proof Tests (PT) are 100% complete and performed correctly according to applicable procedures; therefore, all faults and errors have been detected and removed after every Proof Test (PT). The position presented by the IEC 61508 standard simplifies the reliability computation effort. However, the assumptions are not always valid in practice, even though they are most desirable.

In [30], [51], SIL reliability studies that considered multiple factors such as Diagnostic Coverage (DC), proof test interval, CCF factors, diagnostic system success factor, as well as correctness and completeness of each proof test were conducted. The studies show that the SIL of SIS reduces every time a Proof Test (PT) is performed, causing the overall integrity to degrade over time. This finding is critical and may be used to determine a SIF's useful life. In order to measure the effectiveness of maintenance activity, R. Sekiou et al. [51] introduced a concept of Proof Test Effectiveness (PTE) that considers both completeness and correctness factors of a Proof Test (PT) performed on a SIF as presented in (2-1),

$$PTE = \frac{PFD(T_1 - 1) - PFD(T_1)}{PFD(T_1 - 1)} \tag{2-1}$$

Where PFD(T1-1) is a probability of failure on demand at time $t$ just before a Proof Test (PT) and PFD(T1) is a probability of failure on demand at time $t$ just after a Proof Test (PT). The safety-related system's selected safety integrity should be such that it limits the safety system's failure to an acceptable level and prevents adverse failure that could result in an intolerable risk occurring [53]. The Safety Integrity Level (SIL) of a SIS can be improved by using a redundant design, according to [9]. However, [56] states that although redundancy can improve reliability, it cannot improve a system's safety. Therefore, design principles cannot be substituted by redundant systems. It, therefore, follows that reliability is a subset of safety. Accordingly, developers of software-based systems aim to conform to the functional safety standard IEC 61508 [56]. In [52], it is stated that the EUC risk shall be evaluated or estimated for each determined hazardous event. Furthermore, the risk level can be determined using qualitative or quantitative methods, wherein guidelines are provided in the IEC 61508 standard.

## 2.6 Determination of SIL rating for Safety Instrumented Functions

IEC 61508 standard adopts a risk-based approach to determine a SIL rating of SIFs and requires that each safety function's performance be determined, wherein the risk assessment approach considers both the probability and consequences associated with the process abnormality [53], [54].

A guideline for determining a SIL level of homogeneous systems is presented in the IEC 61508 standard. However, safety instrumented systems are generally heterogeneous. Therefore, the SIL verification for heterogeneous systems based on the IEC 61508 standard guideline may be inadequate [59]. Redundant and complex SIFs are continuously implemented in industries. The main objective is to achieve high dependability to avoid or lessen the effects of process abnormalities. Redundancy is a widely used technique to improve the reliability and availability of safety-related systems, where the system's high availability must be maintained to guarantee availability on-demand [51]. However, redundancy also introduces other factors such as voting consideration and Common Cause Failures (CCF); which have the potential to nullify the redundant nature of the system by bringing down all the channels of the system at the same time [20], [45], [51], [59].

A Common Cause Failure (CCF) is defined as a type of failure where a single failure results in multiple components and or subsystems failing within a specified time such that the dependability of the system would be uncertain. The IEC 61511 (2003) standard, which is the safety standard for the process industry, defines a CCF as a "*failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure*", which is possible to occur in a digital-based SIS [45], [47]. The complexity of a SIS is worsened by introducing diversity in redundancy, which results when different components, algorithms, electronics, design methodology, etcetera, perform the same task. The application of diverse redundant technologies increases the SIS's capabilities to reduce common causes of failures and systematic failures due to design flaws. Diversity, therefore, is recommended to ensure that systematic and hardware flaws are not introduced to redundant systems. Moreover, CCFs can be avoided by ensuring that redundant systems are located in separate locations, ensuring that they are not exposed to the same physical stress and functional independence between redundant channels. The impact of CCF can be investigated by qualitative analysis to demonstrate compliance with the CCF criterion set for the SIS [45], [47].

N. Lui et al. [9] presents a qualitative evaluation method of a SIS hardware using Failure Mode Effect Diagnostic Analysis (FMEDA). The approach can determine dangerous failures in a system as a bottom-up approach. The approach also identifies what failures need to be revealed during a functionality proof test, which is most desirable to ensure that SIS errors and failures are corrected at each Proof Test (PT). However, the approach does not produce a holistic state of the system since it cannot evaluate the hardware components' reliability; complementing the method with a quantitative analysis method would produce a holistic system state.

The Funnel Risk Graph Method (FRGM) and Layer of Protection Analysis (LOPA) approaches can be used to determine a SIL of a safety system. The FRGM is qualitative, while

LAOP is a semi-quantitative method. The FRGM method is economical and straightforward but inaccurate for higher SIL rated systems. The results of FRGM also depend on the people conducting the risk assessment to derive a SIL rating; thus, the results may be subjective [54], [55]. The results of FRGM are said to be comparable to Event Tree Analysis (ETA) and semi-quantitative methods based on LOPA for lower SIL rated systems, according to the authors in [54], [55].

## 2.7 Reliability evaluation of Safety Instrumented Functions

Numerous reliability evaluation methods [9], [20], [59], [60] have been used to evaluate the SIL rating of E/E/PE based Safety Instrumented Systems. In [9], fuzzy probabilistic and the RBD are used to determine a SIF rating within a Safety Instrumented System. However, this approach lacks the capability of evaluating state transitions on the system. In [9], [20], SIL verification of a SIF using the RBD, Fault Tree Analysis (FTA) and Simple Equations (SE) are said to cover few aspects of the system's safety behaviour since they only consider failure rates; and do not consider the effects of repair rates in the form of components and subsystems state transitions, as well as system degradation.

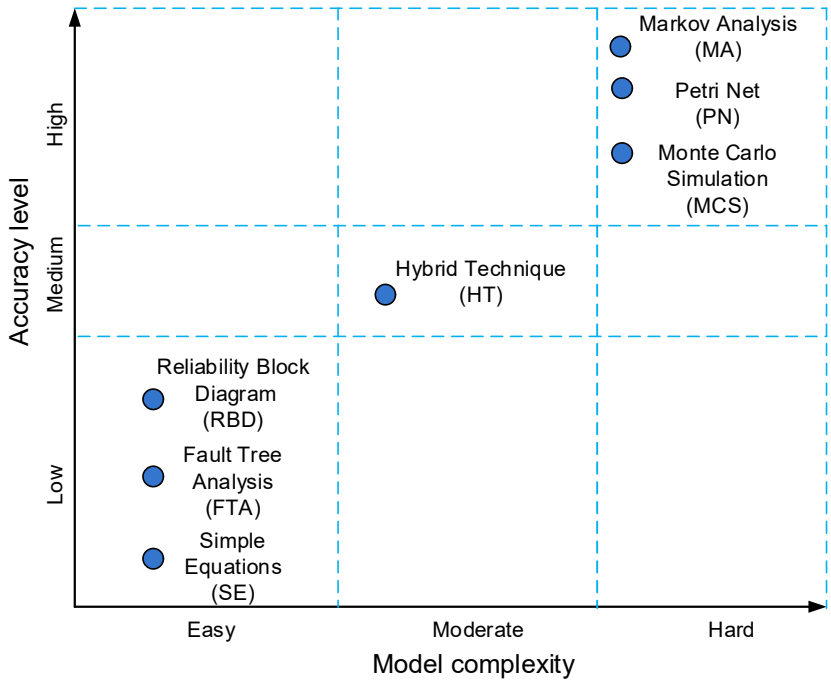


Figure 2-12: SIL verification complexity and accuracy of reliability analysis methods [20]

Hence, these methods are said to be inadequate for SIL verification of SIFs. The authors in [9], [59] proposed an analytical approach and Markov process modelling as the best method that considers system state transition caused by repair rates and system degradation. However, it is acknowledged in [20]; that the Markov process method is intensive and complex, along with Petri Nets and Monte Carlo Simulation. In [60], a simplified Markov process model is

used to study the reliability of a SIS considering the impact of Proof Test (PT) effectiveness under the influence of PT correctness and completeness and diagnostic coverage. In this study [60], the Markov process' capability to evaluate system state transitions is demonstrated. Figure 2-12 depicts the accuracy versus the complexity of various SIL verification techniques [20]. Therefore, the evaluation of a system SIL rating should aim to consider both systematic and hardware probability of failure, as well as state transition of safety systems in order to produce a holistic dependability state of a SIS, achieved by using quantitative and qualitative techniques [9], [52], [58], [60]. The next section reviews the reliability studies of IEC 61850 based SCNs.

## 2.8 Reliability evaluation of IEC 61850 based Substation Communication Network

The Reliability Block Diagram (RBD) method and mathematical analysis are used in the studies presented in [37], [61]–[74] to study the reliability and availability of IEC 61850 based SCN; while Optimised Network Engineering Tools (OPNET) software is used to investigate data transfer efficiency. The RBD method assumes that all system faults are identified and fully repaired [75], which is not necessarily the case in practice [2], [8]. Hence, the approach may lead to inaccurate results concerning the performance of the system. Moreover, the introduction of new technologies with onboard system diagnostic capability require unique expertise to ensure that faults are identified and fully repaired [2]. Nevertheless, these aspects have not been considered by the studies presented in [36], [37], [61]–[65], [67]–[74].

Another area of interest that is investigated in the studies is network recovery time. This aspect is applicable in redundant systems where one of the SCN links can fail. The studies presented in [36], [37], [62]–[65], [67]–[74] investigated the application of Parallel Redundancy Protocol (PRP) and Highly-available Seamless Redundancy (HSR) to resolve the problem associated with the network recovery time. The drawbacks of PRP and HSR protocols are high cost and high traffic, respectively. In [76], an algorithm that can minimise traffic congestion in HSR without affecting the protocol's functionality is presented and discussed. However, these studies do not consider the impact of the availability of practical skills and system diagnostic capabilities required to ensure that the desired system performance regarding reliability and availability is maintained during the system’s useful life [2]. It can be inferred that the studies assume that all system faults are identified and fully repaired since the studies in [32], [65], [67] used RBD and OPNET simulator as the primary method and simulation tool, respectively.

Various modelling techniques are used to study the reliability and availability of industrial systems. One method estimates parameters for different variations of Weibull distribution to obtain a proper fit for reliability distribution; this approach is well suited for systems where the hazard rate changes over time [75], [77]. In complex repairable systems, stochastic

modelling techniques are suitable where failures are random [2], [78]–[80]. Although combinatorial analysis modelling methods are practically simple and easy to apply, their application's drawback is to model complex state dependencies and the inability to include all combinations of scenarios, as discussed in section 2.7. In a FTA approach, for instance, the objective is to predict the likelihood of one event; therefore, multiple Fault Trees (FT) are needed if there is more than one failure event which makes the approach cumbersome [2], [81]. Monte Carlo Simulation can be employed to study multi-channel systems' reliability; yet, a high number of simulation cycles is desirable to obtain statistically meaningful outcomes. In addition, minor system modifications need the simulations to be rerun at a significant cost [2], [74], [81]. The Markov process method includes sequence-dependent events naturally in the model and, therefore, does not have the limitations cited above [2], [81].

Hardware repairs are constrained by failure detection, skills and the capacity to perform repairs in electronic systems and computational systems in general. The Markov process' modelling flexibility allows maintenance policies and safety consideration and self-testing in digital protection schemes to be investigated to determine their impact on system reliability [81]–[83]. Markov Chain analysis can model the impact of failed undetected components on the dependability of the system. Moreover, Markov modelling can also be used to model complex schemes where different devices and technologies with specific maintenance strategies are used on respective channels of reparable multi-channel systems to eliminate CCF [20], [54], [58], [83], [84]. According to [85], the Markov process's disadvantage is that failures are assumed to be purely stochastic [75]. Even so, the benefit associated with the level of simplification of analysis outweighs the assumption [13], [15], [80], [86].

## 2.9 Suitability and flexibility of reliability models

A mission-critical system's reliability performance must be modelled with high accuracy to ensure its performance level [8]. It is clear from the review presented by L. Ding et al. [20] that anyone of the Markov process, Petri Nets and Monte Carlo Simulation methods can be considered to investigate the reliability of a mission-critical system, as depicted in Figure 2-12. Even though the three Simulation methods offer high accuracy, consideration concerning their flexibilities, complexity level and ease of implementation in modelling systems' reliability is needed. Petri Nets offers both state and transition modelling using places and arcs [75], [87]. However, the method does not consider time and requires further translation into stochastic Petri Nets to simulate discrete systems, whereas the Markov process can naturally model discrete and continuous times [8], [88]. Moreover, there is still insufficient information about the utilisation of Petri Nets application integration than the Markov process, which is commonly used to investigate safety-related systems' reliability [20], [75], [89].

In contrast to the Markov process, the Monte Carlo Simulation method can model various individual parameter failure distributions by sampling multiple parameter values for computation, making it more flexible than the Markov process. Nevertheless, the said flexibility is not needed during the system's useful life, where only exponential distribution is considered for E/E/PE systems. The Markov process offers more comprehension of the system dynamics' insights through its transition probability matrix. The transition probability matrix enables various theoretical concepts to investigate the behavioural characteristics, including transient and asymptotic system response to system parameter changes [13], [15], [16]. The seamless transformation of the transition probability diagram into a transition probability matrix allows the integration of varied system parameters, enabling a holism approach to studying the interaction of a system's subsystems, its environment, and human intervention through Systems Thinking [8], [75], [90], [91]. In addition, unlike the Monte Carlo Simulation, where a high number of simulations are required to obtain statistically meaningful results, the same is not true for the Markov process using mathematical analysis of the transition probability matrix based on dynamical system studies and calculus methods [13], [15], [16]. Hence, the Markov process is the most suitable for studying mission-critical safety-related systems' reliability during the system's useful life because of its flexibility and accuracy, yet simple to implement than Petri Nets and Monte Carlo Simulation methods.

## 2.10 Chapter conclusion

An overview of SCN standard IEC 61850 is presented in the literature review. It is evident that the standard, aided by the real-time deterministic transmission of GOOSE protection application messages, can be considered to implement SIS to complete the digitalisation of power distribution centres. Detail experimental analysis of IEC 61850 GOOSE message transmission shows that it complies with IEC 61784-3 regarding error detection capability. Various reliability techniques have been used to evaluate IEC 61850 based SCNs, where the majority of the studies employed combinatorial analysis techniques such as the RBD, FTA and SE. However, the methods cannot accurately evaluate the reliability of multi-state systems resulting from E/E/PE technologies. Markov Chain analysis method is found to have the capability to naturally model sequence-dependent events and, therefore, well suited to evaluate multi-state systems' reliability.

In some cases, the Markov process has been used to evaluate the reliability and availability of IEC 61850 based SCN. However, the studies do not consider the effect of Diagnostic Coverage (DC), Proof Test (PT) and Proof Test Coverage (PTC), as well as PT correctness and PT completeness that collectively impact the quality of repairs; whereas the factors impact the reliability of E/E/PE based systems. Therefore, it is concluded that the studies presented in the literature do not present a holistic view of the reliability of IEC 61850

based SCN for use to implement SIS according to IEC 61508 in a digitalised power distribution centre because the methods do not consider repair efficiency and diagnostic coverage. Thus, in this thesis, the Markov process is used to model the reliability and availability of IEC 61850 SCN due to its flexibility in integrating system diagnostic coverage and repair efficiency (viz. completeness and correctness of repairs). In addition, the approach enables the system repair philosophy to be easily integrated into the model.

# CHAPTER 3

# RESEARCH METHODOLOGY

## 3.1 Introduction

This chapter presents the methodology followed to investigate the reliability of IEC 61850 mission-critical SCN based on a stochastic model using the Markov process. The Markov process enables the system state's interactions to be included in the reliability performance analysis model [2], [8], [75]. The impact of human intervention in substation communication systems during the design and maintenance stages is also integrated into the reliability model using Systems Thinking, which allows the system and its environment to be investigated as a whole. Studying the system based on holism's approach reveals the actual system dynamics and its performance based on the mean state transitions and the system's transitioning behaviours [8], [92]. The mean state transitions on the system are estimated using mathematical expectation studies of the system's transitioning states based on the transition probability matrix [8], [75].

The impact of Common Cause Failures (CCFs) is investigated by integrating the β-factor model into the Markov process model, where the transition failure rate due to CCFs impact is considered a percentage of the system's overall failure rates [93], [94]. The system's dynamics are investigated by introducing Markov partitions based on the structure-function modelling to study the state transitioning patterns considering a finite set of symbols representing the system's transitioning behaviour as chaos is generated in the context of linear dynamical systems. Linear dynamical systems' theory enables the system's dynamics to be studied based on the state transition probability matrix's eigenvalues' responses to various system parameters [13], [95]. Sensitivity and elasticity studies are then used to determine the transient system's response based on absorbing Markov chain process and matrix calculus methods through matrix similarity concept, which complements the asymptotic approach offered by the eigenvalue analysis method [15], [16], [96]. MATLAB programming software is used to develop the reliability models presented in this thesis and the simulation results' presentation, wherein the main program scrips of the models are presented in Appendix A.

Section 3.2 discusses the concepts of reliability and availability evaluation, including the derivation of the reliability function and presents essential reliability and availability formulae. Section 3.3 discusses the modelling of the quality of repairs based on the Markov process incorporating Systems Thinking. System dynamics analysis is discussed in section 3.4. Preliminaries and notation of matrix calculus used in the thesis are presented in section 3.5, while section 3.6 discusses the research work's boundaries and limitations. The summary of the research methods used is presented in section 3.7.

## 3.2 Reliability and availability evaluation concepts

The research work considers the system performance and behaviour during its useful life when the individual subsystems' failure rates are assumed constant. In multi-channel systems, the focus is on a group of components or subsystems that causes the system's state to change when one of the subsystems' components fail or is restored to functionality. Hence, a group of components or subsystems whose failure and repairs results in the loss of (or full) functionality of the group are modelled as one subsystem comprising a failure rate (λ) and a repair rate (μ) [8], [75]. The failure rate function λ(t), also referred to as the hazard rate function, is the most commonly used function to express component or system reliability. Substation communication devices based on Electrical, Electronic and or Programmable Electronic (E/E/PE) components exhibit a constant failure rate during their normal useful operating life, which is observed to be region II of the bathtub curve as depicted in Figure 3-1 [28], [75]. Regions I and III of the bathtub curve represent a decrease and increase of component failure rate caused by early bug fixes and ageing or worn-out components, respectively.

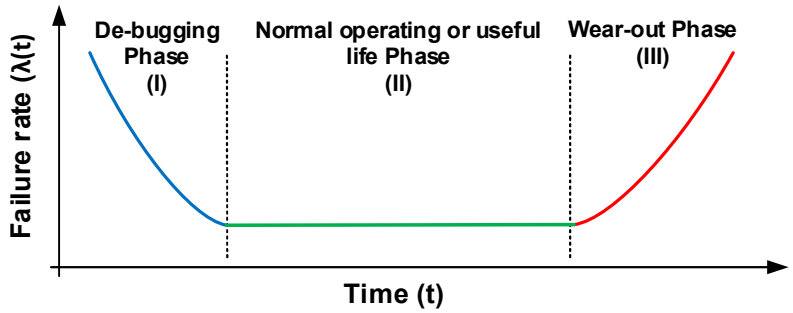


Figure 3-1: Typical electronic component hazards failure rate as a function of age [75]

Considering the failure rate to be constant during the system's useful life, exponential and poison distributions can be used to model the failure rate of E/E/PE components. Poison distribution gives the probability of an event's occurrences within a specified time interval, while exponential distribution is concerned with the time distribution between successive event occurrences as time progresses continuously; hence exponential distribution is used in this research [28], [75]. The following section presents the reliability function's derivation to offer appreciation and comprehension of the underlying assumptions.

### 3.2.1 The reliability functions

Reliability is defined as the probability that a system satisfactorily performs the intended purpose within a specified time, denoted as $R(t)$ at time $t$. Similarly, the probability of failure at time $t$ is denoted as $Q(t)$, where $Q(t)$ is the complementary of $R(t)$ as given by (3-1),

$$R(t) = 1 - Q(t) \tag{3-1}$$

In reliability studies, the rate of change of the cumulative failure distribution $Q(t)$ gives the failure density function $f(t)$ given by (3-2) [75], [97],

$$f(t) = \frac{dQ(t)}{dt}$$

$$f(t) = -\frac{dR(t)}{dt} \tag{3-2}$$

Alternatively,

$$Q(t) = \int_0^t f(t)dt \tag{3-3}$$

Mathematically, considering a case where $N_o$ is the fixed number of identical components under test, and letting $N_s(t)$ and $N_f(t)$ to be a number of surviving and failed components at time *t* respectively, it follows that the sum of $N_s(t)$ and $N_f(t)$ equal $N_o$. Thus, the reliability of the components $R(t)$ is given by (3-4),

$$R(t) = \frac{N_S(t)}{N_o} \tag{3-4}$$

Which can be written as,

$$R(t) = \frac{N_o - N_f(t)}{N_o}$$

And simplifies to,

$$R(t) = 1 - \frac{N_f(t)}{N_o} \tag{3-5}$$

Therefore, the probability of failure of the components is given by (3-6)

$$Q(t) = \frac{N_f(t)}{N_o} \tag{3-6}$$

Furthermore, considering a component's reliability $R(t)$ and the probability of failure $Q(t)$ given by (3-5) and (3-6) respectively, the rate of change of reliability is given by (3-7),

$$\frac{dR(t)}{dt} = -\frac{dQ(t)}{dt}$$

Which can also be written as,

$$\frac{dR(t)}{dt} = -\frac{1}{N_o}.\frac{dN_f(t)}{dt} \tag{3-7}$$

As $dt$ approaches zero, the failure density function (3-2) can be expressed by a function $f(t)$ as given by (3-8),

$$f(t) = \frac{1}{N_o}.\frac{dN_f(t)}{dt} \tag{3-8}$$

In addition, defining the hazard rate λ(t) as the ratio of the number of failures per unit time over the number of components exposed to failure, to measure the rate at which failure of a component or system occurs [28], [72], [75], then (3-9) gives the hazard rate,

$$\lambda(t) = \frac{1}{N_S(t)}.\frac{dN_f(t)}{dt} \tag{3-9}$$

In addition, it can be shown that (3-9) can be written in the form of (3-10),

$$\lambda(t) = -\frac{1}{R(t)}.\frac{dR(t)}{dt} \tag{3-10}$$

Where (3-10) simplifies to:

$$\int_1^{R(t)} \frac{1}{R(t)}.dR(t) = \int_0^t -\lambda(t)dt$$

Hence,

$$lnR(t) = \int_0^t -\lambda(t)dt$$

Which also simplifies to (3-11),

$$R(t) = exp\left[\int_0^t -\lambda(t)dt\right] \tag{3-11}$$

Therefore, in a special case where the failure rate function λ is constant and independent of time, (3-11) simplifies to (3-12) [75].

$$R(t) = e^{-\lambda t} \tag{3-12}$$

The following section presents the generalised reliability and availability functions used in the following chapters and forms the basis of the transition rates of the various system states transition discussed in section 3.3.

### 3.2.2 Generalised reliability and availability functions

A system's reliability is a function of its subsystems or components, considering the individual subsystems or components' configuration. Hence, if the failure rate is constant, as discussed in section 3.2.1, then the reliability function of the $i^{th}$ component is given by (3-13) [72], [75], [97].

$$R_i(t) = e^{-\lambda_i t} \tag{3-13}$$

Where $i$ represents the $i^{th}$ component, $\lambda$ is the failure rate function, $t$ is the mission time. The mean time to failure (MTTF) and availability of a component or subsystem is given by (3-14) and (3-15), respectively. The $i^{th}$ component's Mean Time To Repair (MTTR) is designated by $MTTR_i$ [72], [75], [97],

$$MTTF_i = \int_0^\infty R_i(t)dt$$

Which simplifies to,

$$MTTF_i = \frac{1}{\lambda} \tag{3-14}$$

$$A_i = \frac{MTTF_i}{MTTF_i + MTTR_i} \tag{3-15}$$

The Reliability Block Diagram modelling method is used to model a group of components where any one of the group's components' failure causes the system's state to change. The method depicts the logical connections of system components needed to successfully perform a function [28], [72], [75]. Components needed to perform a function are connected in series, while redundant components are connected in parallel [28], [72], [75]. Figure 3-2(a) depicts the components or subsystems connected in series, where the system's reliability, MTTF, and availability, are respectively given by (3-16), (3-17) and (3-18); which form the basis of the reliability evaluation method used at subsystem level based on the selected grouping of the various system components.

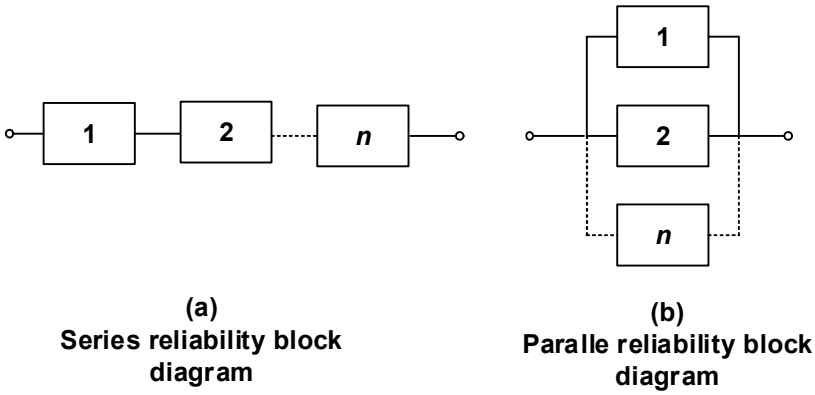


Figure 3-2: Series and parallel subsystems [28], [72]

$$R(t)_s = \prod_i^n R_i(t)$$

Which simplifies to,

$$R(t)_s = e^{-(\sum_i^n \lambda_i)t} \tag{3-16}$$

And,

$$MTTF_S = \int_0^\infty R_s(t)dt$$

Which also simplifies to,

$$MTTF_S = \frac{1}{\lambda_1 + \lambda_2 + \cdots + \lambda_n} \tag{3-17}$$

Whereas,

$$A_s = A_1.A_2 \tag{3-18}$$

Figure 3-2(b) shows the Reliability Block Diagram (RBD) comprising parallel components or subsystems. System reliability, MTTF, as well as availability for two components are respectively given by (3-19), (3-21) and (3-22).

$$R_p = 1 - \prod_{i=1}^n Q_i(t) \tag{3-19}$$

Where the system parameter $Q_i(t)$ is the unreliability of the subsystem given by (3-6),

$$Q_i(t) = 1 - e^{-\lambda_i t} \tag{3-20}$$

$$MTTF_p = \int_0^\infty R_p(t)dt$$

Which can also be written as,

$$MTTF_p = \frac{1}{\lambda_2} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2} \tag{3-21}$$

$$A_p = A_1 + A_2 - A_1.A_2 \tag{3-22}$$

Hence, it follows that the unreliability of a system is given by (3-23)

$$Q_{sys}(t) = 1 - R_{sys}(t) \tag{3-23}$$

Therefore, equations (3-13) to (3-22) can be used to determine the reliability and availability of a system based on the RBD analysis method [28], [72], [75]. The following section presents the Markov chain process used to model the system's reliability at the highest level of system abstraction incorporating quality of repairs and CCFs.

### 3.3 System reliability with imperfect repairs based on the Markov process

The Markov Chain (MC) process is used to model the system state transitions due to subsystem failures and repair activities in IEC 61850 based SCN reliability study presented in this work [98]. Markov modelling is a pliable, graphically-assisted quantitative evaluation technique that can be used in the design for reliability performance decision making and verification of system design to satisfy intended objectives and optimisation of maintenance strategies for complex dynamic systems [75], [78], [81]. The transitioning rates between the various states of the system are exponentially distributed [82]. Since the failure rates of E/E/PE systems are considered constant during the system's useful life and follow the exponential distribution [3], [44], [72], [75], a stochastic state transition probability matrix can be generated, where a stochastic process is a family of random variables $\{X_n\}$, for $n$ = 1, 2, 3, … [79]. A random variable $X_n$ with a value $x_n$ at the time $n$ is referred to as the state of the random variable at that point in time. Therefore, all possible values that the random variable $X_n$ can assume form the state space $S$ of the system. According to Markov process, the value of a random variable $X_{n+1}$, is entirely dependent on the previous value $x_n$ of random variable $X_n$, such that the next system state is defined by (3-24) [91],

$$[X_{n+1} = x_{n+1} | X_1 = x_1, X_2 = x_2, \ldots., X_n = x_n]\, P\left[X_{n+1} = x_{n\_1} | X_n = x_n\right] \tag{3-24}$$

Therefore, a transition probability matrix of a state transition diagram depicted in Figure 3-3 can be generated as presented in (3-25),

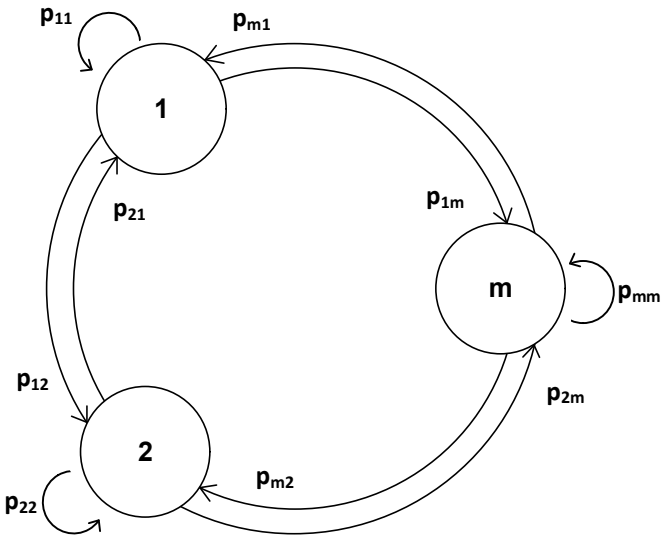


Figure 3-3: Generalised Markov process transition diagram [8], [75]

$$P = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \vdots & \ddots & \ddots & \vdots \\ p_{m1} & p_{m2} & \cdots & p_{mm} \end{pmatrix} \tag{3-25}$$

Where $P_{jk}$ is the transition probability from a random state variable $X_n$ to a random state variable $X_{n+1}$. Hence, (3-26) holds according to the Markov process [75], [91],

$$P(n) = P(0)P^{(n)} \tag{3-26}$$

Where $n$ in (3-26) is the number of state transitions, and $P(0)$ is the initial state distribution vector. The state transition probabilities of the system can be determined using the Markov ratio property, which states that for *n* number of events to occur in the next time step, the $i^{th}$ event's probability of occurrence is given by (3-27) [78],

$$\Pr\left(i^{th} \text{ is the first event}\right) = \frac{\lambda_i}{\lambda_1 + \lambda_2 + \cdots + \lambda_n} \tag{3-27}$$

Where the $i^{th}$ failure and repair transition rates between the respective states of the system are given by (3-28) and (3-29) [75], [78],

$$\lambda_i = \frac{1}{MTTF_i} \tag{3-28}$$

$$\mu_i = \frac{1}{MTTR_i} \tag{3-29}$$

The Markov chain states are determined using a structure-function modelling approach, assuming that each subsystem is in one of the functional or non-functional states at any given point in time and not both states. The structure-function modelling of the system's states and the associated hypotheses are discussed in Chapter 4. The integration of system repair efficiency and diagnostic coverage based on Systems Thinking is also presented in Chapter 4, wherein the preliminary results of the impact of repair efficiency and diagnostic coverage are presented and discussed. The β-factor modelling approach is used to model the impact of common causes of failure in Chapter 5 by modifying the Markov model to enable the impact of common causes of failure to be investigated at various system parameter levels. The following section discusses the concept of linear dynamical systems.

### 3.4 Systems dynamics and performance

The system's state transitioning patterns are investigated by characterising the system's trajectory movements based on linear dynamical systems. This section defines the main concepts used in Chapter 6 to study the system's dynamics, considering its movements as a series of finite symbols. At the highest level of system abstraction, it is considered that the next system's state is only dependent on the current state based on some rule, such that the next system state is given by (3-30), assuming that $x$ is a vector in $R^n$, where $n$ represents the dimension of the system if a linear map exists such that $X: R^n \to R^n$ [13], [95], [99], [100].

$$x_{n+1} = X(x_n) \tag{3-30}$$

Hence, given $X: R^n \to R^n$ as a linear map, its matrix form is given by (3-31) [99],

$$X(x) = \begin{pmatrix} X_1(x_1, \dots, x_n) \\ \vdots \\ X_n(x_1, \dots, x_n) \end{pmatrix} \tag{3-31}$$

Hence, (3-31) can also be written in the form of (3-32),

$$X(x) = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \tag{3-32}$$

So that (3-30) simplifies to (3-33),

$$x_{n+1} = X(x_n) = Cx_n \tag{3-33}$$

where $C$ is the coefficient matrix comprising of the elements $(c_{ij})$. Hence, any change to the system variables based on some new variable requires the expression of $x_i$ (for $i = 0, \dots, n$) given by (3-34) [95], [99],

$$x_i = \sum_{j=1}^{n} m_{ij} y_j \text{ for } i = 0, \dots, n), \tag{3-34}$$

which may also be expressed as given by (3-35),

$$x = My \tag{3-35}$$

where $m_{ij}$ is a real constant $\forall$ $i$ and $j$, implying a bijection such that $M$ is a non-singular matrix. Thus, the columns $m_i$ of $M$ are linearly independent. Hence, $x$ is given by (3-36),

$$x = \sum_{i=1}^{n} y_i m_i \tag{3-36}$$

It follows, therefore, that (3-33) simplifies to (3-37),

$$x_{n+1} = My_{n+1} = CMy_n \tag{3-37}$$

Consequently,

$$y_{n+1} = By_n, \tag{3-38}$$

if $A$ and $B$ are similar matrices, such that

$$B = M^{-1}CM, \tag{3-39}$$

where the matrix $B$ is the Jordan form of matrix $A$ [95], [99], [101]. The concepts and applications of matrix similarity and the Jordan form matrices to studying system dynamics are discussed in Chapter 6. The following section presents the preliminaries and notation of matrix calculus methods used to study system sensitivity and elasticity in Chapter 7.

### 3.5 Preliminaries and notation of matrix calculus methods

The absorbing Markov Chain process and matrix calculus methods are used to study the system's responsiveness to repairs' quality in Chapter 7, wherein the absorbing Markov chain process is introduced in Chapter 4. This section focuses on the preliminaries of derivatives and notations concerning matrices. Matrix calculus enables orderly differentiation of various forms of valued functions, including scalar, vector and matrices. Among several conventions of matrix calculus methods, vector arrangement is used in this research because it is conceptually simple to comprehend and logical to apply [102]–[105]. In addition, the vector

arrangement is implementable in software packages without losing its formation. This aspect lessens the required level of effort to present, interpret and analyse the results. Henceforth, the notation used to represent scalars is non-bold non-capital letters, while vectors are represented by bold non-capital letters. Matrices are represented by bold capital letters.

### 3.5.1 Derivatives

The derivative of a function $y$ with respect to $x$ is given by $\frac{dy}{dx}$, if both $x$ and $y$ are scalars. If the function $\boldsymbol{y}$ is a vector and $x$ a scalar, the derivative of the function $\boldsymbol{y}$ with respect to $x$ is given by a $n$ x 1 vector (3-40), where $n$ is the length of the vector function $\boldsymbol{y}$ and $\boldsymbol{b}^{\mathrm{T}}$is a transpose of $\boldsymbol{b}$,

$$\frac{d\boldsymbol{y}}{dx} = \left(\frac{dy_1}{dx} \dots \frac{dy_n}{dx}\right)^T \tag{3-40}$$

If the function $y$ is a scalar and $\boldsymbol{x}$ a vector, the derivative of the function y with respect to $\boldsymbol{x}$ is given by a 1 x $m$ gradient vector (3-41), where $m$ is the length of the vector function $\boldsymbol{x}$,

$$\frac{dy}{d\boldsymbol{x}^{\mathrm{T}}} = \left(\frac{dy}{d\boldsymbol{x}_1} \quad \cdots \quad \frac{dy}{d\boldsymbol{x}_m}\right). \tag{3-41}$$

The difference between the output of (3-40) and (3-41) is that (3-40) is a column vector, whereas (3-41) is a row vector. This arrangement is maintained throughout the thesis. Extending the results of (3-40) and (3-41), if both $\boldsymbol{x}$ and $\boldsymbol{y}$ are vectors, then the derivative of $\boldsymbol{y}$ with respect to $\boldsymbol{x}$ is a $n$ x $m$ Jacobian matrix given by (3-42) if $\boldsymbol{y}$ is a $n$ x 1 vector and $\boldsymbol{x}$ is a $m$ x 1 vector [102]–[105],

$$\frac{d\boldsymbol{y}}{d\boldsymbol{x}^{\mathrm{T}}} = \left(\frac{d\boldsymbol{y}_i}{d\boldsymbol{x}_j}\right) = \begin{pmatrix} \frac{dy_1}{dx_1} & \cdots & \frac{dy_1}{dx_n} \\ \vdots & \ddots & \vdots \\ \frac{dy_m}{dx_1} & \cdots & \frac{dy_m}{dx_n} \end{pmatrix} \tag{3-42}$$

Matrix derivatives are calculated by transforming the matrix into a vector formation using the vector operator first and then applying vector differentiation principles to the vectors. In order to maintain consistent notation, the vector operator is written as $'\mathrm{vec}'$ operator from here on. The vec operator stacks the columns of a $n$ x $m$ matrix to a $nm$ x 1 vector. Hence, if $\boldsymbol{X}$ is a $n$ x $m$ matrix and $\boldsymbol{Y}$ is a $p$ x $q$ matrix, the derivative of $\boldsymbol{Y}$ with respect to $\boldsymbol{X}$ is a matrix $nm$ x $pq$ given by (3-43) [101], [102], [105], [106],

$$\frac{d\mathrm{vec}\,\boldsymbol{Y}}{d\mathrm{vec}\,\boldsymbol{X}^{\mathrm{T}}} = \left(\frac{d\mathrm{vec}\,\boldsymbol{Y}_i}{d\mathrm{vec}\,\boldsymbol{X}_j}\right) \tag{3-43}$$

Thus, by chain rule, if $\boldsymbol{Y}$ is a function of $\boldsymbol{X}$, and $\boldsymbol{X}$ is a function $\boldsymbol{Z}$; then (3-44) holds,

$$\frac{d\text{vec}\,\boldsymbol{Y}}{d\text{vec}\,\boldsymbol{Z}^{\mathrm{T}}} = \frac{d\text{vec}\,\boldsymbol{Y}}{d\text{vec}\,\boldsymbol{X}^{\mathrm{T}}}\,\frac{d\text{vec}\,\boldsymbol{X}}{d\text{vec}\,\boldsymbol{Z}^{\mathrm{T}}} \tag{3-44}$$

### 3.5.2 The Kronecker product and Roth's theorem

The Kronecker product is also used in Chapter 7, and its definition is given by (3-45). The product is also referred to as a tensor or direct product [15], [103]–[105],

$$\boldsymbol{A} \otimes \boldsymbol{B} = (a_{ij}\boldsymbol{B}) \tag{3-45}$$

The Kronecker product is related to the vec operator by Roth's theorem. The relationship is such that if (3-46) holds, then (3-47) defines Roth's relation on block matrices [102]–[104],

$$\boldsymbol{D} = \boldsymbol{ABC}, \tag{3-46}$$

$$\text{vec}\,\boldsymbol{D} = \left(\boldsymbol{C}^{\mathrm{T}} \otimes \boldsymbol{A}\right) \text{vec}\,\boldsymbol{B} \tag{3-47}$$

The definitions and the notation presented above are used to derive the fundamental matrix's sensitivity and elasticity, representing the mean state transitions' sensitivity and elasticity. The fundamental matrix's elements are the mean number of system states transitions, with each row representing unique initial conditions. The following section highlights the boundaries and limitations of the research work presents in the thesis.

## 3.6 Limitations and boundaries of the research

The research work presented in the thesis focuses on the system's reliability during its useful life depicted by region II of Figure 3-1. In particular, the focus is on the SCN that interfaces with external protection systems to enable tripping of circuit breakers as final elements of Safety-Related Systems. It is acknowledged that varying failure rates may characterise protection systems during their infancy stage or late in their life due to the ageing of system components. However, the aspects mentioned above do not form part of the research's scope because it is usual practice that protection systems are thoroughly tested before being in service, while replacements are often made towards the end of the system's useful life. Nevertheless, a system can be in operation while its failure rate is characterised by the infancy stage or the ageing of system components as depicted in Figure 3-1 (viz. regions I and III), even though it is undesirable.

The proportions of the individual subsystems contributing to common causes of failure are modelled using one $\beta$ parameter to demonstrate the analysis approach. However, it is acknowledged that the subsystems failure rates may have varying proportions to the system's

common causes of failure. The following section summarises the key discussion points of the chapter.

## 3.7 Chapter conclusions

The chapter discusses the methods used to investigate the performance of a multi-channel IEC 61850 based SCN considering combinatorial analysis methods at a component or subsystem level and the Markov process simulation method at a system level. The system's subsystems are considered groupings of components that result in the functionality of a subsystem. Hence, individual system components are considered replaceable to ensure full functionality upon failure. Consequently, generalised reliability and availability concepts are adequate to model system component reliability because they assume that faults are fully discoverable and repaired, which is not necessarily the case at a system level comprising multiple subsystems of various configurations.

The subsystems' interactions at a system level are formulated using a modified Markov chain process that allows the quality of repairs to be investigated based on mean system state transitions. The Markov process enables the impact of the quality of repairs on the system dynamics to be investigated through the system's transition probability matrix based on linear dynamical systems' perspective. Also, to complement the asymptotic analysis method, absorbing Markov chain incorporating matrix calculus methods is used to determine the system's responsiveness to imperfect repairs based on sensitivity and elasticity studies. The next chapter focuses on a Substation Communication Network's reliability with imperfect repairs and limited diagnostic coverage.

# CHAPTER 4

# RELIABILITY OF SUBSTATION COMMUNICATION NETWORKS WITH IMPERFECT REPAIRS

## 4.1 Introduction

The chapter focuses on integrating imperfect repairs and system diagnostic coverage as factors that should be considered in determining the reliability and availability of a mission-critical system based on IEC 61850 and IEC 61508 [2], [8]. Structure-function and Markov modelling are used to model the system's respective states and reliability, while System Thinking integrates imperfect repair factors (viz. repair efficiency and diagnostic coverage) into the Markov model. The system's reliability based on mean state transitions is estimated using mathematical expectation. The aim is to demonstrate the impact of imperfect repairs and system diagnostic coverage on the reliability and availability of multi-channel repairable IEC 61850 based SCN, as well as to develop a reliability model that can be used to investigate the dynamical behaviour of the system under various levels of imperfect repairs and diagnostic coverage. Further, the model could be used to determine the required capabilities of the subsystems. The chapter's scope covers the reliability and availability performance evaluation considerations in a mission-critical SCN when it interfaces to IEC 61508 systems and integrates repair efficiency and system diagnostic coverage factors to evaluate system performance. Subsequently, the criticality and the impact of the repair factors on the system's mean state transitions are determined and compared.

Section 4.2 presents an overview of an industrial power distribution centre and the case studies basis. Modelling imperfect repairs and system diagnostic coverage using structure-function, Systems Thinking, and the Markov process is covered in section 4.3. Section 4.4 presents the estimation of the system's mean state transitions. The overview of system diagnostic coverage levels is discussed in section 4.5. The results and discussions are presented in section 4.6. The case studies findings and conclusions are discussed in section 4.7.

## 4.2 Overview of an industrial power distribution centre

This section presents an overview of the industrial power distribution centre and the basis for the research work's case studies. IEC 61850 based power distribution system's high reliability and availability are needed to maintain the continuous power supply to various process plant loads and ensure execution of trip commands, as and when it is required to safeguard the plant and personnel [24]. IEC 60870-4 standard states that a single point of failure on the SCN should not cause the system to be inoperable [28]; however, IEC 61850 standard does not prescribe any architecture for SCN and leaves it to the designer of the system to determine according to the functional requirements of the SCN. In this paper, two IEEE

Power System Relaying Committee (PSRC) SCN architectures are considered (viz. cascaded and star configurations) [41].

### 4.2.1 Plant configuration and substation communication architecture

A typical power distribution centre comprises an incoming circuit breaker onto the switchboard, from which the power is distributed to various plant loads. In a thermal power plant, most of the loads are auxiliary boiler loads [24], where high reliability and availability of the draught system protection circuits are critical to isolating electrical machines when the process deviates from normal operating limits [24]. Detailed requirements of these types of circuits are addressed in IEC 61508 and IEC 61511. IEC 61850 based SCNs are designed so that a single point of failure on the system should not cause the system to become inoperable, especially where SRS mission-critical functions are required [28], [32].

In IEC 61850 based SAS, this requirement is fulfilled by implementing multi-channel systems with voting capabilities such as a ‘one-out-of-two’ system to increase the overall system's reliability and availability. This configuration ensures that the independent subsystem’s channels are repairable without completely isolating the whole protection system [9], [59]. Figure 4-1 depicts a typical IEC 61850 based SCN that interfaces with a Boiler Protection System (BPS) through the respective Remote Terminal Units (RTU) [24], [41].

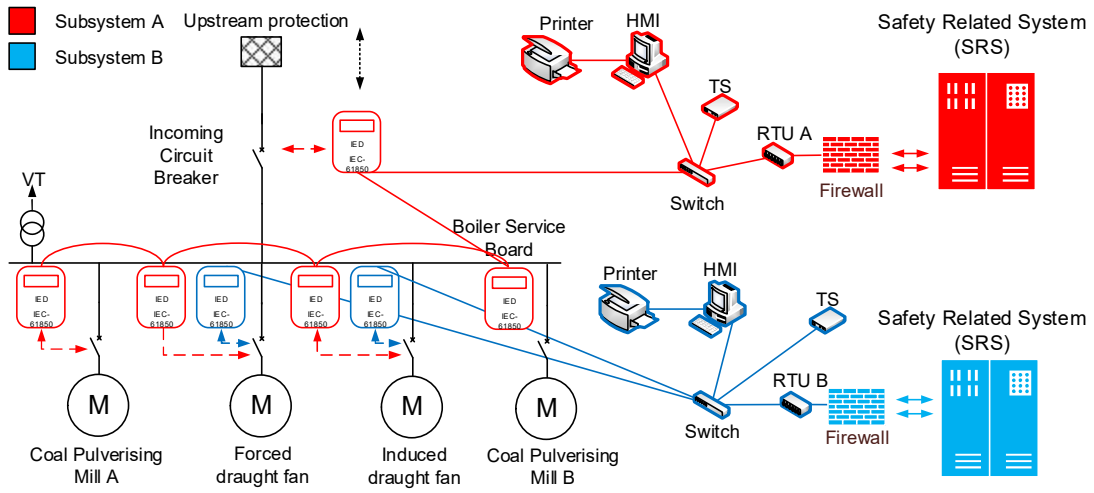


Figure 4-1: Typical IEC 61850 based thermal industrial power distribution centre [24], [41].

For analysis purposes, the tripping message is assumed to travel between the two most distant IEDs as the worst-case to evaluate the reliability and availability of protection functions for IEC 61850 based SCN. It is also assumed that the protection IED output signals are hardwired to the tripping circuit breaker, as is usually the case for industrial plant power distribution centres [2].

### 4.2.2 Availability evaluation of IEC 61850 SCN based on RDB method

It is assumed in the study that the Mean Time To Failure (MTTF) of SCN links is comparatively very high and therefore not considered in the calculations presented in the study [72], [107]. The MTTF data of the SCN devices are given in Table 4-1, whereas the MTTR of each device is considered 8 hours.

Table 4-1: Mean Time To Failure Data of Substation Devices [72]

| Intra-bay Substation Communication Network Devices | MTTF (Years) |
|---|---|
| Protection IED/RTU | 150 |
| Ethernet switch (SW) | 50 |
| Time synchronisation (TS) | 150 |

Using the RBD method, the failure rates ($\lambda_A$ and $\lambda_B$) of the respective subsystems is 0.13999 and 0.11333 [28], [72], [75].The availabilities of the individual subsystems A, subsystem B and the overall system AB are presented in Table 4-2 for comparative analysis at a later stage.

Table 4-2: System availability

| System | Subsystem A | Subsystem B | Overall system AB 'one-out-of-two.' |
|---|---|---|---|
| Availability | 0.99981 | 0.99984 | 0.9999 |

The data of SCN devices used in this research is obtained from the research case studies conducted in [28], [72], while the Mean Time To Repair (MTTR) is assumed to be 12 hours for the respective subsystems.

## 4.3 Reliability modelling based on structure-function and Markov

The reliability of engineering systems can be studied using structure-function models to elicit system state and system performance resulting from individual subsystems [108]. Structure-function is a mathematical concept representing a system's reliability using binary state and multi-state systems, where a binary state system relates to functional and non-functional states of the subsystems. Hence, the multi-channel system's states determine the systems' performance level [75], [108].

### 4.3.1 State-space modelling of multi-state systems

The arrangement of subsystems determines the level of system redundancy. In this study, components that have been configured to function together such that failure of one component

leads to mission failure are viewed as one system or subsystem where several such groupings exist together [7]. Hence, the following hypotheses are made [97]:

a) A subsystem can be in a functional or non-functional state at any given point in time and not both states simultaneously.
b) Subsystems comprise *r* number of components (i.e., 1, 2… *r*), of which their behaviour is governed (a) above.

Considering a system S, of *r* number of components; state variable of each component $x_i$ (for $i = 1, 2 \ldots r$) can be assigned such that:

$$x_i = \begin{cases} 1, & \text{functional} \\ 0, & \text{non} - \text{functional} \end{cases} \tag{4-1}$$

Therefore, if $e = \{e_1, e_2, \ldots, e_r\}$ is the set of system components, the state of the set of components is given by:

$$x = \{x_1, x_2, \ldots, x_r\} \tag{4-2}$$

Hence the set of components will have $2^r$ different states. Now, let *y* be the system state 'variable' according to the hypotheses made earlier on, then

$$y = \begin{cases} 1, & \text{functional} \\ 0, & \text{non} - \text{functional} \end{cases} \tag{4-2}$$

If $y$ depends on $x$, then there exists a function $f(x)$ such that $y = f(x)$, or $y = f(x_1, x_2, .. x_r)$, and $f(x)$ is a structure-function [97], [108]. It follows, therefore, that a function of $x_1$ and $x_2$ can represent the 'one-out-of-two' system depicted in Figure 2-1; where $x_1$ and $x_2$ are the state variables of the subsystems A and B respectively [75], [97]. Hence,

$$y = f(x) = 1 - \prod_{i=1}^{2}(1 - x_i) \tag{4-3}$$

The two paralleled systems' state-space model can be summarised as four states, as presented in Table 4-3.

Table 4-3: System AB state description

| A | B | System Availability | State |
|---|---|---|---|
| $x_1$ | $x_2$ | $y = 1 - ((1 - x_1)(1 - x_2))$ | |
| 1 | 1 | Yes (1) | S-1 |
| 1 | 0 | Yes (1) | S-2 |
| 0 | 1 | Yes (1) | S-3 |
| 0 | 0 | No (0) | S-4 |

In Table 4-3, state S-1 represents a system condition where both subsystems A and B are fully functional. In states S-2 and S-3, one of the subsystems A or B is fully functional, while the other is not available and could be under repair. Even so, the system's overall functional availability is sufficient to satisfy mission execution requirements while the system is in one of the two states. State S-4 represents a system condition where both subsystems A and B cannot execute mission functions, resulting in the overall system becoming unavailable since no mission can be executed. The state transitions of a structure function are modelled using the Markov process in the following subsection [75], [97].

### 4.3.2 State transitions based on the Markov process

The state-space of a 'one-out-of-two' redundant IEC 61850 based SCN was derived in the previous subsection. In this subsection, the Markov process is used to model the state-space transitions of the SCN [98]. Markov modelling is a pliable, graphically-assisted quantitative evaluation method used in the design for reliability and availability decision making and validation of system design based on envisioned objectives. The process can optimise maintenance strategies in complex dynamic systems [2], [78]. Figure 4-2 depicts the state transition diagram of the two subsystems depicted in Figure 4-1.

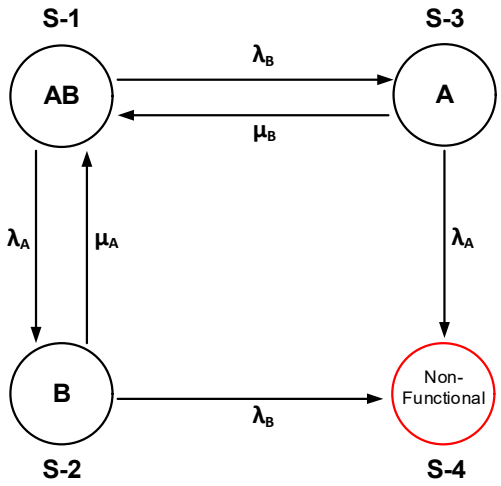


Figure 4-2: Markov state transition diagram of 'one-out-of-two' protection system [75]

Since the failure rates of subsystems are constant and follow exponential distribution during the cause of the system's useful life [3], [44], [72], [75], the state transitions of the system depicted in Figure 4-2 is, therefore, stochastic [75], [91]. Hence, the impact of imperfect repairs on the system's availability is investigated while the system components' failure rates are constant. The development of the systematic model is presented in the following subsection.

### 4.3.3 Modelling imperfect repairs based on the Systems Thinking approach

The involvement of a human component in complex systems of diverse fields makes it challenging to analyse systems' performance and their improvement thereof [92]. The systems Thinking concept has been used to study and analyse the dynamical behaviour of systems. The approach followed in Systems Thinking investigates cause and effect relations between different elements of a system and its environment using systematic casual loop model diagrams to systematically model such a system [91], [109].

Systems Thinking is based on the concept of holism, asserting that a system's behaviour or performance is understood by considering the interactions between its elements; and not only by individually studying the behaviour or properties of its elements [90], [109]–[111]. Systematic models are orderly structures that focus on interactions between subsystems and require identifying and understanding various system element configurations to study their interactions [110], [112]. Thus, Systems Thinking offers a method of formulating and solving complex dynamic systems with visual illustrations using casual loop diagrams. The diagrams ensure understanding of the problem statement and the associated dynamics [110], [113]. Also, causal loop diagrams capture and articulate deeper insights into complex systems' behavioural structure or aspect, while modelling delays in the system highlight the relative system dynamics [114].

System dependability is a broader concept used to analyse complex dynamic systems' performance and focuses on reliability, availability, maintainability, safety, and integrity. Reliability, availability and maintainability are quantitative attributes of dependability, while safety and integrity are qualitative attributes [92], [115]. The safety and integrity of the IEC 61850 based system satisfy the requirements of IEC 61784 and IEC 61508 [4], [5]. The availability of a system is dependent on its MTTF and MTTR. During the useful life of a system, failures are random, and its failure rate ($\lambda$) is assumed to be constant [28], [72], [75], [79]. Figure 4-3 depicts a systematic model of system availability with perfect repairs.

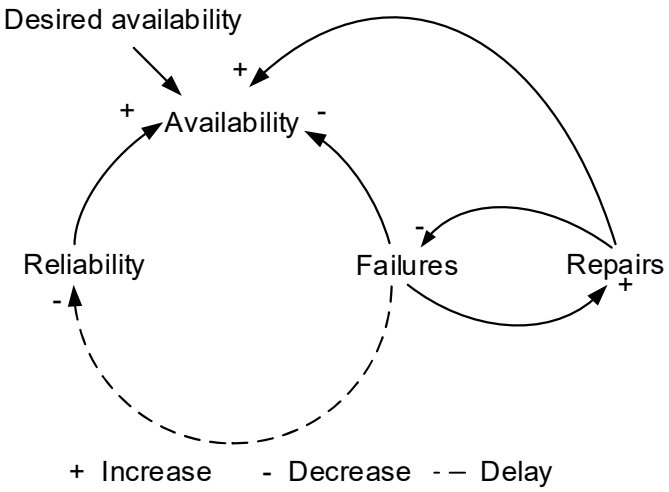


Figure 4-3: A basic systematic model of system reliability and availability

The arrows on the diagram depicted in Figure 4-3 indicate the system element impacted by another element from which the arrow is drawn. The '+' and '-' signs indicate the impact's nature, as shown on the diagram's legend. The dashed lines on the arrow indicate a delayed impact. In the systematic model of Figure 4-3, failures decrease the system's availability while repairs increase. However, repairs increase the availability of the system. The dashed line on the arrow between failures and reliability indicates no impact on the system reliability in the immediate future. It is accepted that a change in failure rate can negatively impact the system's reliability, which will reduce system availability. In Figure 4-4, the systematic model presented in Figure 4-3 is extended to include the impact of imperfect repairs, the increase in repairs increases diagnostic tools, and technical expertise ($T_{expertise}$) needed to diagnose and repair system faults.

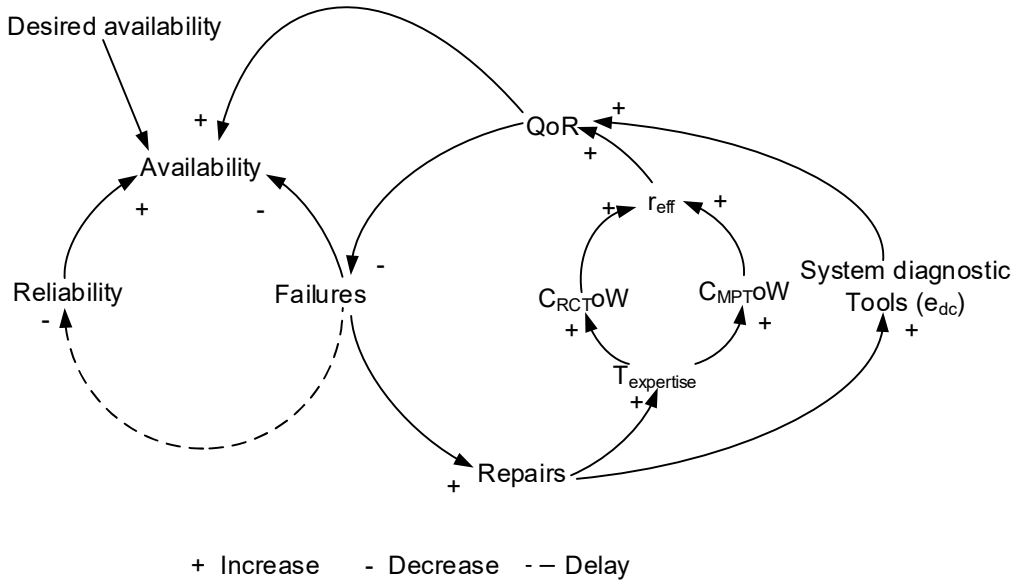


Figure 4-4: An expanded systematic reliability and availability model with quality of repairs

Technical expertise, in turn, increases both correctness and completeness of work (viz. $C_{RCTo}W$ and $C_{MPTo}W$) performed; which has a positive impact on repair efficiency ($r_{eff}$). System diagnostic ($e_{dc}$) coverage and repair efficiency increase the quality of repairs (QoR), increasing system availability while reducing failures. In the following subsection, imperfect repairs are integrated into the Markov process model depicted in Figure 4-2.

### 4.3.4 Imperfect repairs based on Markov incorporating Systems Thinking

To account for the factors described in Figure 4-4, a diagnostic coverage factor ($e_{dc}$) is introduced in the state transition diagram model of Figure 4-2 to model the level of identifiable system faults [60], [98], [116]. Another factor also included in the state transition diagram of Figure 4-2 is associated with the correctness and completeness of repair activities during maintenance and testing, referred to as repair efficiency ($r_{eff}$) [60]. Figure 4-5 depicts the modified Markov Chain (MC) state transition diagram of the system presented in Figure 4-2.

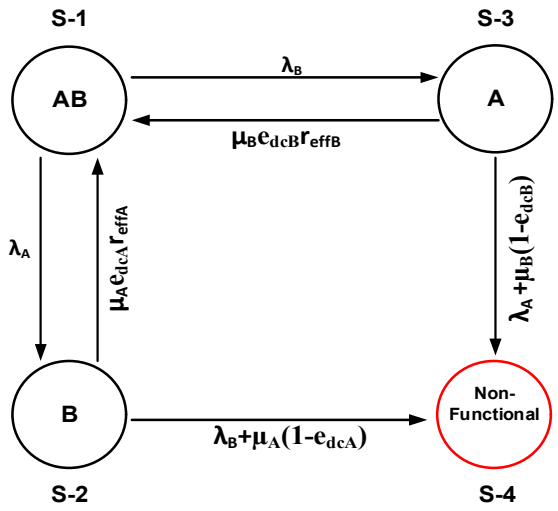


Figure 4-5: Modified Markov state transition diagram of a 'one-out-of-two' protection system

The factors introduced in the model collectively impact the quality of repairs (QoR) performed in the system, as discussed in the previous section. Thus, the state transition probability matrix of the system depicted in Figure 4-5 is given by (4-4) [49], [60], [91]. In the following subsection, the MTTF of the system is estimated from the state transition probability matrix using mathematical expectation based on mean state transitions.

$$\boldsymbol{P} = \begin{bmatrix} 1-\lambda_A-\lambda_B & \lambda_A & \\ \mu_A e_{dcA} r_{effA} & 1-\mu_A e_{dcA} r_{effA} - (\lambda_B + \mu_A(1-e_{dcA})) & \cdots \\ \mu_B e_{dcB} r_{effB} & 0 & \\ 0 & 0 & \end{bmatrix}$$

$$\begin{matrix} \lambda_B & 0 \\ 0 & \lambda_B + \mu_A(1 - e_{dcA}) \\ \cdots\ 1 - \mu_B e_{dcB} r_{effB} - (\lambda_A + \mu_B(1 - e_{dcB})) & \lambda_A + \mu_B(1 - e_{dcB}) \\ 0 & 1 \end{matrix}\Bigg] \quad (4\text{-}4)$$

### 4.4 Estimation of system Mean time to failure using Mathematical Expectation

Failure of protection aided SCN system occurs when substation devices are not able to communicate mission-critical messages. Hence, the number of system state transitions before it enters a failed state (i.e. S-4 of Figure 4-5) represents the MTTF of the system, which is determinable using mathematical expectation [75], [82]. The mathematical expectation principle shows that a 'two-state' system starting at state '1' has a progressively smaller probability of remaining in state '1' given that it will eventually enter state '2'. Expressing the statement mathematically,

$$\lim_{n\to\infty} \left(\frac{1}{2}\right)^n = 0 \quad (4\text{-}5)$$

where $n$ is the number of system state transitions given that (4-5) is iterated multiple times. Based on a stochastic transition state probability matrix $\boldsymbol{P}$, a truncated matrix $\boldsymbol{Q}$ of $\boldsymbol{P}$ with all state transition probabilities (i.e. column and row entries) associated with failed system state deleted can be obtained, such that (4-6) holds [75].

$$\boldsymbol{N} = \boldsymbol{I} + \boldsymbol{Q} + \boldsymbol{Q}^2 + \cdots + \boldsymbol{Q}^{n-1} \quad (4\text{-}6)$$

Where $N$ is the matrix of the average number of time intervals the system stays in the respective states before entering a failed state (i.e., the absorbing state), and $\boldsymbol{I}$ is the identity matrix. In this context, $\boldsymbol{N}$ is the expected value according to the principle of mathematical expectation described by (4-7) [75].

$$E(x) = \sum_{i=0}^{\infty} x_i P_i \quad (4\text{-}7)$$

Where $E(x)$ is an expected value of a discrete random variable $x$ that has $n$ possible outcomes $x_i$, and $P_i$ is the probability of occurrence of $x_i$, and $\sum_{i=1}^{n} x_i P_i = 1$. To solve (4-7), (4-8) is considered.

$$[\boldsymbol{I} - Q][\boldsymbol{I} + \boldsymbol{Q} + \boldsymbol{Q}^2 + \cdots + \boldsymbol{Q}^{n-1}] = \boldsymbol{I} - \boldsymbol{Q}^n \quad (4\text{-}8)$$

Following (4-5),

$$\lim_{n\to\infty} \boldsymbol{Q}^n = 0 \tag{4-9}$$

Therefore, as $n \to \infty$,

$$\boldsymbol{I} - \boldsymbol{Q}^n \ \to \boldsymbol{I}$$

Further evaluation of (4-8) leads to (4-10)

$$\boldsymbol{I} + \boldsymbol{Q} + \boldsymbol{Q}^2 + \cdots + \boldsymbol{Q}^{n-1} = [\boldsymbol{I} - \boldsymbol{Q}]^{-1} \tag{4-10}$$

Thus,

$$\boldsymbol{N} = [\boldsymbol{I} - \boldsymbol{Q}]^{-1} \tag{4-11}$$

Where $N_{jk}$ is the average number of transitions the system enters state *k*, given that the system's initial state is *j*, which is easy to evaluate compared to (4-6) [75]. Thus, in the system of Figure 4-5, with the initial state being S-1, the average number of steps before the system enters the state S-4 is given by (12).

$$\text{Mean state transitions } = \sum_{k=1}^{\text{length}(\boldsymbol{N}(j:))} N_{jk} \tag{4-12}$$

Where $j$ is the matrix row number representing the initial state of the system, and $k$ is the vector element of $\boldsymbol{N}(j:)$.

### 4.5 Levels of System diagnostic coverage

This section presents an overview of system diagnostic coverage levels according to ISO 13849-1 used as the basis in the case studies. ISO 13849-1 defines four diagnostic coverage levels based on their effectiveness. The levels are used as a basis to simplify design efforts in industrial systems. A wide range of technical scopes, including electrical, electronic, and programmable electronic devices, are addressed in ISO 13849. The standard references IEC 61508 for the definition of system diagnostic coverage [117]–[120]. Table 4-4 presents the four levels and associated ranges of system diagnostic coverage defined in ISO 13849-1 [118]–

[120]. Diagnostic coverage of less than 60% is not denoted in the standard, while 60%, 90% and 99% are denoted as presented in Table 4-4 [117]–[120].

Table 4-4: Denotation of diagnostic coverage levels and ranges

| Denotation | Range |
|---|---|
| None | $e_{dc} < 60\%$ |
| Low | $60\% \leq e_{dc} < 90\%$ |
| Medium | $90\% \leq e_{dc} < 99\%$ |
| High | $99\% \leq e_{dc}$ |

In the case studies, the impact of repair efficiency at 85%, 90%, 95% and 100% is simulated at 100%, 99%, 90% and 60% system diagnostic coverage to demonstrate imperfect repairs on the system availability. The ideal case study at 100% diagnostic coverage represents a condition where all system faults are identifiable; hence, this case study is similar to the RBD method.

## 4.6 Results and discussions

This section presents case studies, simulation results and discussions. To be able to demonstrate the impact of the described factors while simplifying the effort that is required to analyse the results, the following is assumed:

a) Subsystems A and B are of the same technology; hence they have the same diagnostic capability.
b) Same resources are used to support both subsystems A and B such that identical repair efficiency for both subsystems is used.
c) The system is fully functional at the beginning of the simulation.

### 4.6.1 Ideal and high diagnostic coverage levels

In this case study, 100% repair efficiency is comparable to the RBD method, of which the results are presented in Table 4-2, where all system faults are assumed to be identified and fully repaired. The heatmap of the transition probability matrix at 100% repair efficiency and diagnostic coverage is depicted in Figure 4-6 to enable the visualisation and comprehension of the system's state transition probabilities.

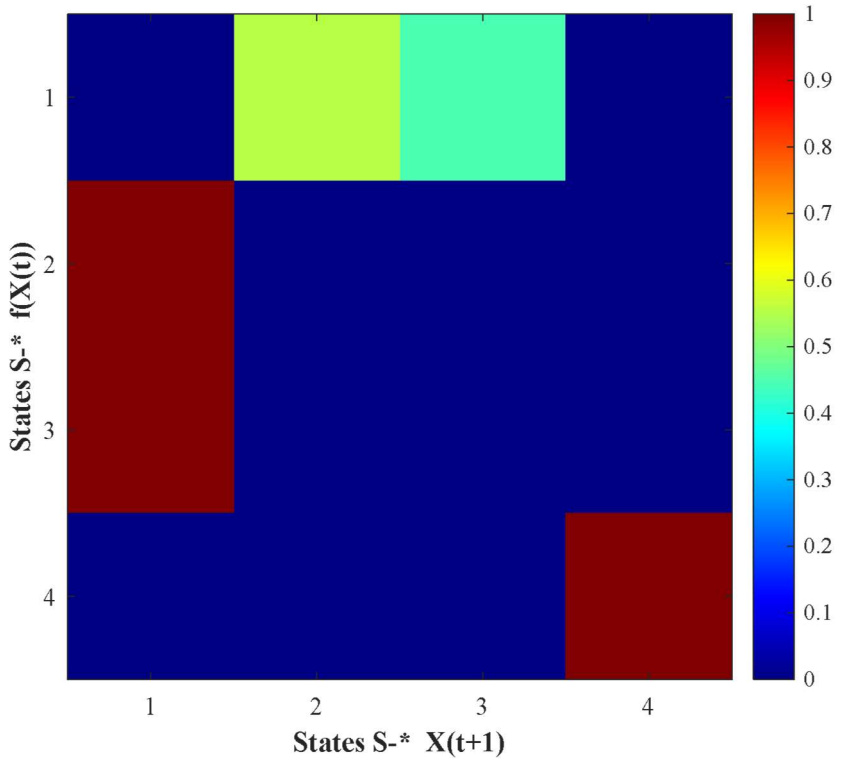


Figure 4-6: Transition probability matrix heatmap - 100% diagnostic coverage

It can be observed that the system can transit to either states S-2 or S-3 with a high probability that it will transit into S-2, given that its initial state is S-1. Thereafter, the system would transition back to state S-1 because the probability of transiting into any other state from either states S-2 or S-3 is almost zero. Hence, this system condition makes it to have a very high number of mean state transitions before failure. However, the system will remain in state S-4 once it transits into the state because it has a zero-transition probability to transit to any other state from there.

Figure 4-7 the probability of system availability reaches zero after 50000-time steps, which is considered to be practically very high. The impact of low repair efficiency is evident on 95%, 90% and 85% repair efficiency ($r_{eff}$) curves as the probability of the system availability reduce with reduced repair efficiency, though the impact is marginal. The reduction in system performance results from a slight improvement of transition probabilities of the system to transition to state S-4 from states S-2 and S-3 when the repair efficiency is reduced; given that S-1, S-2 and S-3 all combined represent the probability of system availability, and state S-4 represents system unavailability.

Figure 4-8 depicts the system's transition probability heatmap at 99% diagnostic coverage, implying that 1% of the system faults remain unidentified. In contrast to Figure 4-6, the heatmap shows that the system's probability of transitioning to state S-4 from either S-2 or S-3 is no longer zero.

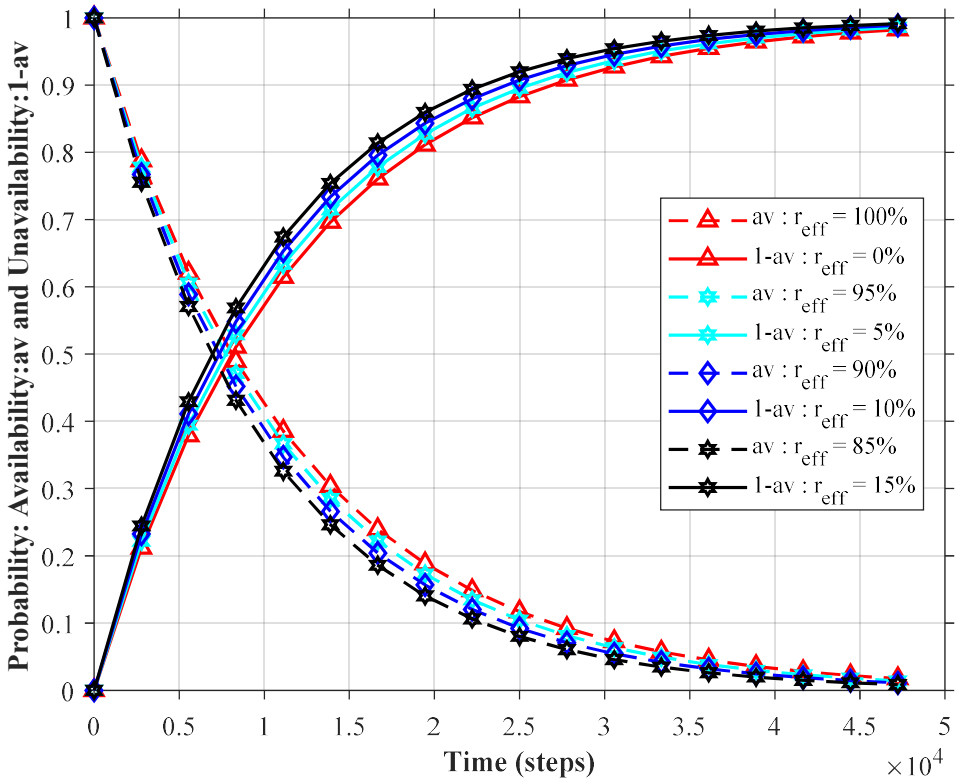


Figure 4-7: Probability of system availability and unavailability - 100% diagnostic coverage

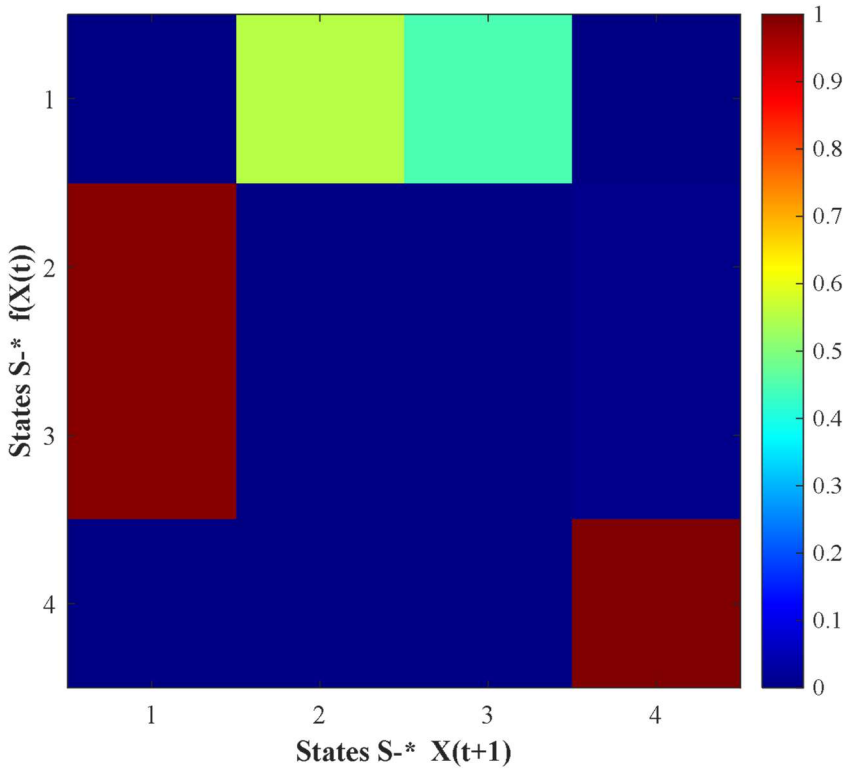


Figure 4-8: Transition probability matrix heatmap - 99% diagnostic coverage

However, the system's probabilities of transiting back to state S-1 from states S-2 or S-3 are relatively still very high. Hence the system is still expected to have a high number of mean

state transitions. Nevertheless, the results depicted in Figure 4-9 shows a drastic reduction in time steps before the system availability reaches zero.

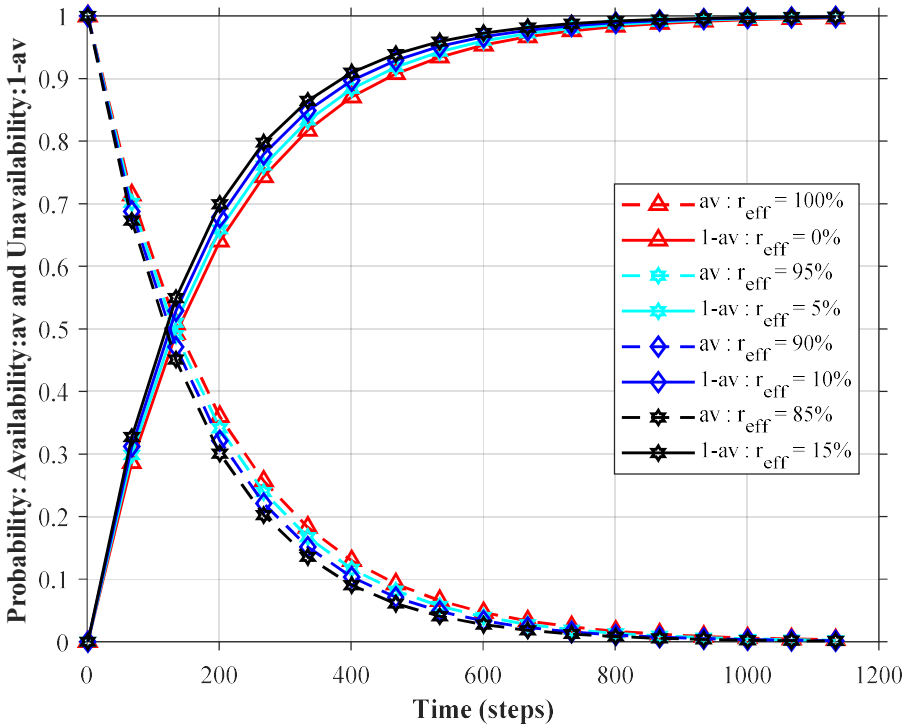


Figure 4-9: Probability of system availability and unavailability - 99% diagnostic coverage

Therefore, the 99% system diagnostic coverage level is not comparable to the RBD method's ideal case. In this case, the probability of system availability reaches zero in about 1000-time steps. The results indicate that a 1% reduction in system diagnostic coverage significantly impacts the system's performance. Notably, the impact of different repair efficiency levels on the system's performance is comparable to the ideal case results presented in Figure 4-7.

### 4.6.2 Medium and low diagnostic coverage levels

Figure 4-10 depicts the system's transition probabilities heatmap at 90% diagnostic coverage, implying that 10% of the system faults remain hidden and therefore not repaired by the time the system is returned to service. In this case study, it can be observed that the system can transit to either states S-2 or S-3 with a high probability that it will transit into S-2, given that its initial state is S-1. However, the system's probability of transitioning back to S-1 from states S-2 or S-3 is relatively reduced than when the diagnostic coverage was 100% or 99%. Notably, the system transiting to state S-4 has increased, as depicted on the heatmap. As before, the system will remain in state S-4 once it transits into the state because it has a zero-transition probability to transit to any other state from there.

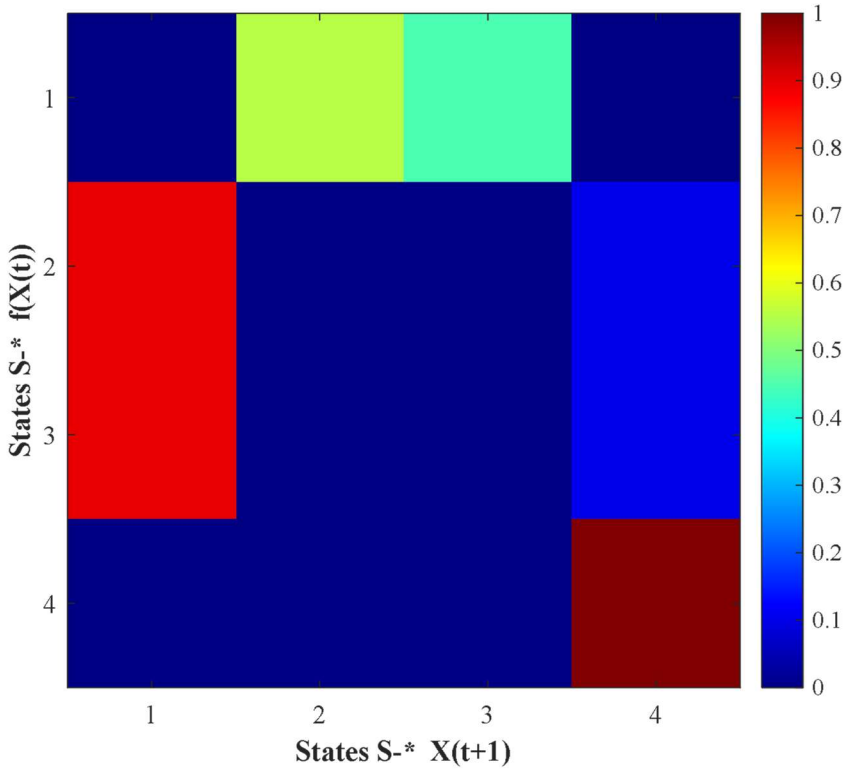


Figure 4-10: Transition probability matrix heatmap - 90% diagnostic coverage

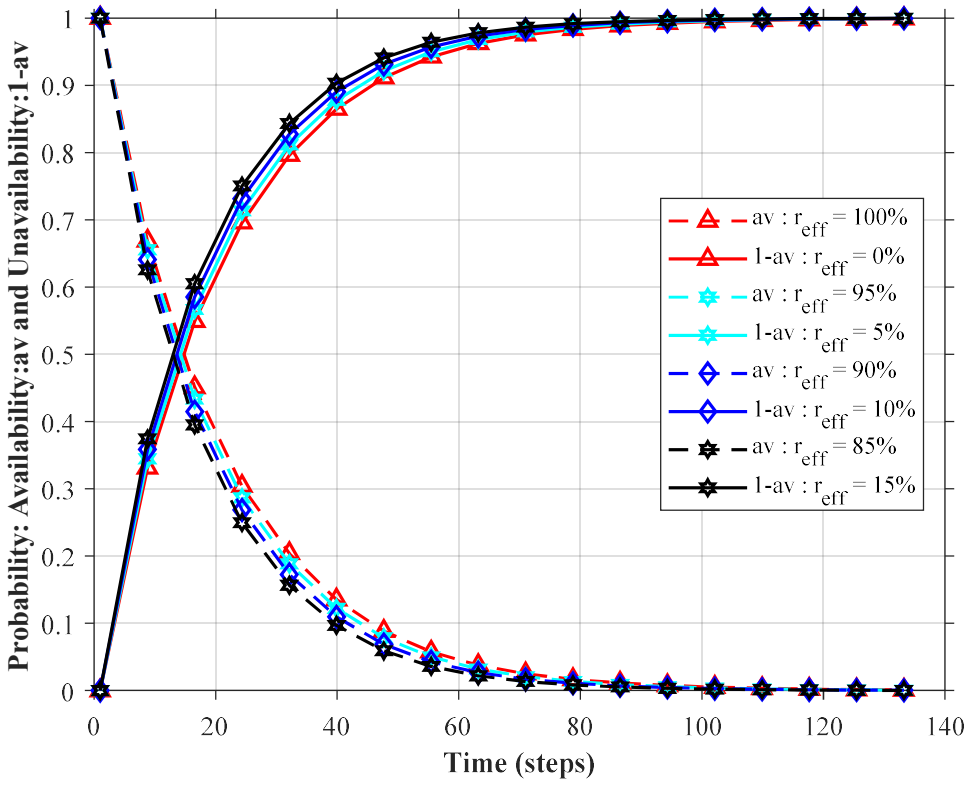


Figure 4-11: Probability of system availability and unavailability - 90% diagnostic coverage

Expectedly so, further reduction of system life is noticeable when the system diagnostic coverage is reduced; the probability of system availability reaches zero in just over 100-time steps, as depicted in Figure 4-11. The drastic reduction in the number of time steps is caused by the increased state transition probabilities of states S-2 and S-3 towards state S-4. The probabilities of the system transiting back to state S-1 from states S-2 and S-3 decrease as the system diagnostic coverage ($e_{dc}$) factor decreases. Therefore, the number of time-steps the system transit through before it enters the failed state S-4 decreases as the diagnostic coverage ($e_{dc}$) factor decreases. As before, the reduction in repair efficiency marginally impacts the system's performance, as depicted in Figure 4-11. Figure 4-12 depicts the heatmap of the system's transition probabilities at 60% diagnostic coverage, which implies that 40% of the system faults remain hidden and therefore not repaired by the time the system is returned to service.

It can be observed that the system can transit to either states S-2 or S-3 with a high probability that it will transit into S-2, given that its initial state is S-1 as before. However, the probabilities of transiting back to S-1 have significantly reduced compared to the case studies when the diagnostic coverage is 100%, 99% and 90%. As expected, the probabilities of the system transiting to state S-4 have increased to about 0.4, as depicted in Figure 4-12.

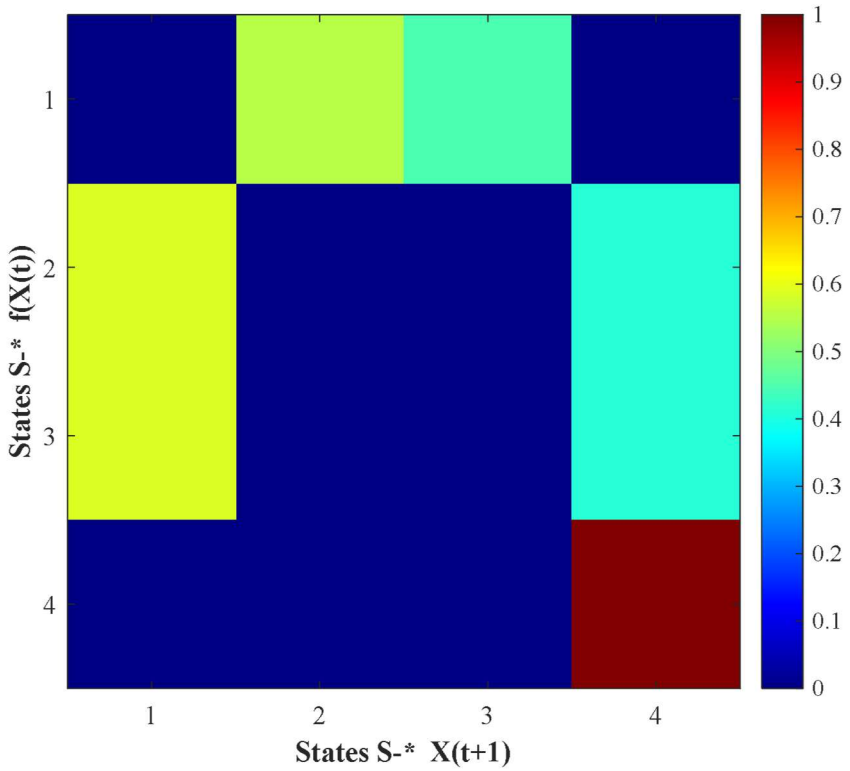


Figure 4-12: Transition probability matrix heatmap - 60% diagnostic coverage

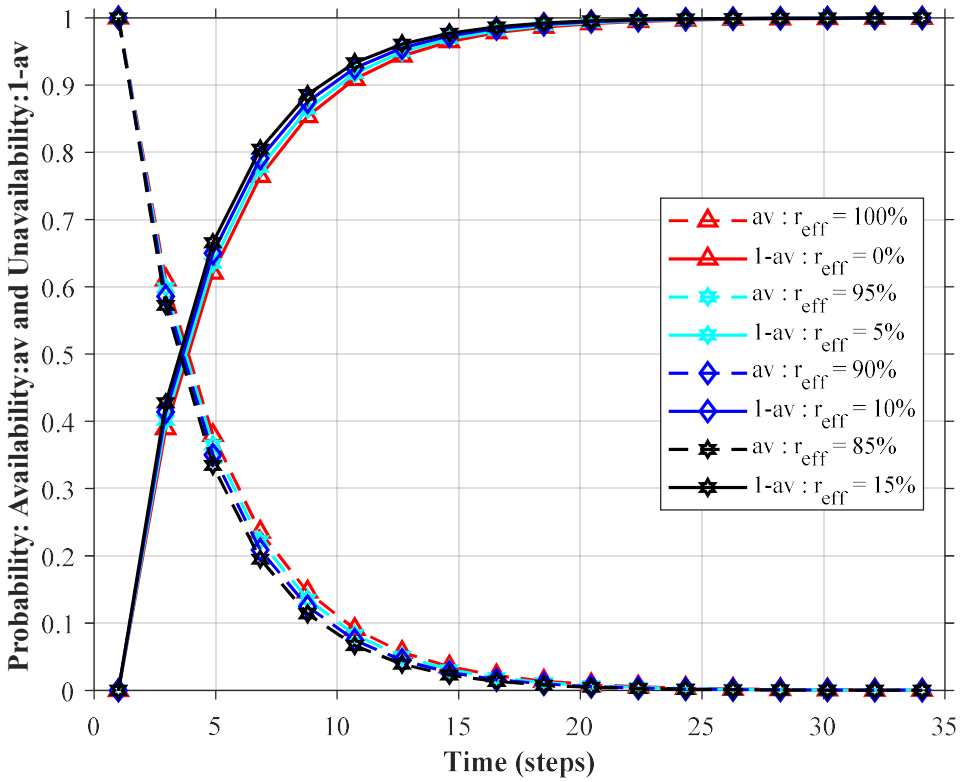


Figure 4-13: Probability of system availability and unavailability - 60% diagnostic coverage

Again, the system will remain in state S-4 once it transits into the state because it has a zero-transition probability to transit to any other state from state S-4. Figure 4-13 depicts the system's performance results at 60% system diagnostic coverage. As before, further reduction of system useful life is noticeable when the system diagnostic coverage is reduced, the probability of system availability reaches zero in just over 20-time steps where 40% of the system faults remain hidden.

### 4.6.3 Mixed diagnostic coverage levels

Two system configurations are considered in this case study (viz. 'high and low' and 'medium and low' configurations). The individual subsystems A and B are assumed to be of different technology to demonstrate the system's reliability performance when the subsystems have different diagnostic coverage levels. Table 4-5 presents the case study diagnostic coverage levels of the 'one-out-of-two' subsystems under consideration.

Table 4-5: Case study system diagnostic coverage levels

| System configuration | High and low (A-1) | Medium and low (A-2) |
|---|---|---|
| Subsystem A diagnostic coverage ($e_{dcA}$) | 99% | 90% |
| Subsystem B diagnostic coverage ($e_{dcB}$) | 60% | 60% |

**a) A-1 system configuration**

Figure 4-14 depicts the system's transition probabilities heatmap at 99% and 60% diagnostic coverages for subsystems A and B, respectively. As in the previous case studies, it can be observed that the system can transit to either states S-2 or S-3 with a high probability that it will transit into S-2, given that its initial state is S-1. Nevertheless, the probabilities of the system transiting back to S-1 from state S-3 has significantly reduced compared to transiting from state S-2 because the diagnostic coverage of subsystem B is relatively low. Instead, the probability of the system transiting to state S-4 from state S-3 has increased, as depicted on the heatmap. As before, the system will remain in state S-4 once it transits into the state because it has a zero-transition probability to transit to any other state from there.

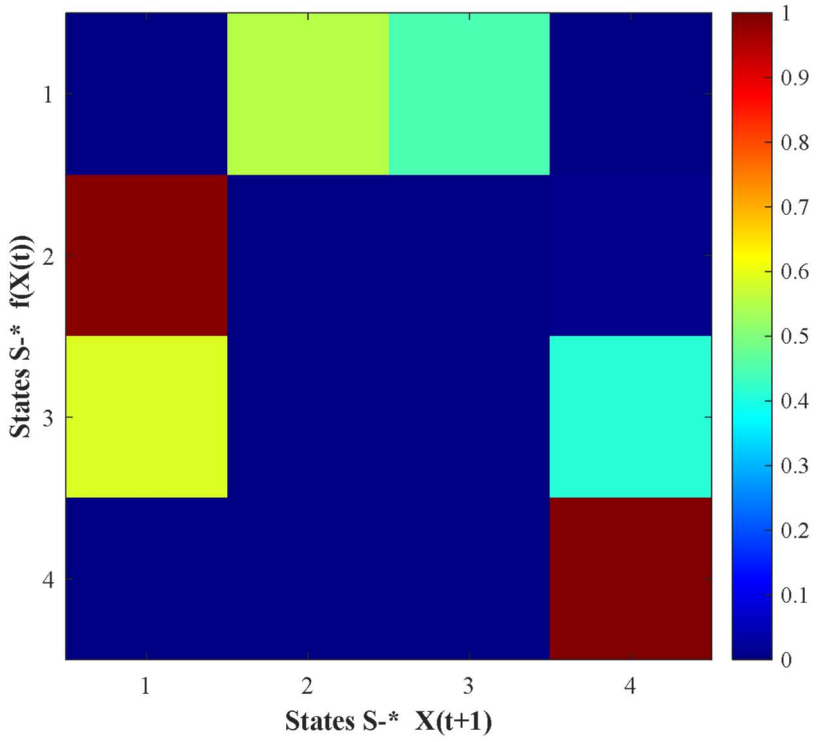


Figure 4-14: Transition probability heatmap – Mixed diagnostic coverages (99% and 60%)

The reduction in system life is noticeable when the system diagnostic coverage of subsystem B is reduced to 60% while subsystem A is 99%. As depicted in Figure 4-15, the probability of system availability reaches zero in just over 50-time steps.

The drastic reduction in the number of time steps is caused by the increased state transition probability of state S-3 towards state S-4, which causes the probability of the system to transit to state S-1 from state S-3 to decrease as the respective subsystem diagnostic coverage ($e_{dc}$) factor decrease. Therefore, the number of time-steps the system transit through before it enters the failed state S-4 decreases as the diagnostic coverage ($e_{dc}$) factor of one of the subsystems decrease. Hence, it is not beneficial to parallel subsystems of high and low

diagnostic coverages. As before, the reduction in repair efficiency marginally impacts the system's performance, as depicted in Figure 4-15.

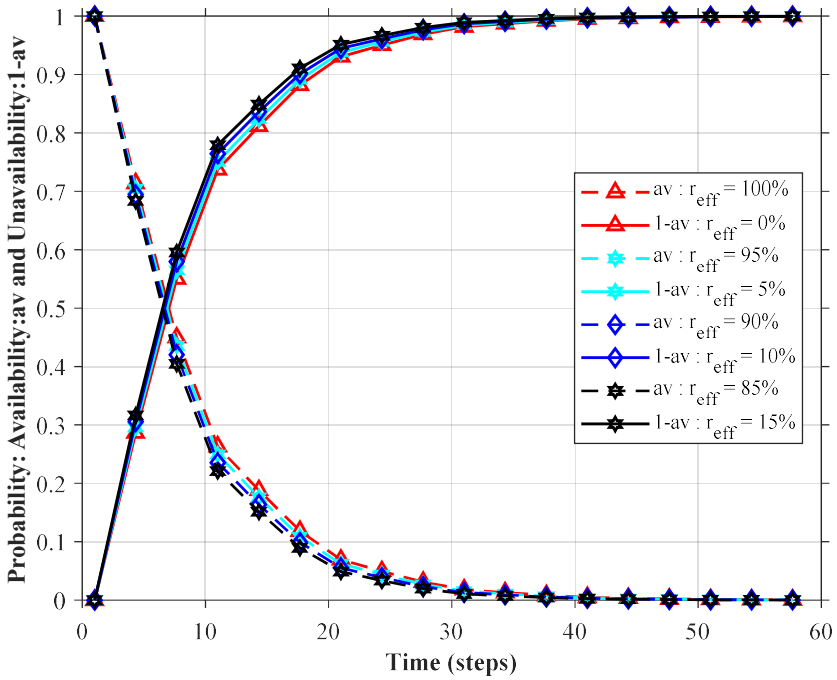


Figure 4-15: Probability of system availability and unavailability – Mixed diagnostic coverages (99% and 60%)

**b) A-2 system configuration**

Figure 4-16 depicts the system's transition probabilities heatmap at 90% and 60% diagnostic coverages for subsystems A and B, respectively. The transitioning characteristics of the system are the same as in the previous case studies. However, the system's probabilities of transiting back to S-1 from either states S-2 or S-3 have significantly reduced further than in the case at 99% and 60% subsystems diagnostic coverage configuration discussed in the previous case study. In contrast, the probabilities of the system transiting to state S-4 from states S-2 and S-3 have increased considerably to between 0.3 and 0.4. As before, the system will remain in state S-4 once it transits into the state because it has a zero-transition probability to transit to any other state from state S-4.

Figure 4-17 depicts the system's performance with mixed diagnostic coverages at 90% and 60%. Reduction of useful system life is noticeable when the system diagnostic coverage of subsystem A is reduced to 90%; the probability of system availability reaches zero in just over 40-time steps. Even though the system's performance has been relatively reduced, the reduction in performance is not significant, which indicates that subsystems of equal performance levels could prove to be most beneficial compared to subsystems of vastly different performance levels.

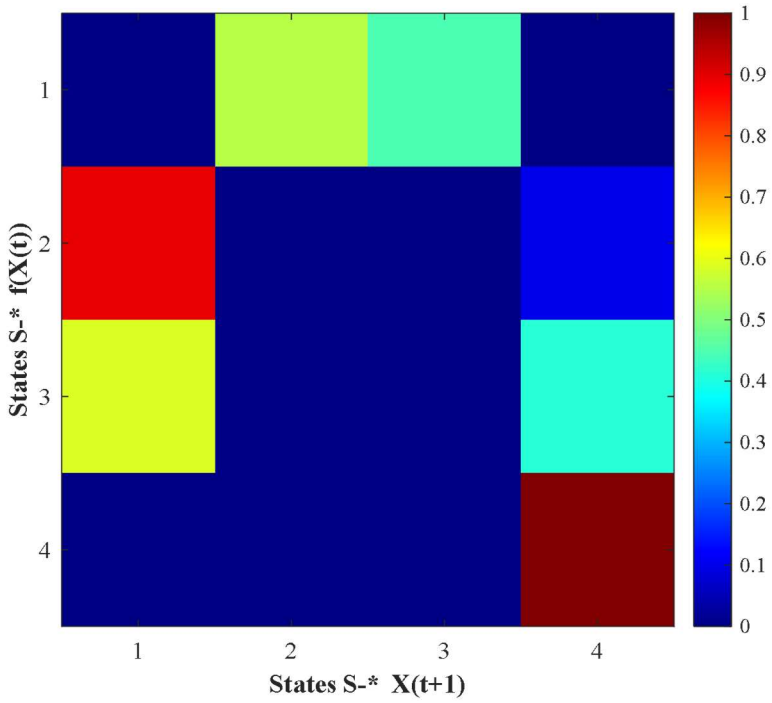


Figure 4-16: Transition probability heatmap – Mixed diagnostic coverages (90% and 60%)

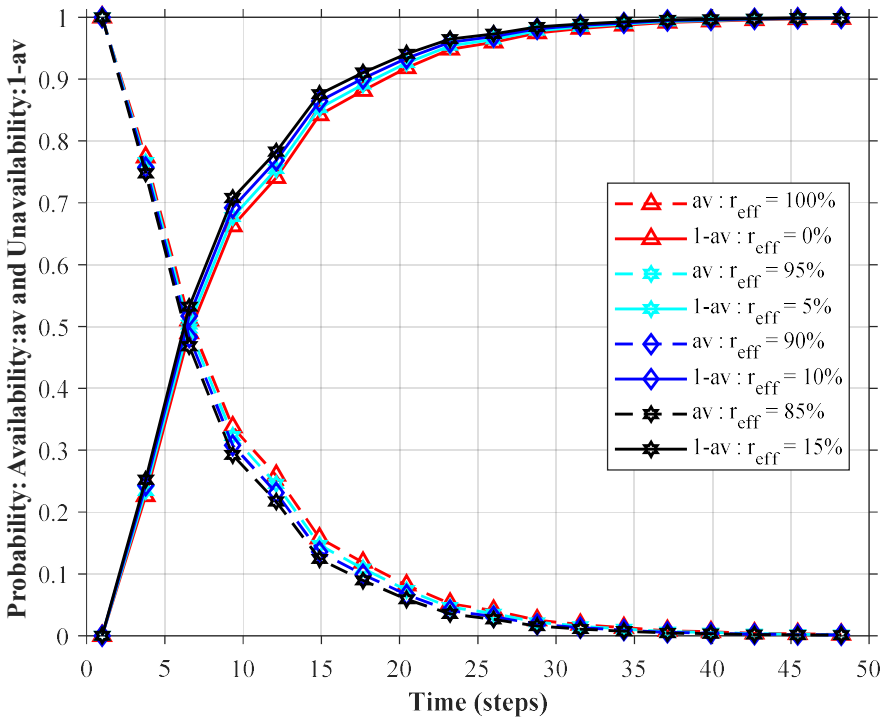


Figure 4-17: Probability of system availability and unavailability – Mixed diagnostic coverages (90% and 60%)

### 4.6.4 Mean system state transition

Figure 4-18 depicts the mean system state transitions before failure simulated at different diagnostic coverage levels and repair efficiency. It is evident that the system diagnostic capability profoundly impacts the mean system state transitions as demonstrated by the results obtained between 100% and 99% diagnostic coverage represented by the ideal and high denotations levels, respectively. At the medium diagnostic capability level, the mean system state transitions are low at 20 at the highest (i.e. 100% repair efficiency); and almost zero at low diagnostic capability because of the high level of system faults that cannot be identified. Hence the performance of the system is compromised when the quality of repairs is low.

The system also shows sensitivity to repair efficiency on the four diagnostic coverage levels, of which the reason is that the overall impact of the repair efficiency is dependent on the number of the mean state transitions. Consequently, every time the system transit from either states S-2 or S-3 to state S-1, it accumulates a percentage of incorrect and or incomplete repairs according to the level of system repair efficiency. The magnitude of the mean state transitions' sensitivity of the system on the repair efficiency is also evident on the high, medium and low diagnostic coverage levels where the individual repair efficiency levels have slight differences compared to the ideal case.

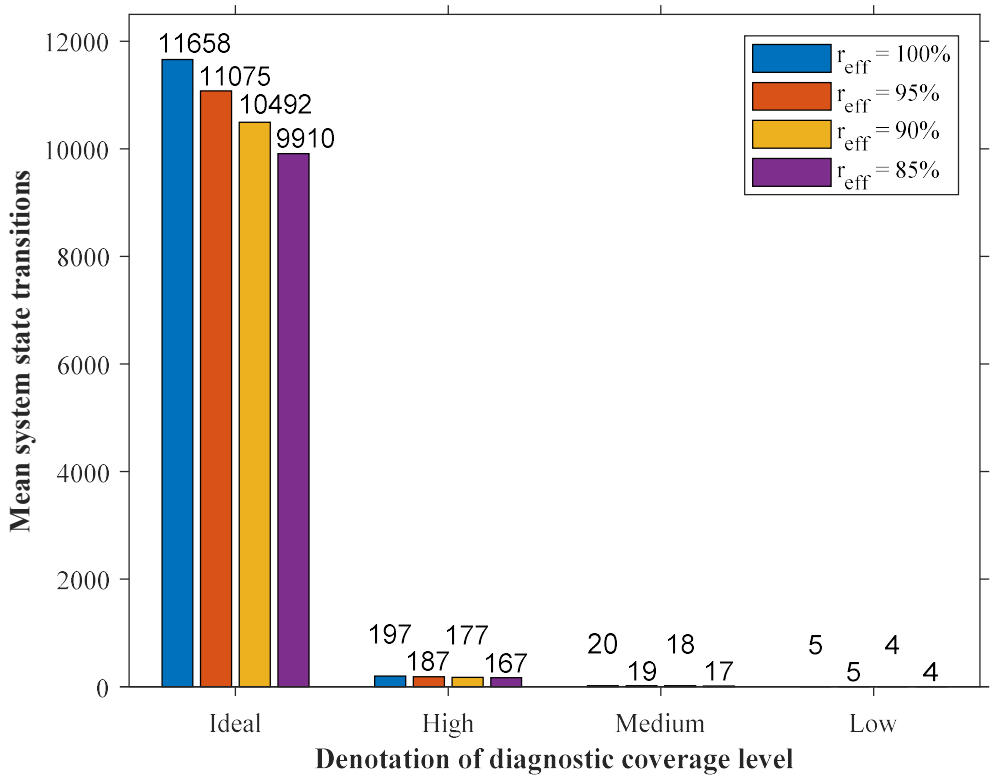


Figure 4-18: Mean system state transitions before complete failure

The difference in the mean system state transitions between the ideal (100%) and high (99%) system diagnostic coverage indicates that the results obtained from the RBD method exaggerate the performance of the system by assuming that all system faults are identified and thoroughly repaired in complex multi-channel systems where repairs go beyond component replacement. Thus, quantifying system diagnostic coverage and repair efficiency is critical to evaluating its reliability and availability performance. In contrast, paralleling subsystems of vastly different diagnostic coverages compromises the performance of the system.

Figure 4-19 depicts the mean state transitions of systems with mixed diagnostic coverages, where it is noticeable that the system's performance is relatively low compared to the high and medium system results, as depicted in Figure 4-18. The low system performance is caused by the decrease in the system's repair rate resulting from the individual subsystems' low diagnostic coverage, increasing the system's probability of transitioning to state S-4. Considering that more failures remain hidden, the system fails at a much lower number of transitions than when the faults are easily identifiable. The characteristic impact of repair efficiency appears to be linear as before at 85% and above, independent of the system diagnostic coverage.

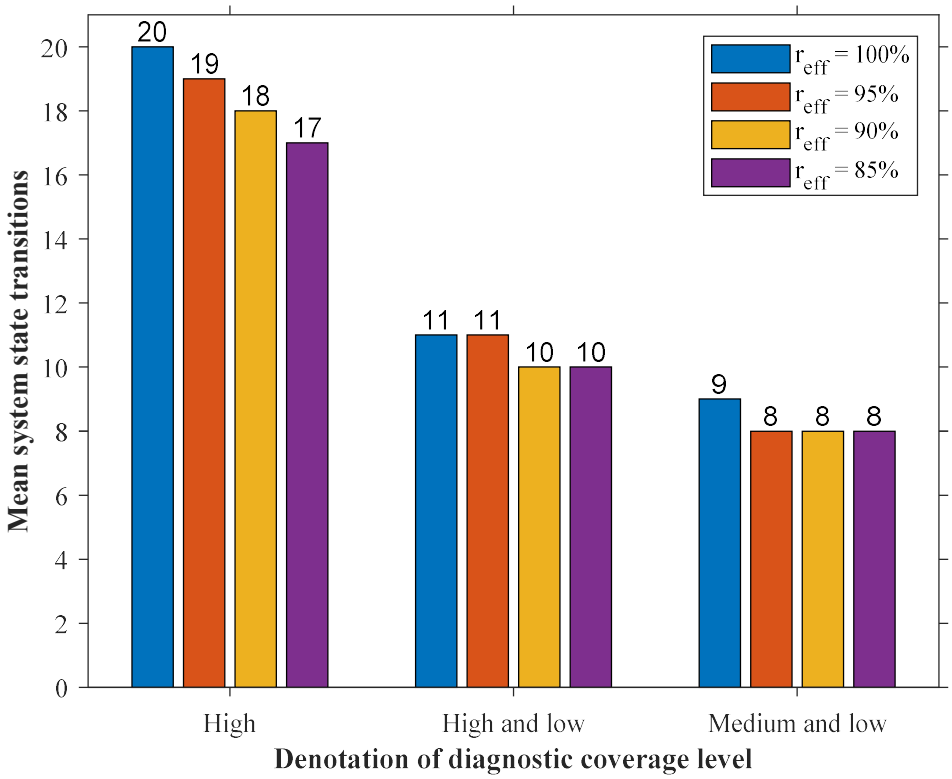


Figure 4-19: Mean system state transitions – Mixed diagnostic coverages

## 4.7 Chapter conclusion

The impact and significance of both the system diagnostic coverage and repair efficiency on the system mean state transitions was demonstrated by incorporating the individual factors

into the Markov model using Systems Thinking to satisfy the requirements of SRS and ISO 13849-1 when IEC 61850 interfaces to IEC 61508 systems in a power distribution centre. Even though the behavioural system response is the same for the different diagnostic coverage levels, the system's performance significantly reduces as the system diagnostic coverage is reduced from the ideal case of 100% down to 60%. However, the similar system response at different diagnostic coverage levels may indicate the dynamic stability of the 'one-out-of-two' system under various imperfect repairs and diagnostic coverage levels. The results emphasise the fact that unknown system faults cannot be repaired. The results also indicate that combinatorial analysis methods do not produce realistic results for reparable multi-channel systems such as the repairable IEC 61850 SCN, primarily applied in mission-critical safety-related protection systems.

Therefore, it is recommended that the diagnostic coverage of power distribution centre devices and the required repair efficiency be quantified to evaluate the system reliability and availability performance. Moreover, it was demonstrated that Markov and mathematical expectation could be used to study the reliability and availability of systems with imperfect repairs; which appears to be more insightful compared to the RBD method for the reason that the simplifying assumptions of the RBD method greatly over-state the reliability and availability performance of the system as observed from the results. Chapter 5 uses the model developed in this chapter and the insights gained from the analysis to investigate the impact of common causes of failure on the system's reliability.

# CHAPTER 5

# IMPACT OF COMMON CAUSE FAILURES

## 5.1 Introduction

Mission-critical systems are designed to tolerate hardware failures to achieve the highest reliability performance based on IEC 61850, which is the prerequisite of the IEC 60870-4 standard [2], [8]. Similarly, the IEC 61508 standard for safety-related systems shares the same prerequisite as the IEC 60870-4 [93]. For this reason, multi-channel systems are used in mission-critical systems within industrial facilities to isolate machinery in process abnormalities. They offer high-reliability performance compared to single-channel systems when their failures are independent between the channels. Undesirably, multi-channel systems introduce Common Cause Failures (CCF) since it is rare that the system's subsystems can be entirely independent. Common Cause Failure factors reduce subsystems' independency in multi-channel architectures [45], [93], [94], [121], [122]. Therefore, incorporating CCFs in reliability models is essential to ensure that meaningful and realistic results are obtained [93], [123]. A Common Cause Failure (CCF) is defined as a single point of failure in a system that simultaneously causes a system's subsystems to become non-functional. The failure could be caused by one or more components failing within a specified time, causing the whole system to become inoperable [93], [122], [124].

Even though dependent failures are primarily due to CCFs and cascading failures, both types of failures are modelled as CCFs in literature [45], [123]–[126]. Hence, dependent failures occur as a result of common stressors that affect multiple subsystems or components in a system [93], [121], [124]. Common causes can result from root causes or coupling factors, where root causes are related to system design and engineering, manufacturing and installation, testing and commissioning, and operating and maintenance. Coupling factors, however, can be associated with the same physical location and design, same hardware and or software, same installation crew and same maintenance team [45], [122], [124], [126]. Nevertheless, root causes are the main reason for component failures, whereas coupling factors make a component susceptible to the same root cause. Hence, mitigating against root causes does not necessarily eliminate coupling factors, making the modelling of CCFs complicated. Consequently, engineers' modelling of CCFs follows a fixed proportion estimation approach based on the subsystem’s overall failure rate as the probability of CCF occurrence, which does not require system-specific data of the CCF itself [124], [127].

The consideration of CCFs as hazards due to which systems can fail necessitates their careful evaluation in system reliability studies to ensure that the reliability performance of the system is not over-stated since they tend to increase joint system probability of failure, which leads to inaccurate system reliability evaluation results [94], [122], [125]. Explicit modelling

and analysis of CCF impact on the reliability and availability of a system can be a challenging task when the failure probabilities due to CCFs are to be used in the development of the system reliability models [98], [124], [127]. Hence, various reliability models have been developed to ease the quantification and the modelling effort of CCFs over the years. The models share one main objective even though their approaches may differ, which is to quantify the level of both the dependent and independent factors [93], [123], [124], [127]. The β-factor model is used in this research work and is discussed in section 5.2. Section 5.3 presents the modelling of CCFs in systems with imperfect repairs and limited diagnostic coverage based on the Markov process. Case studies results and discussions are presented in section 5.4. The findings and conclusions resulting from the studies are presented in section 5.5.

## 5.2 The beta factor model

The β-factor model is the most preferred and commonly used parametric method of evaluating the impact of CCFs in 'one-out-of-two' system configurations [93], [121], [124]. The model is also presented and discussed in IEC 61508 standard as one of the recommended methods of determining the effect of CCFs in multi-channel systems. Modelling of CCFs aims to determine their effect on the system reliability and availability performance and enable the development of extenuating strategies against their impact [98], [124]. Parametric models can be classified into shock and non-shock models. Shock models incorporate CCF basic mechanisms, while non-shock models are based only on the failure probabilities of CCFs. The β-factor model is based on historical time to failure that is broadly applied; however, it is simplified since it does not explicitly account for the individual sub-factors [128].

Nevertheless, considering that only the level of CCFs is needed to determine the impact of common causes on the system's reliability, the β-factor model is used to model CCFs in 'one-out-of-two' system configurations because its application is simple to comprehend and apply. Moreover, it lessens the effort needed to analyse the results [93], [123], [124]. As a single parameter model, the β-factor model assumes that a constant fraction of the system, subsystem or component failure rate can be attributed to the failure probability of the CCFs [123], [124]; such that the total system failure rate $\lambda_T$ is given by (5-1); where $\lambda_{CCF}$ represents the failure rate due to CCFs while $\lambda_{IND}$ represents the failure rate due to the independent components [127],

$$\lambda_T = \lambda_{CCF} + \lambda_{IND} \tag{5-1}$$

The estimation of the β-factor is based on the system diversity or properties, as well as the architecture [98]. Figure 5-1 depicts a Reliability Block Diagram (RBD) model of a 'one-out-of-two' multi-channel system comprising subsystem A and subsystem B, where the failure rates of subsystems A and B are $\lambda_A$ and $\lambda_B$, respectively.

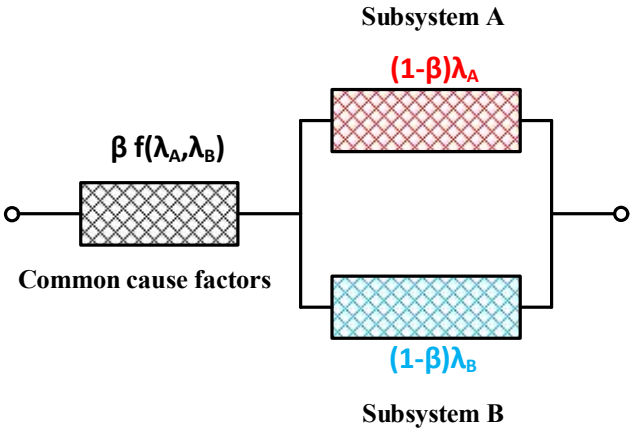


Figure 5-1: Reliability block diagram model of 'one-out-of-two' system incorporating CCFs based on the β-factor model

Notably, the failure of any component represented by the failure rate function (5-2) causes the overall system mission to fail. Hence, the RBD model offers an effortless comprehension of the β-factor model application. The model of Figure 5-1 is remodelled using the Markov process introduced in Chapter 3 and Chapter 4 to enable integrating CCFs and imperfect repairs [2], [8], [12], [80], [91],

$$\lambda_{CCF} = \beta f(\lambda_A, \lambda_B) \tag{5-2}$$

The failure rate associated with the independent failures in the system is represented by (5-3) [121], [122],

$$\lambda_{IND} = (1-\beta)\lambda_A + (1-\beta)\lambda_B \tag{5-3}$$

Figure 5-2 depicts the 'one-out-of-two' Markov state transition diagram model integrating the β-factor [98]. It is assumed that the CCF rate function $f(\lambda_A, \lambda_B)$ given by (5-2) is an averaging function of the two subsystem's failure rates; such that the CCF rate is the fraction of the CCF function value determined by the β-factor. In comparison to the model presented in Chapter 4, the model depicted in Figure 5-2 shows that a system state transition from state S-1 to S-4 is possible due to the presence of CCFs, of which the failure rate is given by (5-2). The complete state transition probability matrix of the 'one-out-of-two' system model depicted in Figure 5-2 is given by (5-4). The Markov state transition β-factor model and its associated state transition matrix are used to enhance the 'one-out-of-two' Markov state transition diagram model presented in Chapter 4 to investigate the impact of CCFs on the reliability performance of the system with imperfect repairs. The integration of the CCF effect on the 'one-out-of-two' model with imperfect repairs and limited system diagnostic coverage is presented in subsection 5.3.

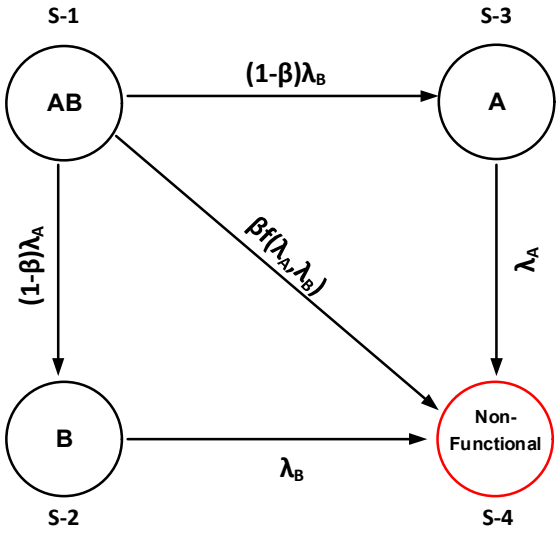


Figure 5-2: Markov state transition diagram of 'one-out-of-two' system incorporating CCFs based on the β factor model

$$P = \begin{bmatrix} 1-(1-\beta)\lambda_A-(1-\beta)\lambda_B-\beta f(\lambda_A,\lambda_B) & (1-\beta)\lambda_A & (1-\beta)\lambda_B & \beta f(\lambda_A,\lambda_B) \\ 0 & 1-\lambda_B & 0 & \lambda_B \\ 0 & 0 & 1-\lambda_A & \lambda_A \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (5\text{-}4)$$

## 5.3 Modelling imperfect repairs and common cause failures

The 'one-out-of-two' system model presented in Chapter 4 is enhanced by incorporating CCFs using the β-factor model described by (5-4) to investigate the impact of imperfect repairs at different CCFs levels. Figure 5-3 depicts the Markov state transition diagram of the 'one-out-of-two' system with imperfect repairs and CCFs [8], [60], [75]. Compared to the 'one-out-of-two' model presented in Chapter 4, the model of Figure 5-3 shows that the system can transit from state S-1 to state S-4 depending on the existence and the level of CCFs in the system. The associated Markov transition probability matrix of the model depicted in Figure 5-3 is given by (5-5), which enables the investigation of system reliability performance based on the number of mean system state transitions at various levels of CCFs; depending on the selected value of the β parameter [8], [98]. The model's flexibility to incorporate various factors enables the impact of the CCFs on system reliability performance to be determined at different levels of imperfect repairs (viz. repair efficiency and system diagnostic coverage).

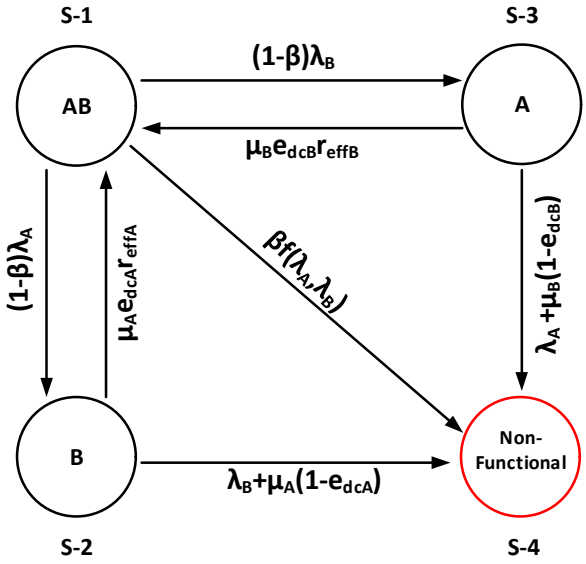


Figure 5-3: Markov state transition diagram of 'one-out-of-two' system with imperfect repairs and CCFs

$$P = \begin{bmatrix} 1-(1-\beta)\lambda_A-(1-\beta)\lambda_B-\beta f(\lambda_A,\lambda_B) & \cdots & (1-\beta)\lambda_A & (1-\beta)\lambda_B & \cdots & \beta f(\lambda_A,\lambda_B) \\ \mu_A e_{dcA} r_{effA} & & 1-\mu_A e_{dcA} r_{effA}-(\lambda_B+\mu_A(1-e_{dcA})) & 0 & & \lambda_B+\mu_A(1-e_{dcA}) \\ \mu_B e_{dcB} r_{effB} & & 0 & 1-\mu_B e_{dcB} r_{effB}-(\lambda_A+\mu_B(1-e_{dcB})) & & \lambda_A+\mu_B(1-e_{dcB}) \\ 0 & & 0 & 0 & & 1 \end{bmatrix} \quad (5\text{-}5)$$

Henceforth, the system's subsystems are assumed to be not entirely independent to improve the accuracy of the reliability performance evaluation results, except in exceptional cases where β is set to zero to represent the non-existence of CCFs in the system [98]. The following section presents the case studies of system reliability performance.

## 5.4 Case studies results and discussions

This section presents the results and analysis of the impact of CCFs on the reliability performance of the 'one-out-of-two' system configuration depicted in Figure 5-3. The basis of the case studies investigated in this chapter is considered to be the results of the 'one-out-of-two' system presented in Chapter 4, where the two subsystems A and B were assumed to be completely independent. Hence, the impact of CCFs is investigated for the three diagnostic

coverage levels denoted in ISO 13849-1. Table 4-4 presents the different system diagnostic coverage levels presented in Chapter 4.

The following assumptions are made to enable the case studies comparable to the results presented in Chapter 4, being cognizant that different levels of subsystem repair efficiency and diagnostic coverage can be simulated for analysis if so required.

a) Subsystems A and B are of the same technology; hence they have the same diagnostic capability.
b) The same resources support both subsystems A and B such that equal repair efficiencies are applied to both subsystems.
c) The system is fully functional at the beginning of the simulation.

Although the system is assumed to be fully functional at the begging of the simulation, any system state can be selected as the system's initial state assuming a partial failure at the beginning of the simulation. Figure 5-4 depicts the system's transition probability heatmap at 90% diagnostic coverage and 95% repair efficiency, assuming that the level of CCFs represented by β is 25% to illustrate the system's characteristic behaviour.

In contrast to the system configuration analysed in Chapter 4, it can be observed that the system under consideration can transition into either states S-2, S-3 or S-4 with a high probability that it will transition into S-2 given that its initial state is S-1. Thereafter, the system would transition back to state S-1 except if it has transitioned into state S-4, the system's failsafe recurrent state. The probability of the system transitioning to state S-4 is relatively low, at about 0.15. This condition implies that the system would probably transition between states S-1, S-2 and S-3 before transitioning to state S-4. Even so, the system can transition to state S-4 any time if one or more of the dependent failures occur. Hence, the performance analysis of the systems under consideration is based on the system’s mean state transitions before failure, which represents the state transition characteristics of the system in its transient state.

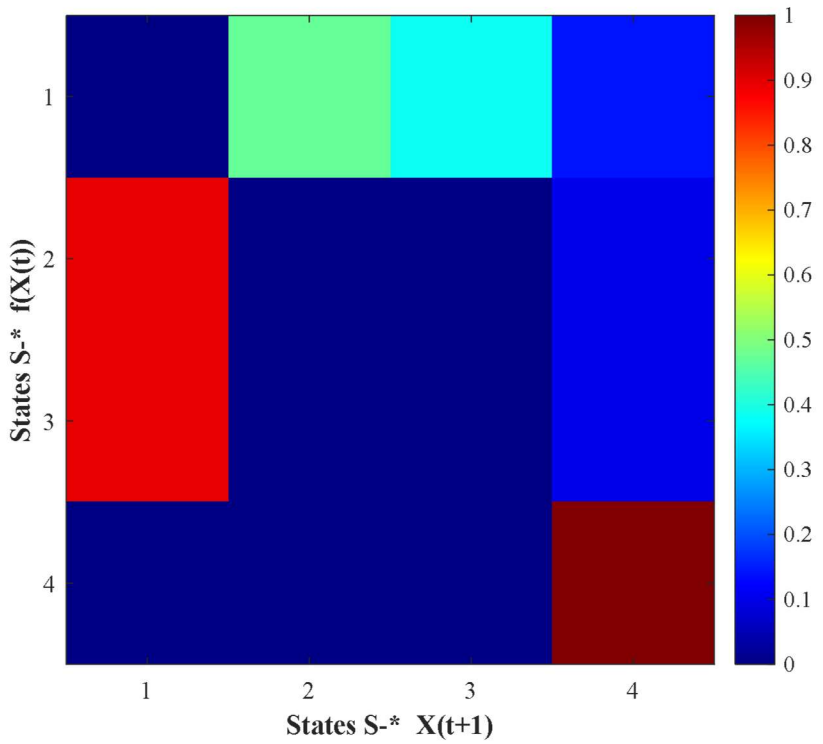


Figure 5-4: Transition probability matrix heatmap with CCFs

### 5.4.1 High diagnostic coverage

In this case study, the system diagnostic coverage level is assumed to be 99%, whereas the system's repair efficiency is 95%. The selected level of repair efficiency is based on the case studies results of Chapter 4, where its impact was observed to be marginally closer to 100%. Also, selecting a level below 100% acknowledges that 100% repair efficiency is challenging to achieve. Figure 5-5 depicts the reliability of the 'one-out-of-two' system depicted in Figure 5-3 for different levels of common causes of failure represented by the β-factors.

It can be observed from Figure 5-5 that the system has the highest reliability performance level when the β-factor is zero; this is because a zero β-factor represents a condition where the subsystems A and B are assumed to be entirely independent of each other. Hence, the probability of the two subsystems A and B simultaneously failing is improbable. Nevertheless, the system's reliability rapidly decreases with increasing common causes of failure as the failure probability due to CCFs increases, represented by the direct state transition from state S-1 to S-4. The results also indicate that the reliability performance is sensitive to changes at low levels of the β-factor. Moreover, the change in the system's probability performance curves can be precisely associated with different levels of mean state transitions, which in turn represents a change in reliability performance. Figure 5-6 depicts the reliability of the system when its subsystems have low repair efficiencies.

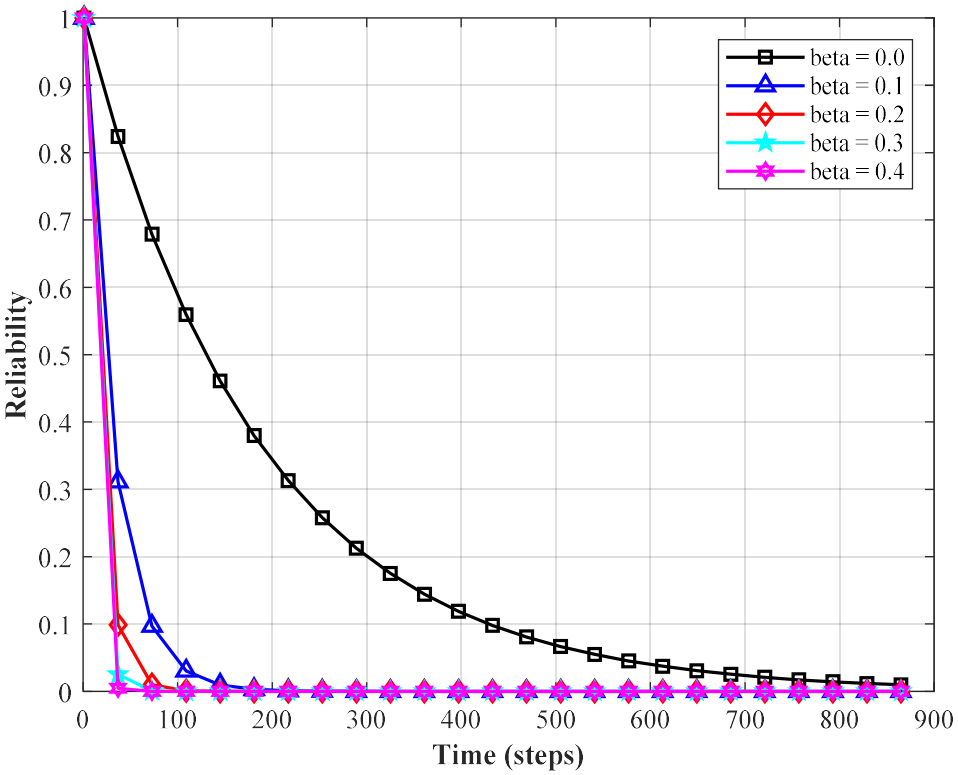


Figure 5-5: Reliability performance at 99% diagnostic coverage and 95% repair efficiency

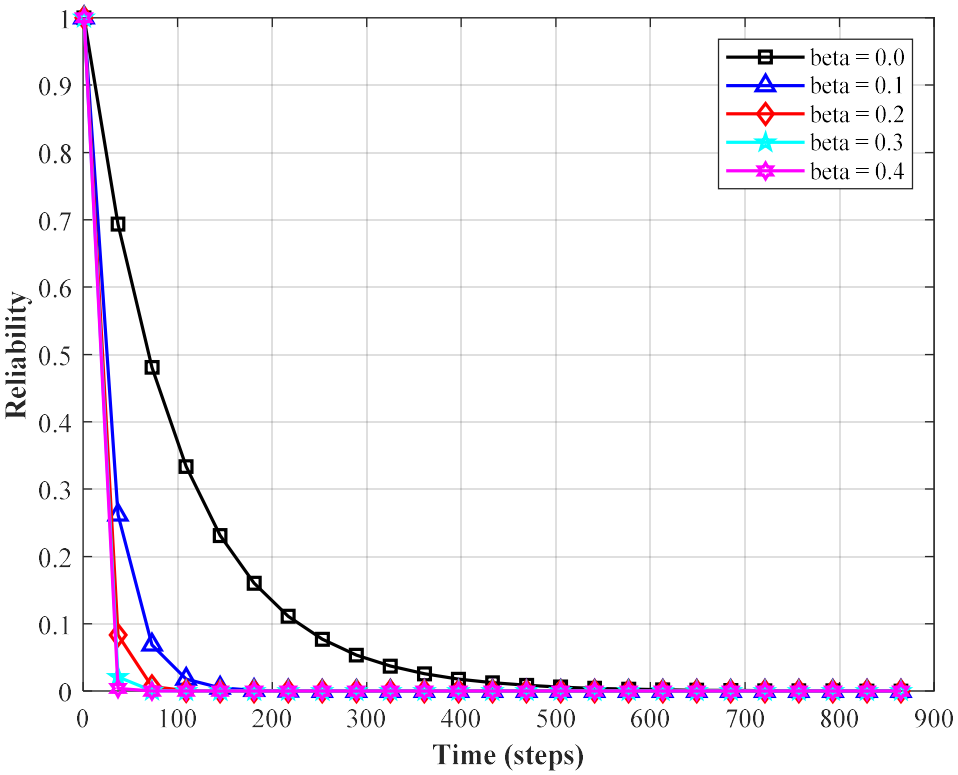


Figure 5-6: Reliability performance at 99% diagnostic coverage and 50% repair efficiency

The low level of repair efficiency represents a high level of incomplete and incorrect repairs on the system. The case study's objective is to investigate the impact of CCFs on system reliability performance when the quality of repairs is deficient. Hence, the repair efficiency of the individual subsystems is assumed to be 50% for simulation purposes. It is noticeable that the impact of CCFs is relatively low to changes of the β-factor than in the previous case study. Moreover, the impact reduces as the level of CCFs increase, as was the case when the repair efficiency was 95%. As expected, the system's reliability becomes zero at lesser time steps, as depicted in Figure 5-6 for the different levels of CCFs represented by the β-factor. However, the impact of CCFs appears to have a small impact on system reliability at low repair efficiency levels than when it is high. The system's behaviour can be attributed to reducing the subsystems' repair rates, which reduces the system's transition probabilities from states S-2 and S-3 back to S-1, whereas the system's probability to transition to state S-4 increases. Figure 5-7 depicts the system mean state transitions at different levels of common causes of failures.

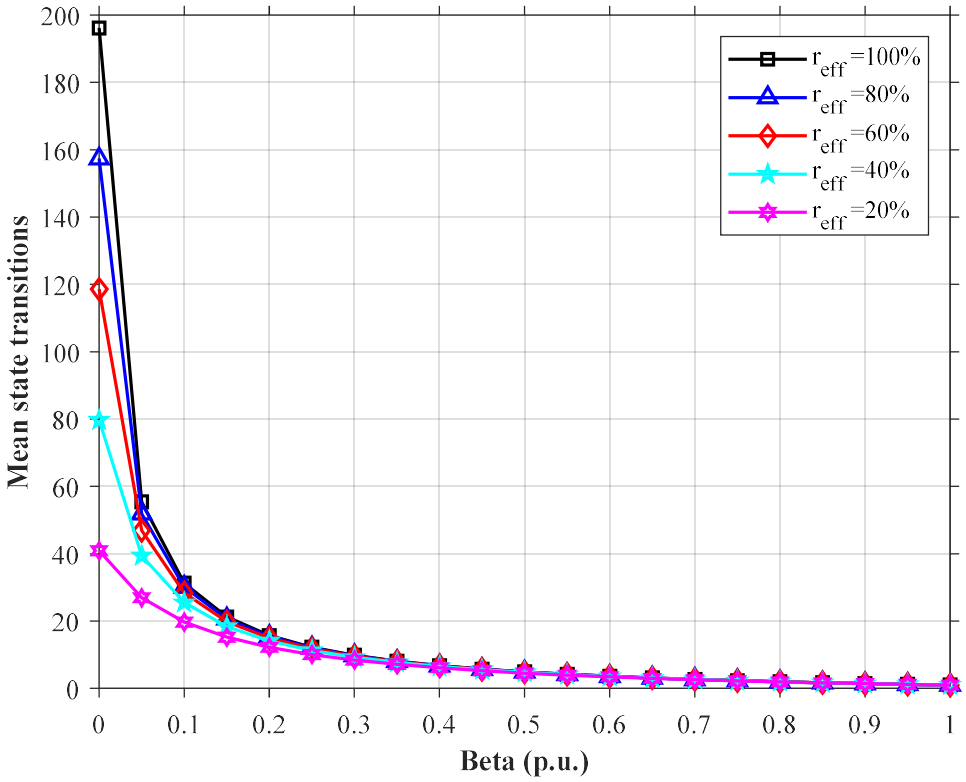


Figure 5-7: Mean system state transitions with imperfect repairs – 99% diagnostic coverage

Notably, the mean system state transitions are highly sensitive to the changes of the β-factor, particularly at low levels of β, which indicates that the mere presence of CCFs significantly reduces the performance regardless of the level of common causes of failure. This observation is the same for the different repair efficiency levels.

### 5.4.2 Medium diagnostic coverage

The system diagnostic coverage level is assumed to be 90%, whereas the repair efficiency remains unchanged at 95%. Figure 5-8 depicts the reliability of the 'one-out-of-two' system depicted in Figure 5-3 for different levels of common causes of failure represented by the β-factors. Again, it is noticeable from Figure 5-8 that the system maintains the highest reliability performance level when the β-factor is zero, as in the case when the diagnostic coverage was considered to be 99%. Expectedly so, the reliability decreases with increasing common causes of failure as the system failure probability increases. The system's reliability becomes zero at even much lower system's state transitions when more system faults remain hidden than when the diagnostic coverage is high at 99%.

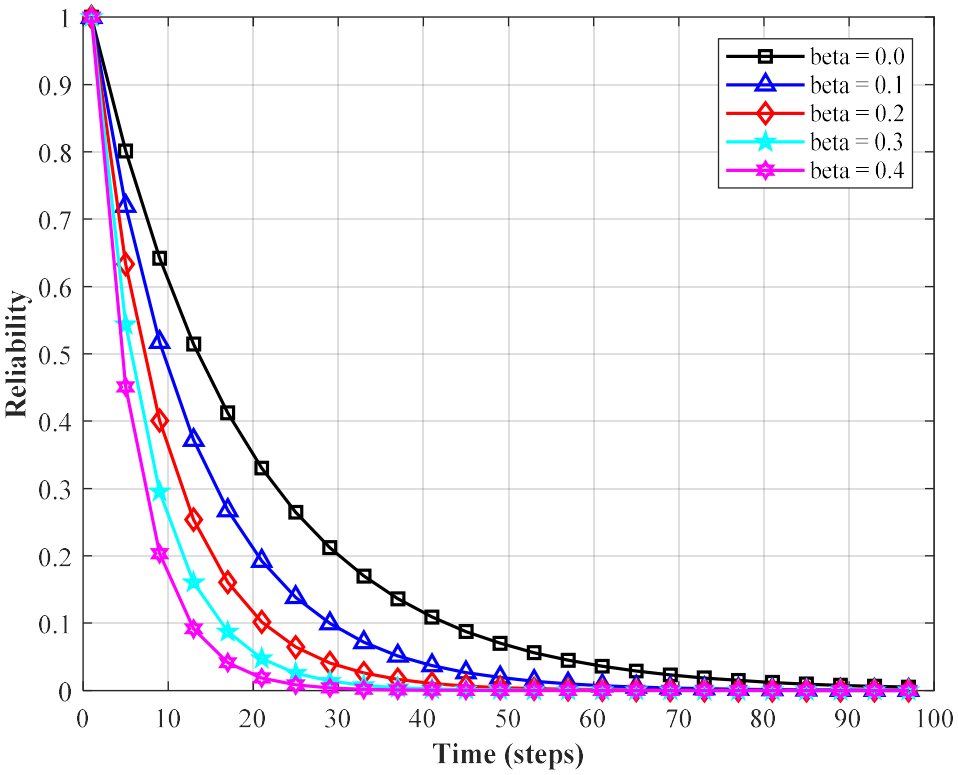


Figure 5-8: Reliability performance at 90% diagnostic coverage and 95% repair efficiency

Figure 5-9 depicts the system's reliability when its subsystems have low repair efficiencies of 50%. As before, the low repair efficiency level represents a condition of poor quality of repairs on the system, enabling the determination of the impact of CCFs on the system reliability performance when the quality of repairs is deficient. It can be observed that the impact of CCFs is relatively uniform for the levels of the β-factors, and the relative impact is less compared to the case study when the repair efficiency was assumed to be 95%. The impact also reduces uniformly as the level of CCFs increases, as was the case when the repair efficiency was 95%.

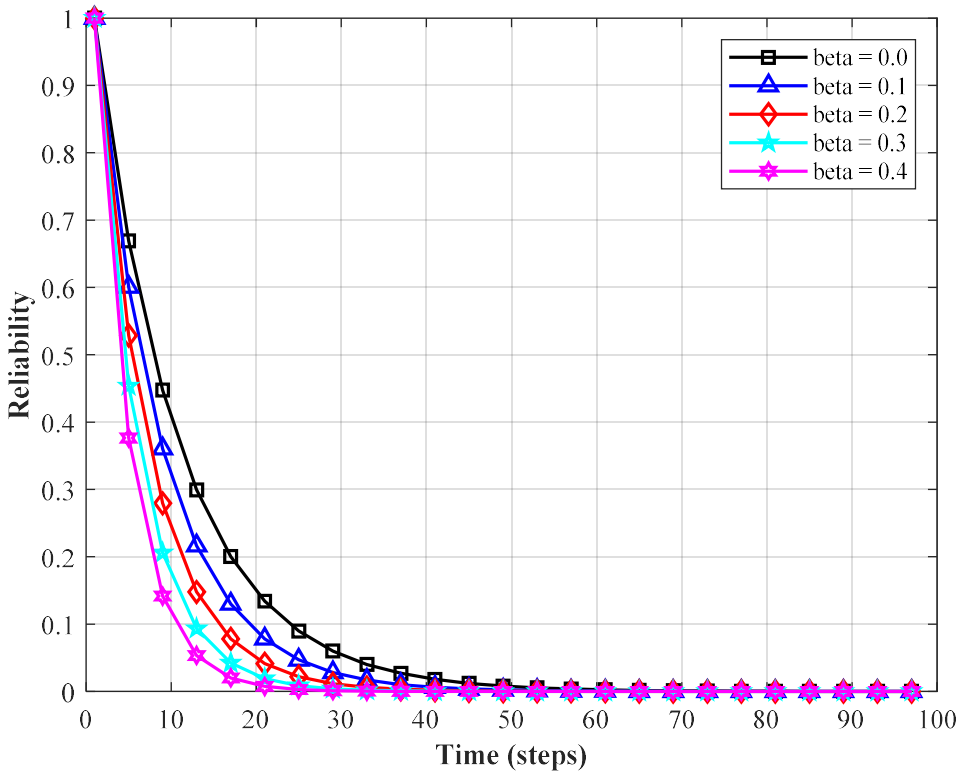


Figure 5-9: Reliability performance at 90% diagnostic coverage and 50% repair efficiency

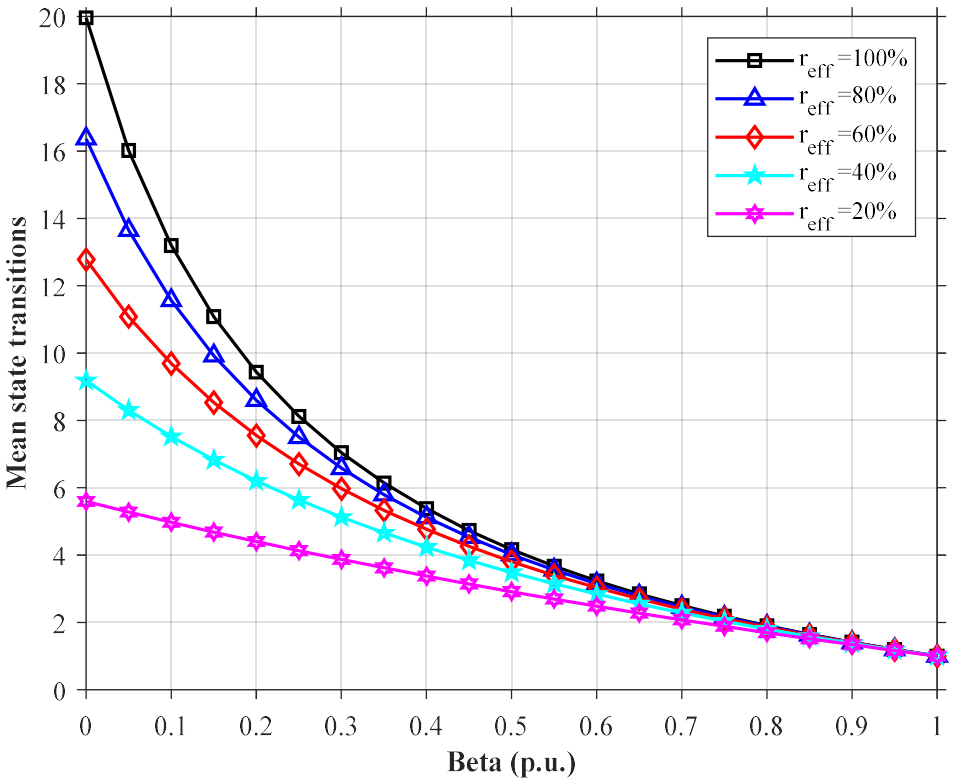


Figure 5-10: Mean system state transitions with imperfect repairs – 90% diagnostic coverage

As expected, the system's reliability becomes zero at lesser time steps, as depicted in Figure 5-9 for the different levels of CCFs represented by the β-factors. However, the impact of CCFs appears to have even a minor effect on system reliability at low repair efficiency levels than when it is high. Again, the system's behaviour can be attributed to reducing the subsystems' repair rates, which reduces the system's transition probabilities from states S-2 and S-3 back to S-1, whereas the system's probability of transitioning to state S-4 increases. Figure 5-10 depicts the system mean state transitions at different levels of common causes of failures. The mean system state transitions magnitude is marginally sensitive to the changes of the β-factor as would be expected; this observation is the same for the different levels of system repair efficiency as in the case when the diagnostic coverage was high at 99% even though the number of transitions has significantly reduced, particularly at low levels of β.

### 5.4.3 Low diagnostic coverage

The system diagnostic coverage level is assumed to be 60% for this case study. Initially, the repair efficiency is 95%, as in the previous case studies. Figure 5-11 depicts the reliability of the 'one-out-of-two' system depicted in Figure 5-3 for different levels of common causes of failure represented by the β-factors, where it is noticeable again that the system has the highest reliability performance level when the β-factor is zero similarly to the previous case studies at 99% and 90% diagnostic coverage levels.

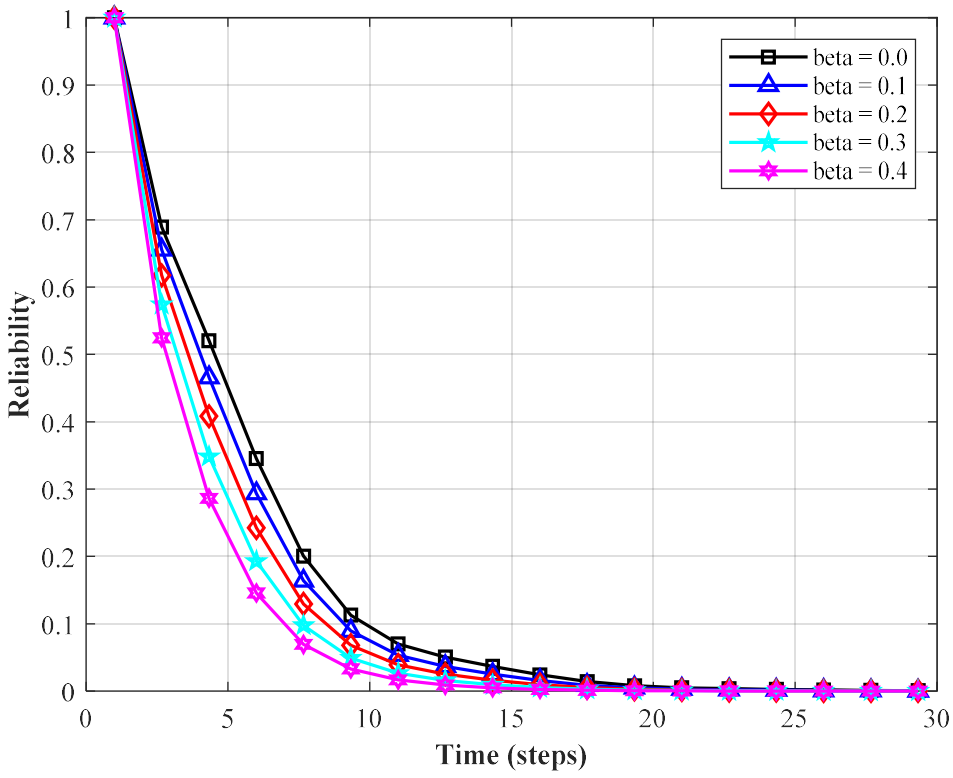


Figure 5-11: Reliability performance at 60% diagnostic coverage and 95% repair efficiency

Contrary to the results obtained when the diagnostic coverage was at 99% and 90%, the system's reliability does not significantly decrease with increasing common causes of failure but decreases marginally. Moreover, the reliability becomes zero at only 20 transitions compared to 875 and 90 transitions when the system diagnostic coverage was at 99% and 90% for β = 0, respectively, as more system faults remain hidden. Even so, the system is characterised by low sensitivity to changes in β levels. Figure 5-12 depicts the system's reliability when its subsystems have low repair efficiencies at 50%. As before, the low repair efficiency level represents a condition of poor quality of repairs on the system.

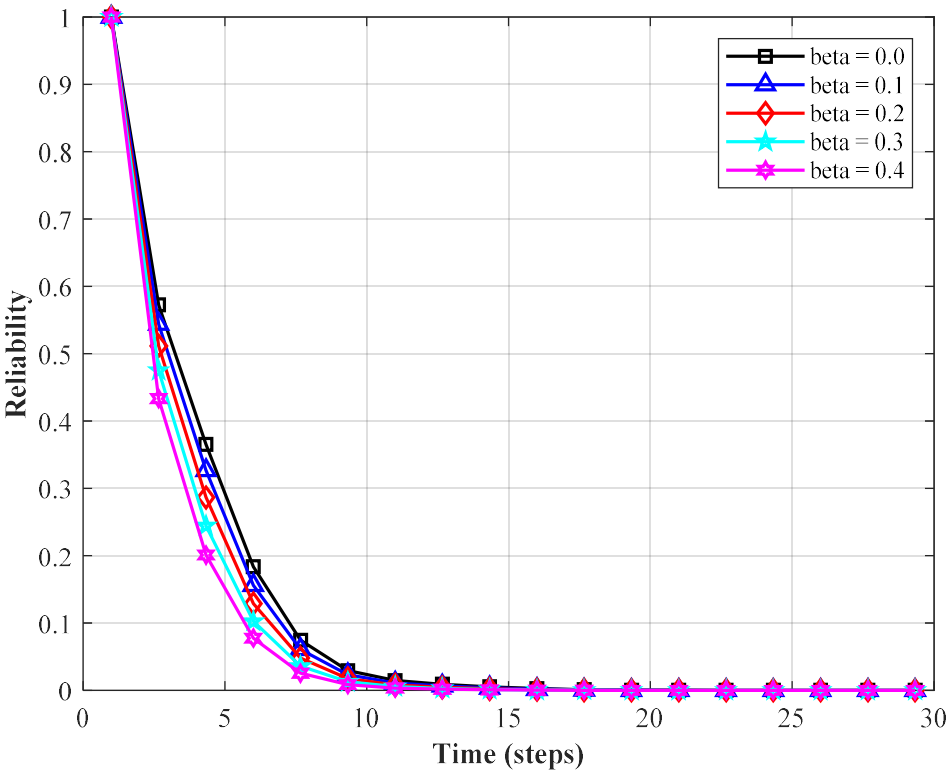


Figure 5-12: Reliability performance at 60% diagnostic coverage and 50% repair efficiency

It is noticeable that the impact of CCFs is relatively low to changes in the β-factor level compared to the scenario when the repair efficiency was assumed to be 95%. Expectedly so, the impact also increases as the level of CCFs increases. As expected, the system's reliability becomes zero at lesser time steps, as depicted in Figure 5-12 for the different levels of CCFs represented by the β-factors. Moreover, the impact of CCFs on system reliability appears to be proportionally the same at all repair efficiency levels as before. The system's behaviour can be attributed to reducing the subsystems' repair rates, which reduces the system's transition probabilities from states S-2 and S-3 back to S-1, whereas the system's probability of transitioning to state S-4 increases. Figure 5-13 depicts the mean state transitions at different

levels of common causes of failures. The mean state transitions are relatively not sensitive to the changes of the β-factor.

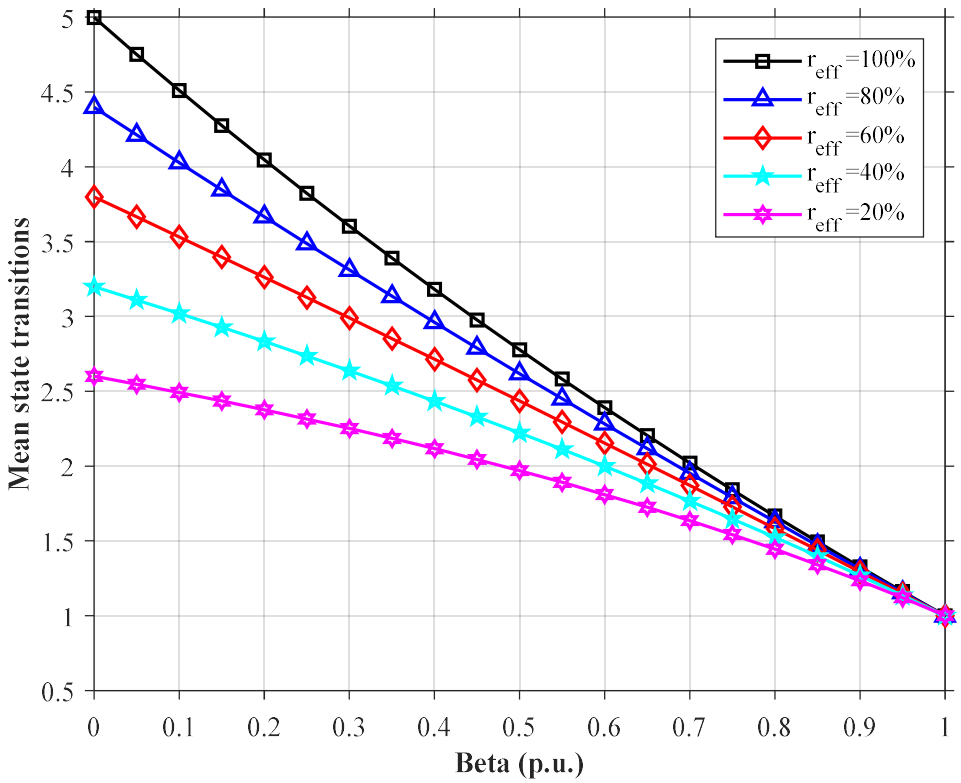


Figure 5-13: Mean system state transitions with imperfect repairs – 60% diagnostic coverage

### 5.4.4 Mixed diagnostic coverages

Three system configurations are considered in this case study (viz 'high and low', 'medium and low' and 'high and medium' configurations). The individual subsystems A and B are assumed to be of different technology to demonstrate the system's performance when the subsystems have different diagnostic coverage levels. Table 5-1 presents the diagnostic coverage levels of the 'one-out-of-two' system under consideration.

Table 5-1: Case study system diagnostic coverage levels

| System configuration | High and low (B-1) | Medium and low (B-2) | Medium and low (B-3) |
|---|---|---|---|
| Subsystem A diagnostic coverage ($e_{dcA}$) | 99% | 90% | 99% |
| Subsystem B diagnostic coverage ($e_{dcB}$) | 60% | 60% | 90% |

**a) Subcase study B-1**

The subsystem's diagnostic coverage levels are assumed to be 99% and 60% for subsystems A and B. The system performance is initially investigated at 95% repair efficiency. Figure 5-14 depicts the reliability of the 'one-out-of-two' system depicted in Figure 5-3 for different levels of common causes of failure represented by the β-factors. It is noticeable again that the system has the highest reliability performance level when the β-factor is zero, similarly to the previous cases. Contrary to the results obtained when the diagnostic coverage was at 99%, 90% and 60%, the system's reliability does not significantly decrease with increasing common causes of failure but decreases uniformly initially.

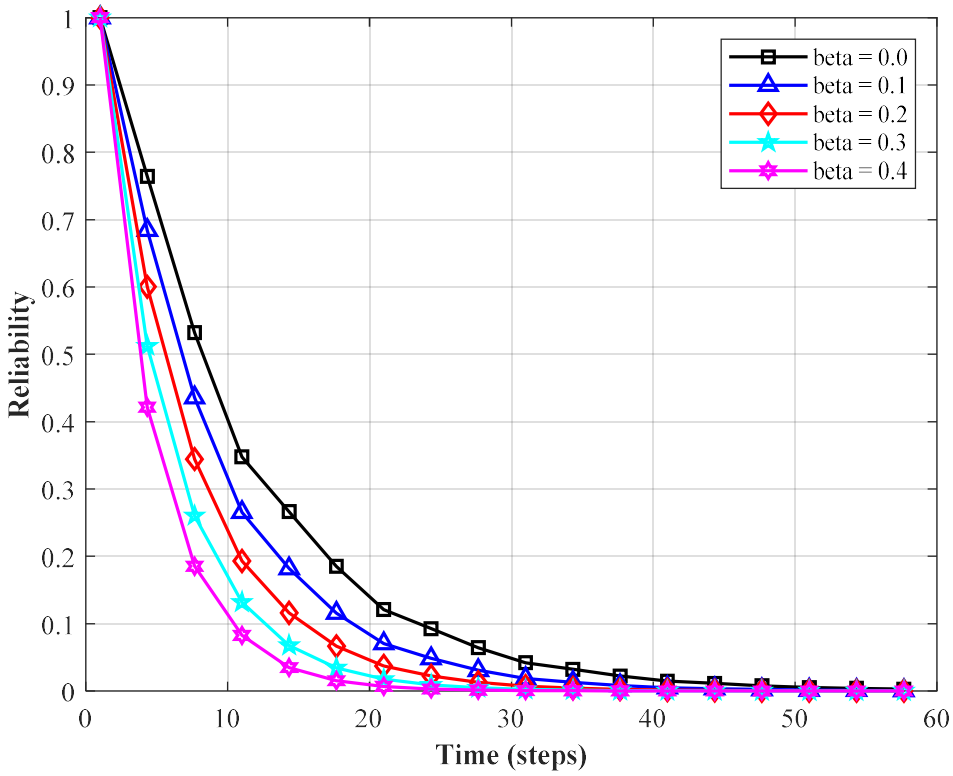


Figure 5-14: Reliability performance at B-1 diagnostic coverage and 95% repair efficiency

Figure 5-15 depicts the system's reliability when its subsystems have low repair efficiencies at 50%. As before, the low repair efficiency level represents a condition of poor quality of repairs on the system. It is noticeable that the impact of CCFs remains uniform for all levels of the β-factors. Also, the relative impact is less than when the repair efficiency was assumed to be 95%. As expected, the system's reliability becomes zero at lesser time steps, as depicted in Figure 5-15 for the different levels of CCFs represented by the β-factors. Again, the system's behaviour can be attributed to reducing the subsystems' repair rates, which reduces the system's transition probabilities from states S-2 and S-3 back to S-1, whereas the system's probability of transitioning to state S-4 increases. Figure 5-16 depicts the mean state

transitions at different levels of common causes of failures. The mean state transitions are relatively sensitive to the changes of the β-factor as would be expected based on the reliability curves.

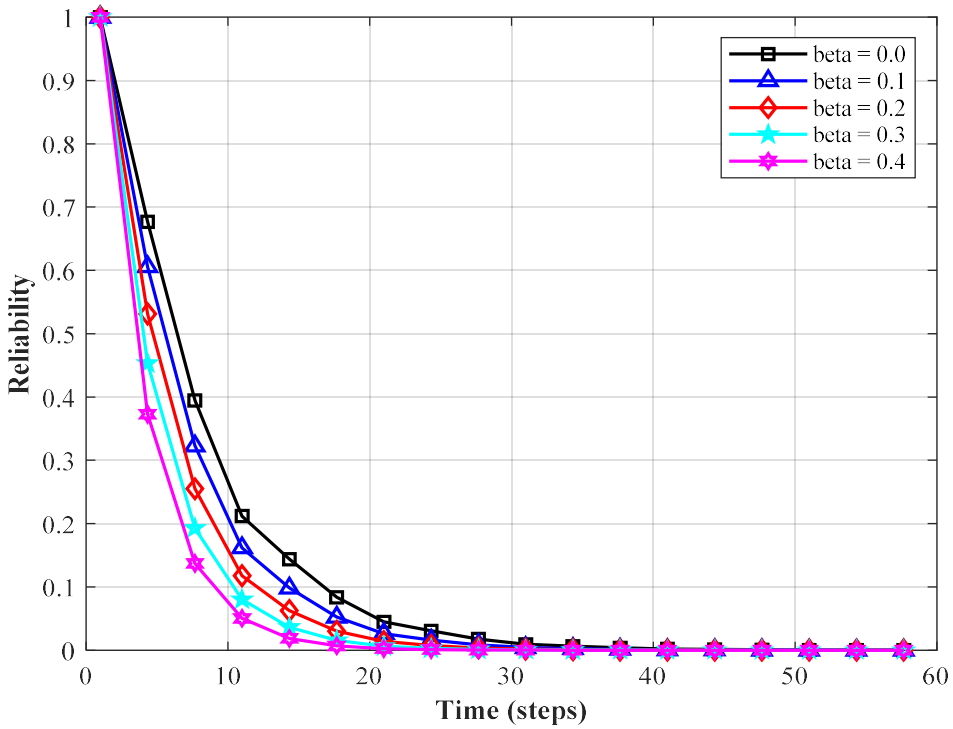


Figure 5-15: Reliability performance at B-1 diagnostic coverage and 50% repair efficiency

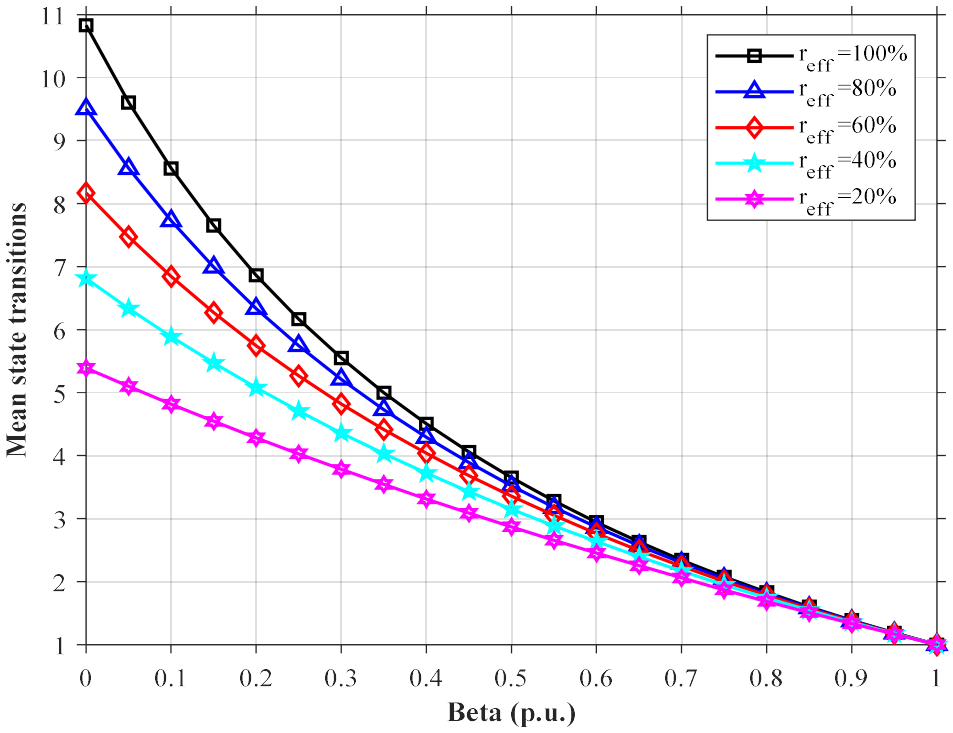


Figure 5-16: Mean system state transitions with imperfect repairs at B-1 diagnostic coverage

**b) Subcase study B-2**

The subsystem's diagnostic coverage levels are assumed to be 90% and 60% for subsystems A and B. As before, the system performance is investigated at 95% first. Figure 5-17 depicts the reliability of the 'one-out-of-two' system depicted in Figure 5-3 for different levels of common causes of failure represented by the β-factors. It is noticeable again that the system has the highest reliability performance level when the β-factor is zero, similarly to the previous case study at 99% and 60% diagnostic coverage levels for subsystems A and B, respectively.

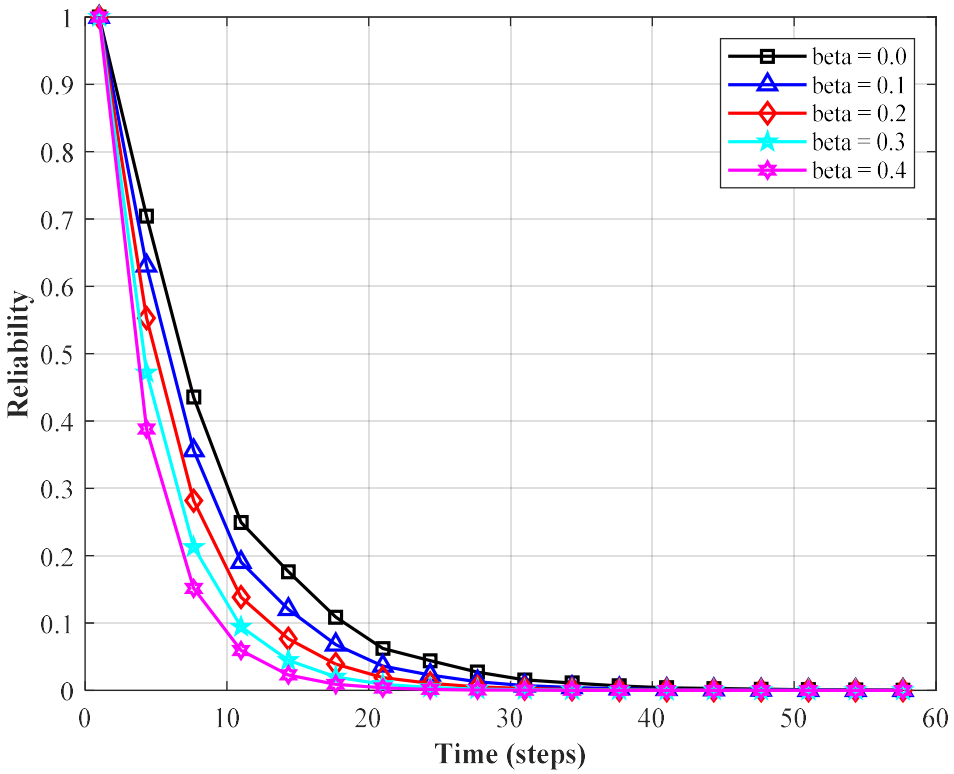


Figure 5-17: Reliability performance at B-2 diagnostic coverage and 95% repair efficiency

In contrast to the results obtained when the diagnostic coverage was at 99% and 60% for subsystems A and B, the system's reliability does not significantly decrease with increasing common causes of failure but decreases uniformly. Nevertheless, the system is still characterised by low sensitivity to changes in β levels. Figure 5-18 depicts the system's reliability when its subsystems have 50% repair efficiencies. It is noticeable that the impact of CCFs is uniform on all levels of the β-factor, although the relative impact is less compared to the scenario when the repair efficiency was assumed to be 95%. Expectedly so, the impact also reduces as the level of CCFs increases. The system's reliability becomes zero at lesser time steps, as depicted in Figure 5-18 for the different levels of CCFs represented by the β-factor.

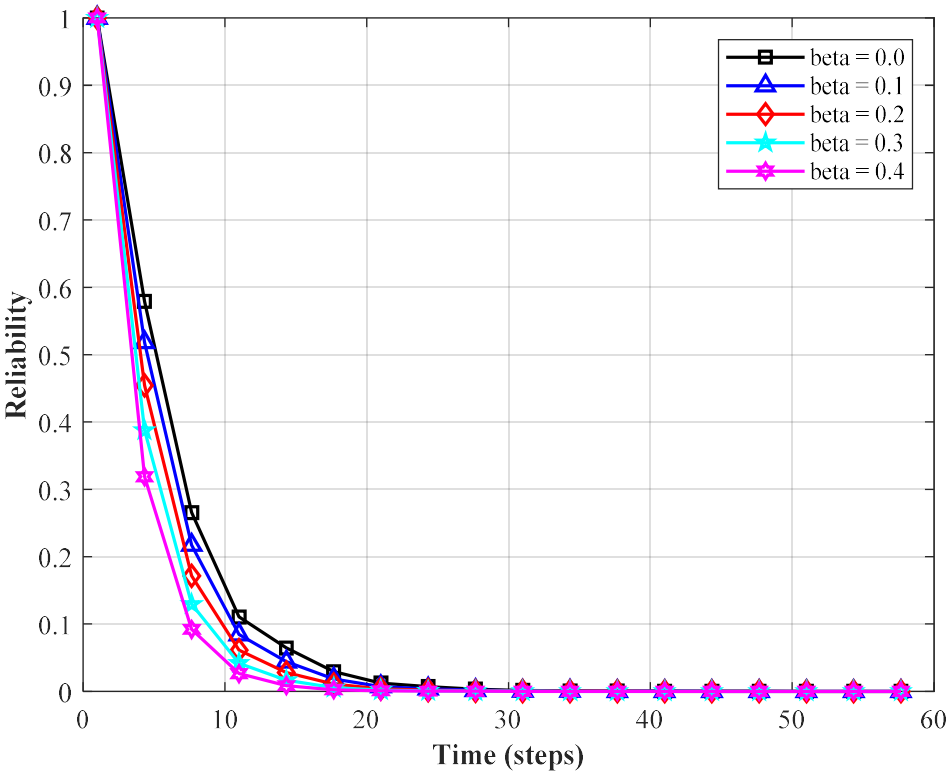


Figure 5-18: Reliability performance at B-2 diagnostic coverage and 50% repair efficiency

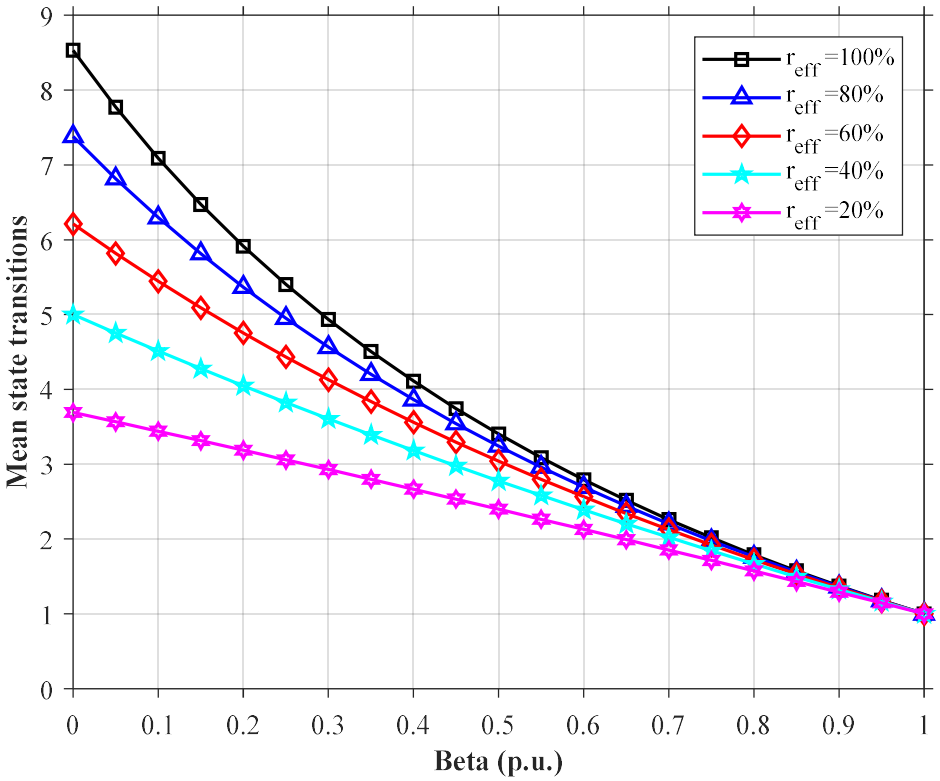


Figure 5-19: Mean system state transitions with imperfect repairs at B-2 diagnostic coverage

Again, the system's behaviour can be attributed to reducing the subsystems' repair rates, which reduces the system's transition probabilities from states S-2 and S-3 back to S-1, whereas the system's probability of transitioning to state S-4 increases. Figure 5-19 depicts the mean state transitions at different levels of common causes of failures. The mean state transitions are relatively less sensitive to the changes of the β-factor as would be expected based on the reliability curves.

**c) Subcase study B-3**

The subsystem's diagnostic coverage levels are assumed to be 99% and 90% for subsystems A and B in this case study. Figure 5-20 depicts the reliability of the 'one-out-of-two' system depicted in Figure 5-3, where it is noticeable again that the system has the highest reliability performance level when the β-factor is zero, as would be expected.

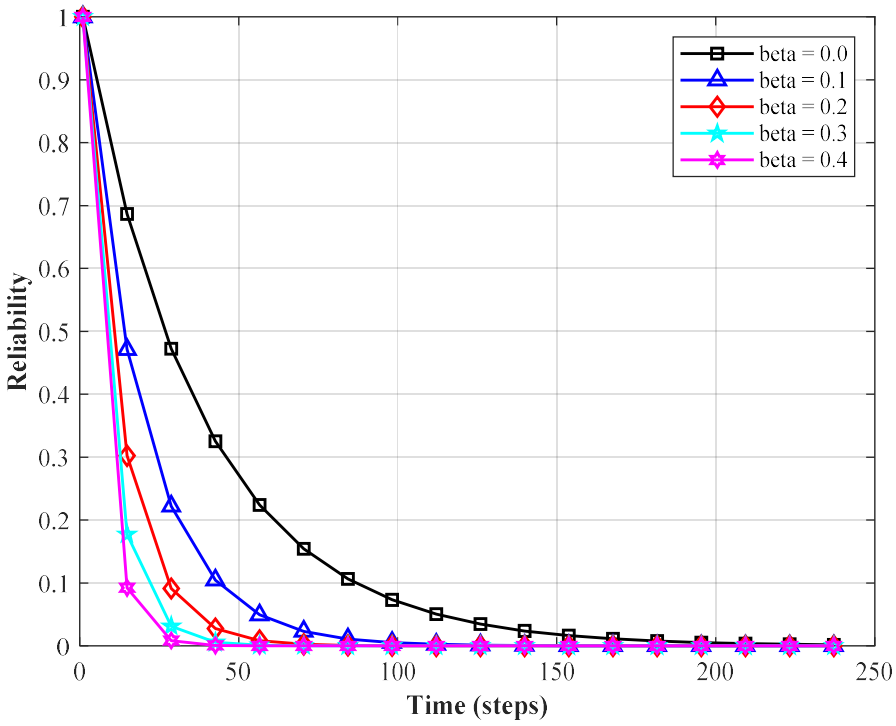


Figure 5-20: Reliability performance at B-3 diagnostic coverage and 95% repair efficiency

The system is still characterised by low sensitivity to changes in β levels. Figure 5-21 depicts the system's reliability when its subsystems have 50% repair efficiencies. Again, it is noticeable that the impact of CCFs is evident on all levels of the β-factors, although the relative impact is less compared to the scenario when the repair efficiency was assumed to be 95%. Also, the impact reduces as the level of CCFs increases. The system's reliability becomes zero at lesser time steps, as depicted in Figure 5-21 for the different levels of CCFs represented by the β-factor.

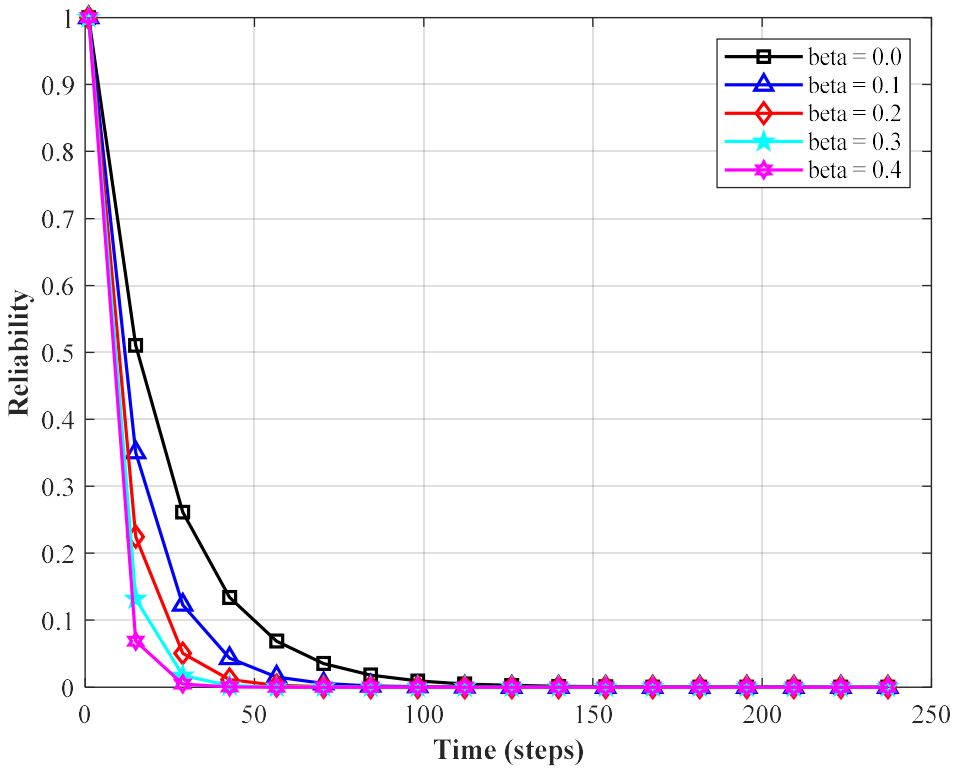


Figure 5-21: Reliability performance at B-3 diagnostic coverage and 50% repair efficiency

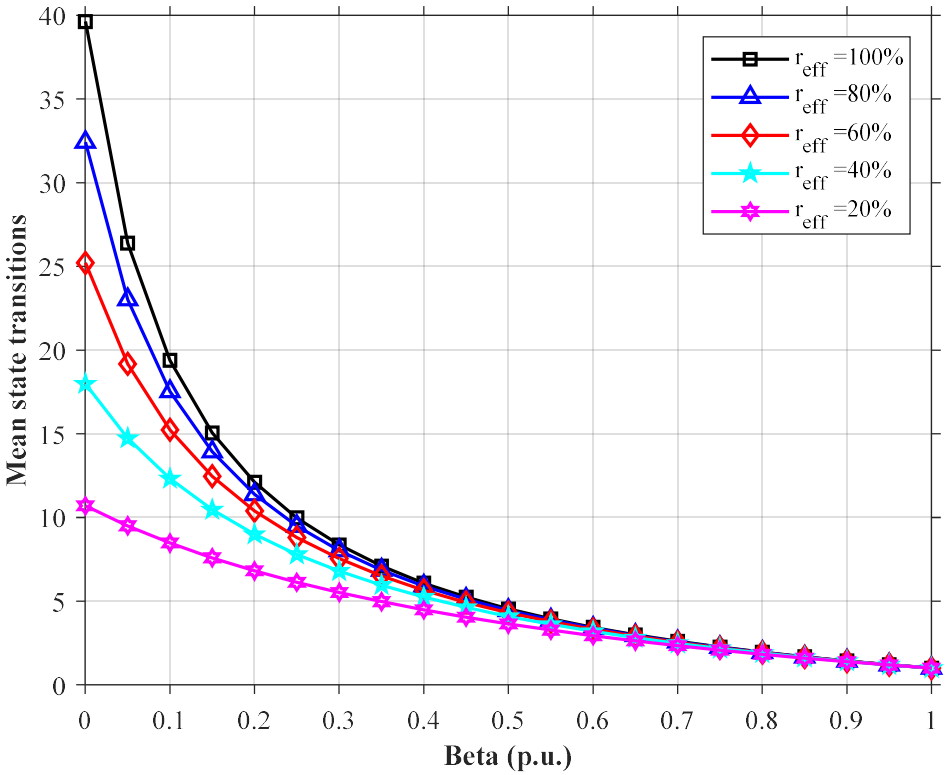


Figure 5-22: Mean system state transitions with imperfect repairs at B-3 diagnostic coverage

As before, the system's behaviour can be attributed to the reduction in the subsystems' repair rates, which reduces the system's transition probabilities from states S-2 and S-3 back to S-1, whereas the system's probability of transitioning to state S-4 increases. Figure 5-19 depicts the mean state transitions at different levels of common causes of failures. The mean state transitions are relatively sensitive to the changes of the β-factor, as would be expected based on the reliability curves.

### 5.4.5 Mixed repair efficiency levels

Three system configurations with different repair efficiencies are considered in this case study. Table 5-2 presents the repair efficiency levels of the 'one-out-of-two' subsystems under consideration. The individual subsystems A and B are assumed to be different technologies to demonstrate the system's performance when the subsystems have different diagnostic coverage levels and repair efficiencies.

Table 5-2: Subsystem repair efficiency levels

| System configuration | High and low (B-4) | High and low (B-5) | Medium and medium (B-6) |
|---|---|---|---|
| Subsystem A repair efficiency ($r_{effA}$) | 95% | 50% | 95% |
| Subsystem A repair efficiency ($r_{effB}$) | 50% | 95% | 50% |

**a) Subcase study B-4**

The subsystem's diagnostic coverage levels are assumed to be 99% and 60% for subsystems A and B. The repair efficiencies of the individual subsystem A and B are 95% and 50%. Figure 5-23 depicts the reliability of the 'one-out-of-two' system depicted in Figure 5-3 for different levels of common causes of failure represented by the β-factors. It is noticeable that the system has the highest reliability performance level when the β-factor is zero, similarly to the previous cases, even though the subsystems have different repair efficiencies. In addition, the system reliability curves show a uniform decrease in system performance than when the subsystems have high diagnostic coverage. Figure 5-24 depicts the mean state transitions at different levels of common causes of failures when subsystem A's repair efficiency is varied from 20% to 100%, while that of subsystem B is kept at 50%. The mean state transitions are relatively not sensitive to the changes of the β-factor as would be expected based on the reliability curves because the impact of the change in repair efficiency to the system probabilities is insignificant.

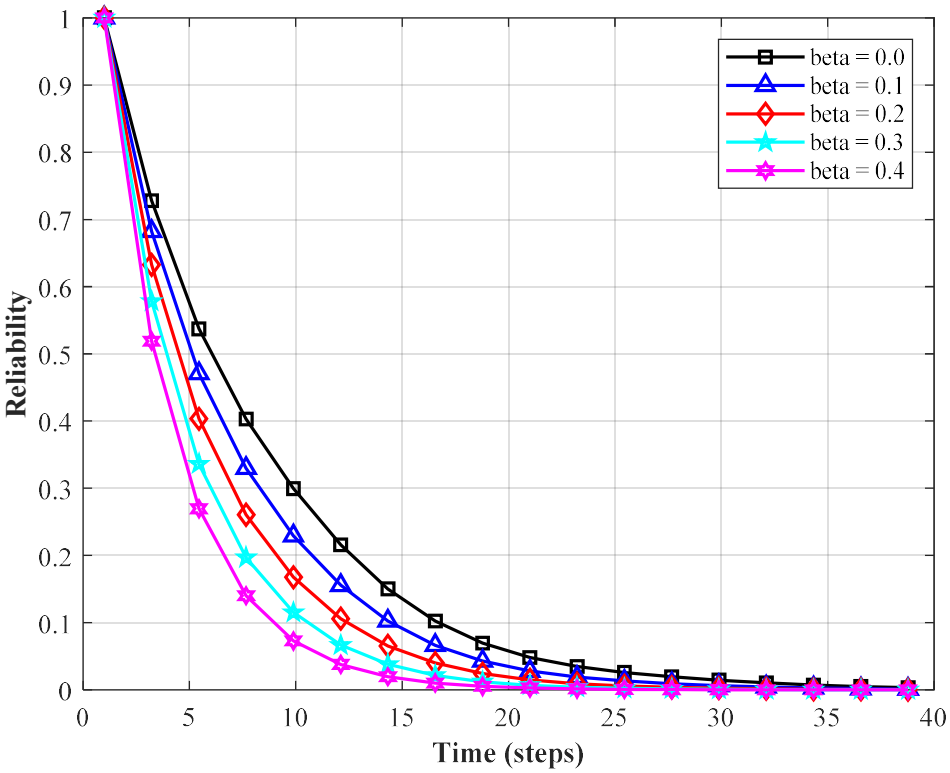


Figure 5-23: Reliability performance at B-4 system configuration

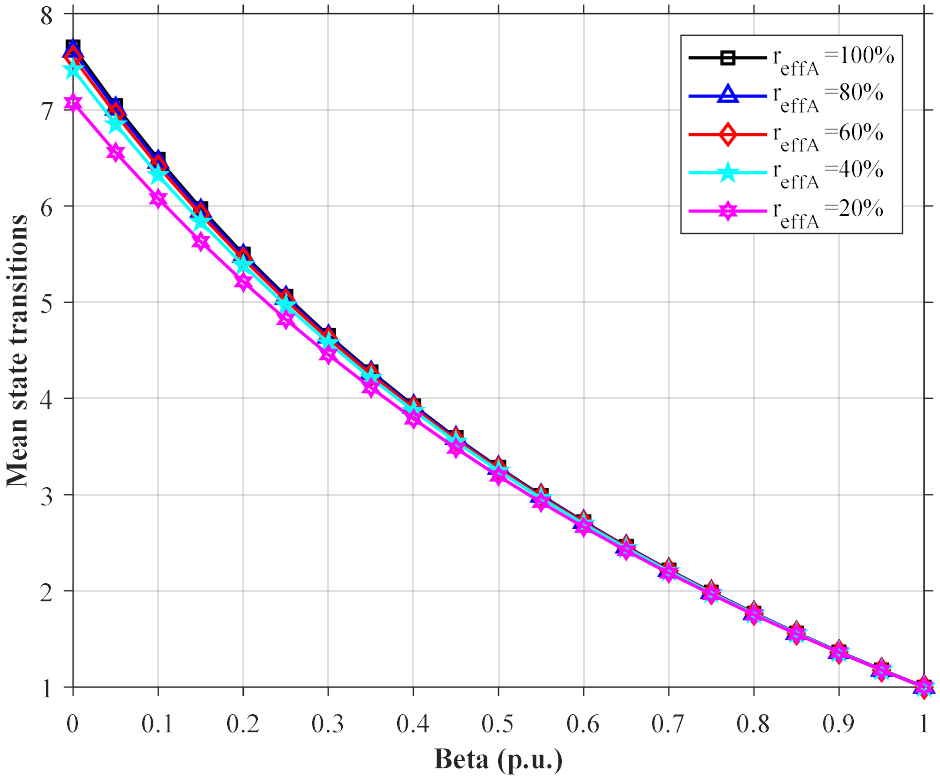


Figure 5-24: Mean system state transitions at B-4 system configuration

**b) Subcase study B-5**

The subsystem's diagnostic coverage levels are assumed to be 99% and 60% for subsystems A and B as before, respectively. The repair efficiencies of the individual subsystem A and B are 50% and 95%. Figure 5-25 depicts the reliability of the 'one-out-of-two' system depicted in Figure 5-3 for different levels of common causes of failure represented by the β-factors. Again, it is noticeable that the system has the highest reliability performance level when the β-factor is zero, similarly to the previous cases, even though the subsystems have different repair efficiencies. In addition, the repair efficiencies appear to have an insignificant impact on the performance of the system. The system reliability curves show a uniform decrease in system performance than when the subsystems have high diagnostic coverage, becoming zero at a lesser time.

The system's behaviour can be attributed to reducing the subsystems' repair rates, which reduces the system's transition probabilities from states S-2 and S-3 back to S-1, whereas the system's probability of transitioning to state S-4 increases. Figure 5-26 depicts the mean state transitions at different levels of common causes of failures when subsystem A's repair efficiency is varied from 20% to 100%, while that of subsystem B is kept at 95%.

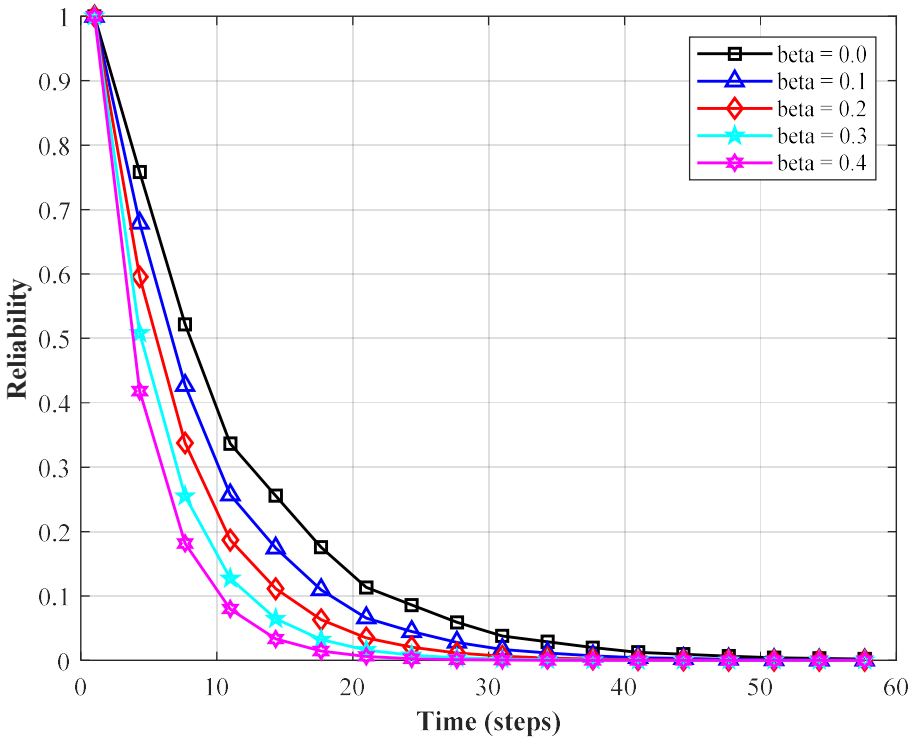


Figure 5-25: Reliability performance at B-5 system configuration

The mean state transitions are relatively sensitive to the changes of the β-factor as would be expected based on the reliability curves, particularly at low levels of β because the impact of the change in repair efficiency to the system probabilities is significant due to the higher system diagnostic coverage.

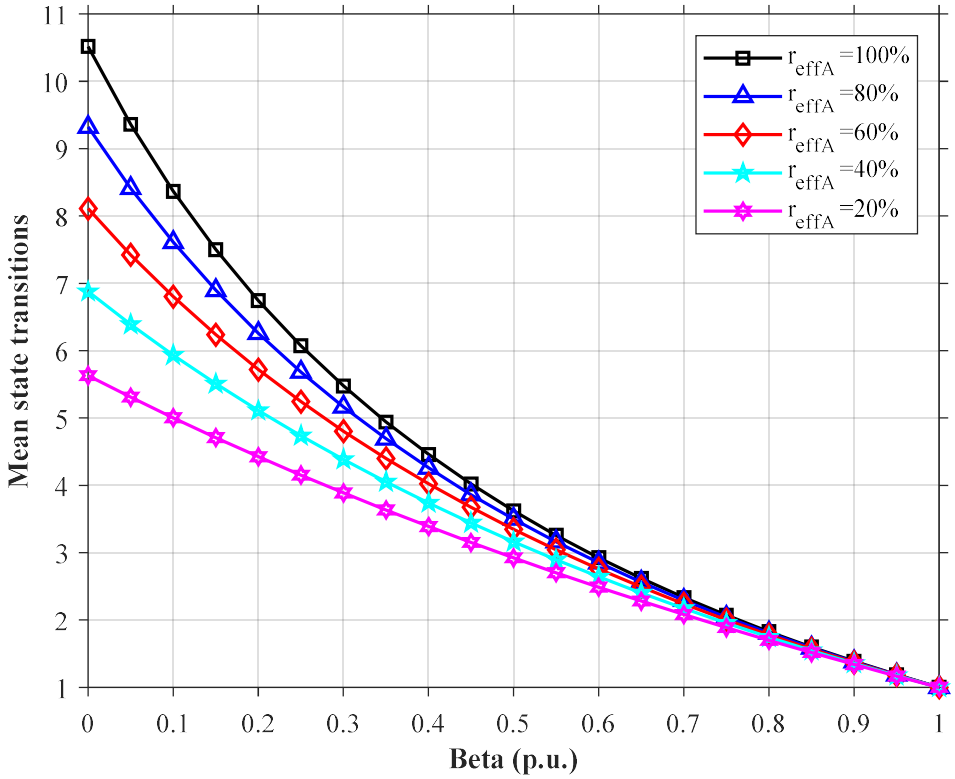


Figure 5-26: Mean system state transitions at B-5 system configuration

**c) Subcase study B-6**

The subsystem's diagnostic coverage levels are assumed to be 90% for subsystems A and B. The repair efficiencies of the individual subsystem A and B are 95% and 50%. Figure 5-27 depicts the reliability of the 'one-out-of-two' system depicted in Figure 5-3 for different levels of common causes of failure represented by the β-factors. As before, it is noticeable that the system has the highest reliability performance level when the β-factor is zero. In addition, the repair efficiencies appear to have an insignificant impact on the system's performance because of the medium level of diagnostic coverage. The system reliability curves show a uniform decrease in system performance than when the subsystems have high diagnostic coverage, which is expected based on the medium level diagnostic coverage case study results.

Again, the system's behaviour can be attributed to reducing the subsystems' repair rates, which reduces the system's transition probabilities from states S-2 and S-3 back to S-1, whereas the system's probability of transitioning to state S-4 increases.

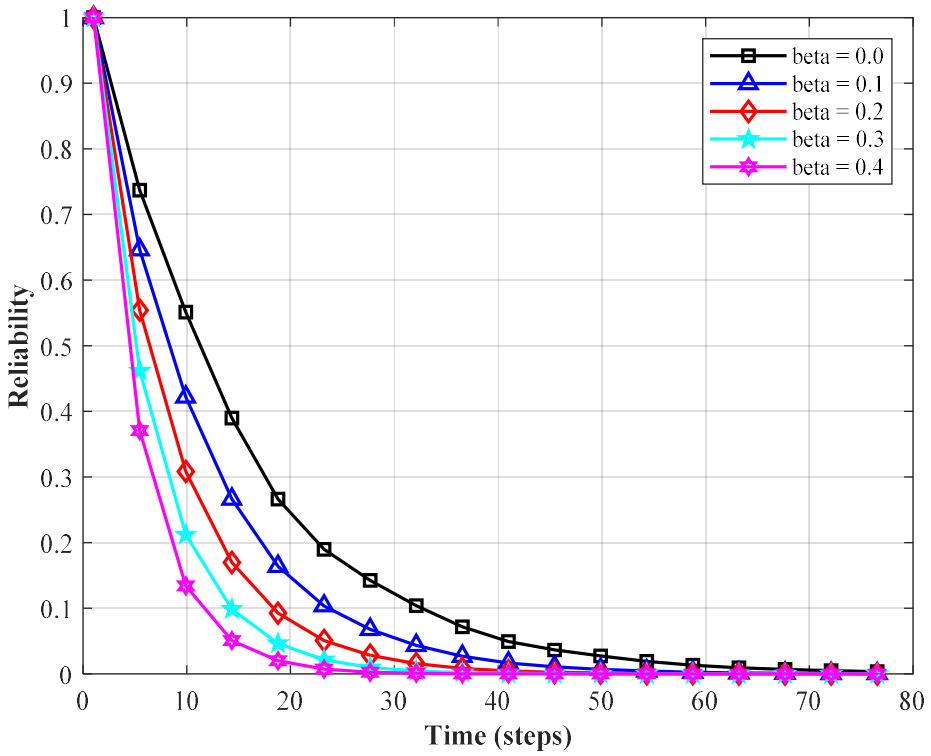


Figure 5-27: Reliability performance at B-6 system configuration

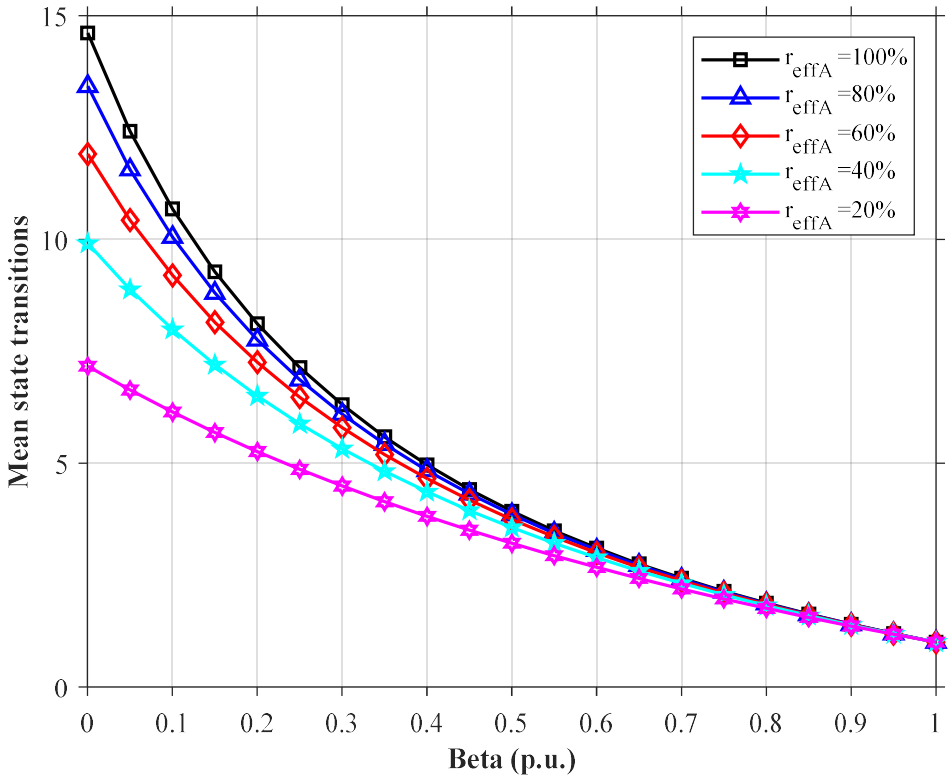


Figure 5-28: Mean system state transitions at B-6 system configuration

Figure 5-28 depicts the mean state transitions at different levels of common causes of failures when subsystem A's repair efficiency is varied from 20% to 100%, while that of subsystem B is kept at 50%. Again, the mean state transitions are relatively sensitive to the changes of the β-factor as would be expected based on the reliability curves, particularly at low levels of β because the impact of the change in repair efficiency to the system probabilities is significant due to the higher system diagnostic coverage.

## 5.5 Chapter conclusion

Integrating the β-factor model into the Markov reliability model enhances the model's flexibility to investigate various system case studies, enabling the impact of common causes of failure to be studied at different imperfect repair levels (viz. repair efficiency and system diagnostic coverage). The case studies results indicate that the existence of CCFs significantly reduces the system's reliability performance. The most impact on system reliability is observed at low levels of CCFs represented by the changes of the β-factor magnitude; where the highest level of impact is noticeable when the system's diagnostic coverage is high at 99% based on ISO 13849-1 and reduces as the level of diagnostic coverage reduces. The characteristic impact of CCFs is relatively similar for a given level of system diagnostic coverage and repair efficiency, as demonstrated by the case studies results. The combination of high and low subsystems of different diagnostic coverages impacts the system's performance; marginal impact is achieved when the subsystems have similar diagnostics coverages.

Nevertheless, it is concluded that the impact of CCFs highly depends on the system diagnostic coverage level than the repair efficiency, even though both factors impact the system's overall performance. Hence, the impact of CCFs must be considered in developing reliability models of a mission-critical system to determine the system's performance accurately. The next chapter investigates the impact of imperfect repairs based on Markov partitions and linear dynamical systems incorporating symbolic dynamics to propose a basis for selecting the system parameters.

# CHAPTER 6

# MULTI-STATE IEC 61850 SUBSTATION COMMUNICATION NETWORK IN THE CONTEXT OF LINEAR DYNAMICAL SYSTEMS

## 6.1 Introduction

In chapter 4, the reliability of the multi-channel IEC 61850 based Substation Communication Network (SCN) was investigated using the structure-function and Markov process. Imperfect repairs and system fault diagnostic coverage were integrated into the Markov model using Systems Thinking, while mean system state transitions before failure was estimated using Mathematical Expectation [75], [97]. The impact of Common Cause Failures (CCFs) on the system's reliability performance was investigated in Chapter 5 based on the β-factor model integrated into the Markov model. The modelling effort in Chapter 4 and Chapter 5 does not only provide insights into the quality of repairs (viz. repair efficiency, diagnostic coverage and CCFs); but also provides a more detailed transition probability matrix of the system that describes the dynamic nature of the system; enabling the impact of system maintainability and supportability to be investigated considering the level of CCFs [92], [115]. In this chapter, the dynamic nature and performance of multi-channel IEC 61850 based SCN are investigated using Markov partitions and symbolic dynamics in the context of linear dynamical systems. The objective of this chapter is to provide a method of analysing the impact of various system factors on the performance and the dynamic nature of multi-channel IEC 61850 based SCN, specifically the impact of repair efficiency, diagnostic coverage and CCFs during the system's useful life [75], [129].

Section 6.2 presents an overview of dynamical systems. The dynamics of the systems based on Markov partitions is presented in section 6.3. The Markov process in the context of linear dynamical systems is discussed in section 6.4, while section 6.5 discusses the dynamics of the system and its performance based on eigenvalues using the concept of matrix similarity. Section 6.6 presents case studies and discusses the findings. Conclusions and recommendations are highlighted in section 6.7

## 6.2 Overview of dynamical systems

Systems can be thought of as a few subsystems or components guided by simple rules, where a complex system comprises many of such subsystems or components, each playing a specific role while guided by simple rules [130]–[132]. The complexity of a system is described by intense, collective dynamical behaviour caused by an interaction between many subsystems or components. Hence, complexity in systems is in the system's dynamical evolution and not the system itself, where the resultant dynamical evolution is purely caused by interactions between subsystems that form a system. Complex systems are composite,

comprising many subsystems that often are composite themselves. These systems are best described as Systems of Systems (SoS) and are adaptive, as well as produce emergent properties and behaviours as a result of interactions between subsystems when viewed from a higher level of abstraction [130]–[133]. The emergent properties and behaviours are caused by the interactions between various subsystems of complex systems feeding into one another, resulting in rich system behavioural characteristics that cannot be deduced from individual subsystems. For this reason, the reductionist approach cannot be used to solve complex dynamical systems because awareness of interactions between various subsystems is needed since the system as a whole is irreducible to simple subsystem interfaces [130]–[133]. Systems of systems (SoS) engineering perspective is therefore required to solve complex engineering systems, including cases where the integration of systems is required [131]–[134].

In contrast to complex systems, chaotic systems have few subsystems. However, the subsystems mutually interact with each other to produce highly complex system dynamics. In addition, chaotic systems appear to be stochastic at an abstract level, even though non-random deterministic processes govern them. Even so, chaotic systems are not easily predictable despite being deterministic [130], [135]. A system is deterministic if both the past and future trajectories can be uniquely determined and semi-deterministic if only its future trajectory can be determined, not the system's past trajectory. A system is also indeterministic if its past trajectory can be determined, not the future trajectory [130].

### 6.3 Behavioural characteristics of dynamical systems

The evolution of system states and variables over time, according to some rule, is a characteristic of dynamical systems. Dynamical systems are often studied using symbolic dynamics, where a topological equivalent of the system is investigated instead of the actual system [130], [136]. In symbolic dynamics, the behavioural characteristic of a finite number of symbols is studied on the topological equivalent system. In contrast, the actual system comprises a trajectory of an infinite length sequence of values that can also be represented using a time series. Therefore, partitions can be introduced in a system's geometrical space to track and observe the system's trajectory between the various partitions as chaos is generated [130], [136]. However, it should be noted that it is not uncommon for the systems' trajectory to settle or be attracted to a point in the system's geometrical space. A system's attractor is a point or a set of points to which the system settles after a transient. The point to which the system settles is referred to as a fixed point. Moreover, a set of points that never comes to rest are referred to as a limiting cycle. The state to which the system settles may also be dependent on the initial condition(s) of the system before the transient [129].

Chaos theory has been reliably used in natural science studies to analyse the system's long-term behaviour using readily available data and recurrence plot techniques. In the field

of systems engineering, categorisation of system's long-term behaviour and emergent behaviours is applicable in the effort of determining the reliability of the system, and the scope may well include maintainability and emergent behaviours resulting from system architectural changes as some of the examples that can be studied using chaos theory. Chaos can be described as complicated, non-periodic, seemingly stochastic behaviour caused by the interaction of a simple rule and sensitivity to initial conditions [130], [137]. Most dynamical systems are chaotic and are characterised by being sensitive to initial conditions, undergo topological transitivity, as well as comprise dense periodic orbit properties[130], [135], [138]. Markov partitions come across as a suitable and preferred set of group partitions that can be used to investigate the behaviour of dynamical systems [130], [135], [139].

### 6.3.1 Markov partitions

Markov chains are stochastic, and therefore may seem mutually incompatible with the idea of a deterministic system. However, they can be considered to be an example of linear dynamical systems, and therefore deterministic! Markov process is applicable in dynamical systems studies due to its memoryless property since its next state is considered dependent only on the system's present state [95], [136]., Markov process can be described as a system comprising multiple finite states, as well as a transition rule that can be represented by a directed graph or a transition probability matrix comprising rows of probability vectors such that row *n* is the state of the Markov chain at time *n* [75], [95]. Therefore, the concept of geometrical or phase space partitions is of utmost importance in dynamical systems' studies because it enables representing a geometrical space by a reduced finite set of symbols [95], [139]. However, the main challenge remains to determine the appropriate number of partitions to sufficiently track the system trajectory [17].

In this research, structure-function modelling is used since each element of the Markov partition can be considered to correspond to a state in the Markov process in a geometrical space $S$ [97], [108], [140]. To define the partition, let $S = [a, b]$, and let $f: S \rightarrow S$. Let $P$ be a partition of $S$ given by the point $a = a_0 < a_1 < \cdots < a_n = b$. For $i = 1, \ldots, n$, let $S_i = (a_{i-1}, a_i)$ and denote the restriction of $f$ to $S_i$ by $f_i$. If $f_i$ is a homeomorphism from $S_i$ onto some connected union of intervals of $P$ represented by $(a_{j(i)}, a_{k(i)})$, then $f$ is said to be Markov, and the partition $P = \{S_i\}_{i=1}^{n}$ is referred to as a Markov partition with reference to the function $f$ [140]–[142].

### 6.3.2 Phase partitions in the context of the structure-function model

In order to determine the reliability performance and dynamics of repairable multi-state IEC 61850 based SCN, the structure-function modelling approach is used to model system's phase-space partitions in dynamical systems [13], [14]; particular where reliability, availability

and maintainability are investigated as quantitative attributes of dependability [97], [108]. Structure-function is preferred because it enables the determination of system states and performance concerning system availability when multiple subsystems interact within a system. The Markov based structure-function model is discussed in Chapter 4 [8], [75], [108]. Hence, the four states of the 'one-out-of-two' system are considered the respective partitions of the system's geometrical space as depicted on the system's state transition diagram in Chapter 4 and Chapter 5; again in Figure 6-1 for ease of reference. The associated state transition probability matrix of the system incorporating CCFs is given by (6-1) [91], [109].

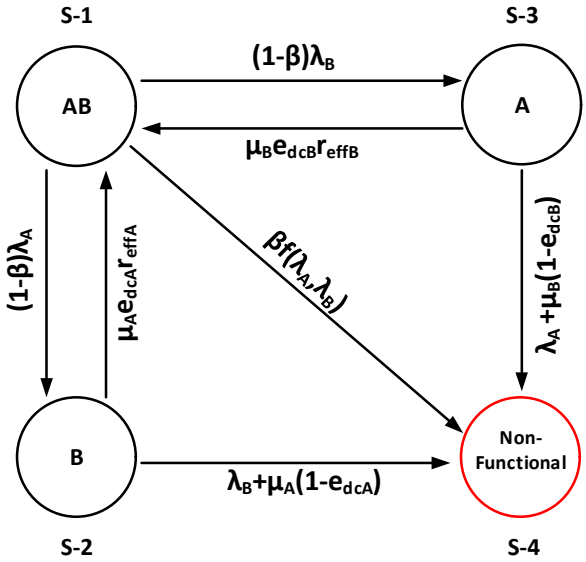


Figure 6-1: 'One-out-of-two' system state transition diagram incorporating quality of repairs

$$\boldsymbol{P} = \begin{bmatrix} 1-(1-\beta)\lambda_A-(1-\beta)\lambda_B-\beta f(\lambda_A,\lambda_B) & \cdots \\ \mu_A e_{dcA} r_{effA} & \\ \mu_B e_{dcB} r_{effB} & \\ 0 & \end{bmatrix}$$

$$\cdots \begin{matrix} (1-\beta)\lambda_A \\ 1-\mu_A e_{dcA} r_{effA}-(\lambda_B+\mu_A(1-e_{dcA})) \\ 0 \\ 0 \end{matrix} \quad \begin{matrix} (1-\beta)\lambda_B \\ 0 \\ 1-\mu_B e_{dcB} r_{effB}-(\lambda_A+\mu_B(1-e_{dcB})) \\ 0 \end{matrix} \cdots$$

$$\cdots \begin{bmatrix} \beta f(\lambda_A,\lambda_B) \\ \lambda_B+\mu_A(1-e_{dcA}) \\ \lambda_A+\mu_B(1-e_{dcB}) \\ 1 \end{bmatrix} \quad (6\text{-}1)$$

The Markov time series of the 'one-out-of-two' system considering the failure rates presented in Chapter 4 at 95% repair efficiency and 99% system diagnostic coverage is depicted in Figure 6-2, assuming that the two subsystems are entirely independent. It is

noticeable in Figure 6-2 that the system transitions between states S-1, S-2 and S-3, but never enters state S-4 over the simulated number of steps. The system behaviour is expected because nearly all system faults are discoverable and almost fully repairable, even though the achievement of such repair and diagnostics level is uncertain in practice. Nevertheless, the dynamic nature of the system state transitions in Figure 6-2 and the mean state transitions cannot be readily determined from the time series, which becomes even more complex to determine for systems having a high number of interconnected states; mainly when the individual system parameters are varied to investigate their effects on the performance of the system.

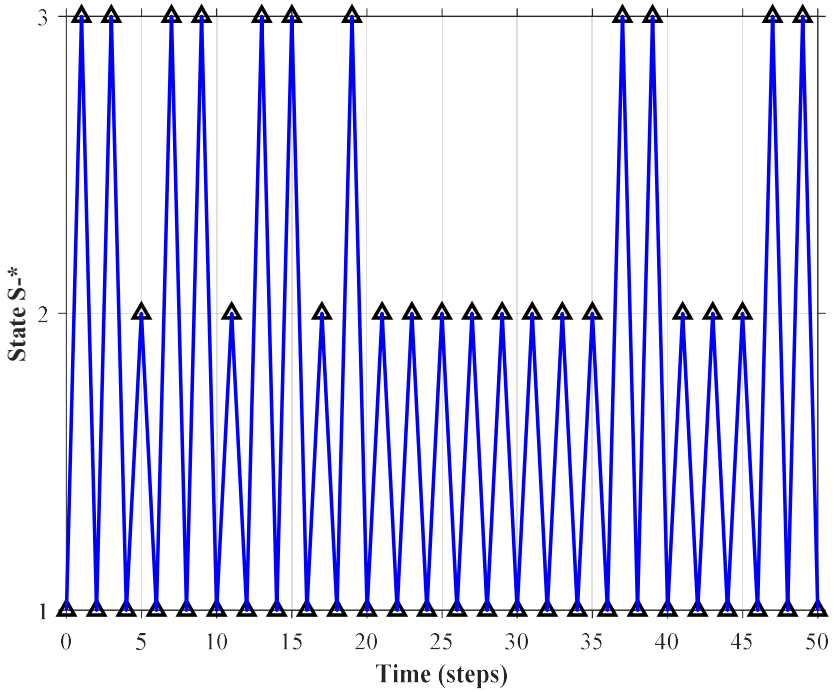


Figure 6-2: Markov state transition time series of 'one-out-of-two IEC 61850 SCN

The following section investigates the Markov process time-series dynamical characteristics and performance based on linear dynamical systems to determine the system's long-term behaviour. The investigation presented in section 6.4 focuses on the effectiveness of the system repair efficiency and CCFs on the system performance and its dynamics at different diagnostic coverage levels.

## 6.4 Dynamical system behavioural characteristics of the Markov process

This section focuses on the system's dynamical behaviour described by the Markov transition probability matrix in section 6.3. In subsection 6.3.1, the proposed Markov partition was described as $f: S \rightarrow S$ to indicate the level of interest as the state space comprising the four states of the system. In this section, however, the Markov transition probability matrix represents a lower abstraction level determining the system's next state. Therefore, to describe

the system of several variables at this level, let $f: R^n \rightarrow R^n$, such that $f(X)$ is given by (6-2) [95], [100], [142], [143]

$$f(X) = \boldsymbol{A}X + B, X \in R^n \tag{6-2}$$

where $\boldsymbol{A}$ is an $n\ x\ n$ matrix, and $B$ is an $n$-fixed vector that can be assumed to be zero so that (6-2) simplifies to (6-3) [95], [144], [145],

$$f(X) = \boldsymbol{A}X, X \in R^n \tag{6-3}$$

Stochastic processes in the form of Markov chain can be depicted graphically to ease process visualisation, which also lessens the level of analysis effort needed in some cases, whereas matrix representation is well suited for algebraic and computational system analysis [142], [146]. The methods are seen to be complementary and therefore used mutually in this research.

Markov chain processes can be considered comprising classes of subsystems grouped according to the behavioural characteristic for analysis purposes. The subsystems, individual states in some cases for that matter, interact in a manner that can be described as dynamic in the context of linear dynamical systems. A class of states $C$ is a set of communicating states in a system, where any two distinct states $i$ and $j$ are said to communicate ($i \leftrightarrow j$) if state $j$ is accessible from state $i$; and state $i$ is accessible from state $j$ [142], [147]. However, it may also be possible to access state $j$ ($i \rightarrow j$) from state $i$ if a walk exists from state $i$ to $j$, while it is not possible to access state $i$ from state $j$. Accessibility is achieved through a walk over the states (i.e., vertices) of a transition probability diagram, such that an $n$-step walk on a state transition probability diagram is an ordered string of states ($S_0, S_1, .., S_n$) for $n \geq 1$, where there is a direct access to state $S_m$ from state $S_{m-1}$ for each $1 \leq m \leq n$. Furthermore, characterising the type of walk that may occur, a path is a walk where no state is repeated, while a cycle is a walk where the start and the end state are one and no other state is repeated. In a finite Markov chain of $M$ states therefore, a path can be $M - 1$ steps maximum, while a cycle can be $M$ steps at the most [142], [147].

The respective Markov chain classes' dynamical behaviour can be recurrent, transient, periodic/aperiodic, or ergodic. State $i$ of a finite Markov chain is recurrent if it is accessible from all states that are accessible from state $i$ [142], [146]. Therefore, all states in a class of a finite Markov chain are either transient or recurrent, as well as have the same period [142], [147]; where the period of a state $i$ denoted by $d(i)$ is the greatest common divisor ($gcd$) of those values of $n$ for which $P_{ii}^n > 0$. The state is said to be aperiodic if it has a period of 1 and periodic if the period is 2 or more [142]. In a case where a class of states in a finite Markov chain is both recurrent and aperiodic, the state is said to be ergodic. Therefore, an ergodic

chain is a finite Markov chain consisting entirely of one ergodic class, such that a chain of $M$ states, $P_{ij}^{m} > 0$ for all $i$ and $j$, for all $m \geq (M-1)^2 + 1$ [142], [148]. Furthermore, a unichain is a finite state Markov chain comprising one recurrent class, as well as transient states in some cases. An ergodic unichain is, therefore, a unichain on which the recurrent class is ergodic [142], [149]

### 6.5 Characteristic polynomial and system dynamics

In order to investigate the dynamical behaviour of the system described in (6-3), the system is modelled in discrete time following the maintenance repair philosophy described in the 'one-out-of-two' IEC 61850 state diagram depicted in Figure 6-1, where the next state of the system is only dependent on the current state of the system and given by (6-4) [95], [144], [145],

$$X(t+1) = f\big(X(t)\big) \tag{6-4}$$

Substituting (6-3) in (6-4) results in (6-5); which determines the next state of the system $X(t+1)$ given the present state $X(t)$, where $\boldsymbol{A}$ is substituted by the state transition probability matrix $\boldsymbol{P}$ [95], [146],

$$X(t+1) = \boldsymbol{P}X(t) \tag{6-5}$$

Therefore, if $X(0) = X_0$, then

$$X(1) = \boldsymbol{P^1}X_0$$

$$X(2) = \boldsymbol{P^2}X_0$$

$$X(3) = \boldsymbol{P^3}X_0$$

Observing the iterative process illustrated above determining $X(t)$, it can be concluded that at any point in time $t$, $X(t)$ is given by (6-6),

$$X(t) = \boldsymbol{P}^t X_0 \tag{6-6}$$

However, the system's characteristic dynamical behaviour as $t \to \infty$ remains unknown or too complex to determine by just observing the time series obtained when chaos is generated by iterating (6-6). The objective is therefore to understand the dynamical behaviour of the system described by $\boldsymbol{P}$ given that $X(0) = X_0$ as $t \to \infty$.

A fundamental concept in matrix analysis is aimed at characterising the set of eigenvalues of a square matrix to determine the dynamical behaviour of a system, of which the eigenvalues can be obtained by solving the characteristic polynomial of the matrix that satisfies the determinant equation given by (6-7) [100], [106], [142], [143], [146], where $\boldsymbol{I}$ is the identity matrix, and $\gamma$ is the eigenvector:

$$det[\boldsymbol{P} - \gamma \boldsymbol{I}] = 0 \tag{6-7}$$

In addition, it is assumed at this stage that $\boldsymbol{P}$ is diagonalisable, and therefore implied as a necessary and sufficient condition for matrix $\boldsymbol{P}$ to have linearly independent eigenvectors $(v_i \dots v_n)$ with associated eigenvalues $(\gamma_i \dots \gamma_n)$ [95], [100], [106], [143].

Now let $\boldsymbol{V}$ be a $n\ x\ n$ matrix where its $i^{th}$ column is $v_i$, such that $\boldsymbol{P}$ is given by (6-8) where $\Lambda$ is a diagonal matrix whose columns comprise the eigenvalues $(\gamma_i \dots \gamma_n)$ of $\boldsymbol{P}$, such that $\boldsymbol{P}$ is similar to $\Lambda$ [95], [143],

$$\boldsymbol{P} = \boldsymbol{V}\Lambda\boldsymbol{V}^{-1} \tag{6-8}$$

It can be shown that $P^t$ can be evaluated using (6-9) comprising $t$ terms,

$$\boldsymbol{P}^t = (\boldsymbol{V}\Lambda\boldsymbol{V}^{-1})(\boldsymbol{V}\Lambda\boldsymbol{V}^{-1}) \dots (\boldsymbol{V}\Lambda\boldsymbol{V}^{-1}) \tag{6-9}$$

And by association, considering that $(\mathbf{V}\mathbf{V}^{-1})$ evaluates to an identity matrix $\boldsymbol{I}$, (6-9) becomes (6-10),

$$\boldsymbol{P}^t = (\boldsymbol{V}\Lambda^t\boldsymbol{V}^{-1}) \tag{6-10}$$

In light of $\Lambda$ being a diagonal matrix comprising eigenvalues $(\gamma_i \dots \gamma_n)$ of $P$, it becomes easier to compute $\Lambda^t$, as given by (6-11) [95],

$$\Lambda^t = \begin{pmatrix} \gamma_1 & 0 & \cdots & 0 \\ 0 & \gamma_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_n \end{pmatrix}^t$$

$$\Lambda^t = \begin{pmatrix} \gamma_1^t & 0 & \cdots & 0 \\ 0 & \gamma_2^t & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_n^t \end{pmatrix} \tag{6-11}$$

It is evident in (6-11) that the behaviour of $\boldsymbol{P}^t$ as $t \to \infty$ can be investigated by studying the behaviour of the eigenvalues $(\gamma_j^t)$ of $\boldsymbol{P}$, where real numbers of $|\gamma_j| < 1$ imply that $\boldsymbol{P}^t$ becomes zero as $t \to \infty$; and $|\gamma_j| > 1$ imply that $\boldsymbol{P}^t$ becomes infinitely large, while terms where $|\gamma_j| = 1$ do not increase nor decrease as $t \to \infty$. However, $\gamma_j$ may also be complicated, for which the polar form can be written as $re^{i\theta_j}$, where $r$ is the magnitude of the eigenvalue and $\theta$ is the angular position on the complex plane, such that (6-12) holds as $t \to \infty$ [95], [100], [101], [129],

$$|\gamma_j^t| = |r_j^t e^{it\theta_j}| \to \begin{cases} 0, & r < 1 \ and \\ \infty, & x > 1 \end{cases} \tag{6-12}$$

Therefore, similar results as those for real eigenvalues are applicable for complex eigenvalues. Thus, if $\boldsymbol{P}$ is a transition probability matrix with $\gamma_j \leq 1$, $\boldsymbol{P}^t$ cannot become infinitely large as $t \to \infty$. Hence, bearing in mind that $\boldsymbol{P}$ is diagonalisable, if $c_i$ is a scalar value, (6-13) holds [95],

$$X(1) = \boldsymbol{P}X(0) = c_1 P v_1 + c_2 P v_2 + \cdots + c_n P v_n \tag{6-13}$$

Substituting $Pv_i = \gamma_i v_i$, (6-13) becomes (6-14) [100], [143], [145],

$$X(1) = c_1\gamma_1 v_1 + c_2\gamma_2 v_2 + \cdots + c_n\gamma_n v_n \tag{6-14}$$

From (6-14), it can be shown that $X(t)$ is given by (6-15) [100], [144],

$$X(t) = c_1\gamma_1^t v_1 + c_2\gamma_2^t v_2 + \cdots + c_n\gamma_n^t v_n \tag{6-15}$$

Therefore, all terms of $X(t)$ become zero where $\gamma_j < 1$ as $t \to \infty$, while all terms of $X(t)$ where $\gamma_j = 1$ remain except in a particular case where $c_i = 0$. In consideration of the fact that Markov transition probability matrix has $\gamma = 1$ as one of the eigenvalues [100], [129], [142], it follows that a period $d$ recurrent chain has $d$ eigenvalues uniformly placed around a unit circle on a complex plane [95], [142], [149]. Even though the analysis presented above assumed that the transition probability matrix is diagonalisable, a similar analysis approach incorporating the Jordan canonical form matrix for non-diagonalisable matrices leads to the same conclusion that the behaviour of $\boldsymbol{P}^t$ as $t \to \infty$ is similar to that of diagonalisable matrices [95], [143].

## 6.6 Case studies results and conclusions

This section presents the case studies results, analysis and discussions of the impact of repair efficiency, diagnostic coverage and CCFs on the reliability performance and dynamical behaviour of the 'one-out-of-two' system configuration depicted in Figure 6-1. As before, the basis of the case studies investigated in this chapter is ISO 13849-1 introduced in Chapter 4. Table 4-4 presents the diagnostic coverage levels.

Although different subsystem repair efficiency levels and diagnostic coverages can be simulated for analysis, the following assumptions are made to ease the respective system parameters' analysis.

a) Subsystems A and B are of the same technology; hence they have the same diagnostic coverage; this assumption is relaxed later on.
b) The same resources support both subsystems A and B such that equal repair efficiencies are applied to both subsystems. In addition, this assumption is relaxed later on.

c) The two subsystems A and B are entirely independent such that the level of CCFs represented by the parameter β is set to zero; this assumption is relaxed later on to investigate the impact of CCFs.

d) The system is fully functional at the beginning of the simulation. Although the system is assumed to be fully functional at the begging of the simulation, any system state can be selected as the system's initial state assuming a partial failure at the beginning of the simulation.

### 6.6.1 High diagnostic coverage level

The system, as described in section 6.3 and depicted in Figure 6-1is investigated assuming that both subsystems A and B have 99% diagnostic coverage ($e_{dc}$). Subsystems A and B failure and repair rates are stated in subsection 6.3 [28], [72]. The long-term dynamical impact of repair efficiency ($r_{eff}$) is examined by observing the magnitudes of the respective system eigenvalues ($\gamma_j$) under varying levels of repair efficiency ($r_{eff}$) from as low as 5% to 100% in steps of 5% for the system described by (6-1) [49], [60], [91], [109]. Figure 6-3 depicts the magnitude of the system eigenvalues ($\gamma_j$) under varying levels of repair efficiency ($r_{eff}$).

It can be observed in Figure 6-3 that only two eigenvalues are affected by the change in repair efficiency, while the other two remain constant at magnitudes 0 and 1, respectively. The behaviour demonstrates one dominant state in the system as time $t\rightarrow\infty$. Very important though, it is evident that the increase in repair efficiency closer to 100% is not as effective as in the lower efficiency range magnitudes only increase marginally. The high eigenvalues result in a smaller spectral gap between the unit circle and the second-largest eigenvalue (i.e. $max_{i:|\gamma_i|<1}|\gamma_i|$), indicating a lower rate of system convergence towards an absorbing state of the system that is represented by eigenvalue magnitude 1-term in (6-15) or a limit cycle if multiple eigenvalues of the magnitude of 1 existed [129], [130]. Although it may seem possible to investigate the system's dynamical nature from Figure 6-3, it is challenging for large complex systems.

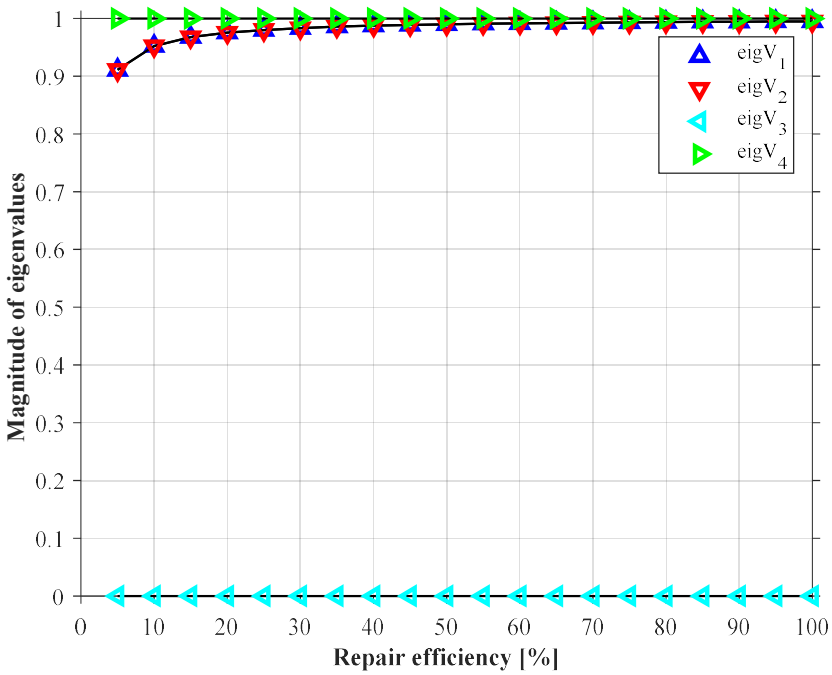


Figure 6-3: Eigenvalue magnitudes of 'one-out-of-two' IEC 61850 SCN at 99% diagnostic coverage

Eigenvalue plot comes across as a complementary technique to determine the dynamical behaviour of the system by simulating different levels of repair efficiency ($r_{eff}$) and fault diagnostic coverage ($e_{dc}$) while observing the behaviour of system eigenvalues on a complex plane. Figure 6-4 depicts the system eigenvalues on a complex plane, where the system dynamics can be determined by observing any changes in the formation of the eigenvalues; as well as how the spectral gap changes with different repair efficiency( $r_{eff}$) levels while diagnostic coverage ($e_{dc}$) is kept constant 99%.

The layout formation of the eigenvalues is not affected by the change in repair efficiency ($r_{eff}$), except that the spectral gap decreases with higher values of repair efficiency ($r_{eff}$). The eigenvalues' consistent formation indicates that only the system rate of convergence is affected, as discussed earlier. In both Figure 6-3 and Figure 6-4, it can be deduced that the system does not become periodic at any level of repair efficiency ($r_{eff}$) since only one eigenvalue has a magnitude of 1. Essentially, Figure 6-4 makes it easy to observe the spectral gap magnitude between the largest and the second-largest eigenvalues (i.e. $max_{i:|\gamma_i|<1}|\gamma_i|$) on a complex plane, which determines the rate at which $\boldsymbol{P}^n$ approaches steady state. In the system presented above, the spectral gap is huge at 5% $r_{eff}$, which implies that the system's rate of convergence to steady-state is high.

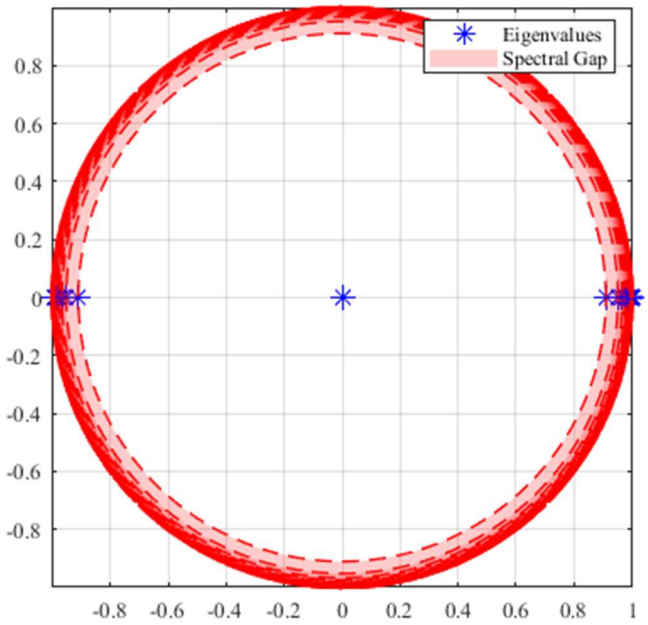


Figure 6-4: Eigenvalues of 'one-out-of-two' IEC 61850 SCN at 99% diagnostic coverage

Figure 6-5 depicts the state transition probability diagram with states grouped into classes according to their behavioural characteristics when the system repair efficiency ($r_{eff}$) is 5%. It can be observed in Figure 6-5 that states S-1, S-2, and S-3 communicate in a transient dynamic manner, while state S-4 is aperiodic and recurrent, which also aligns with the operating and maintenance philosophy of the system as depicted in Figure 6-1. The low transition probability of the system transitioning from states S-2 and S-3 to state S-1 is a result of the low repair efficiency ($r_{eff}$) at the specified system diagnostic coverage ($e_{dc}$) factor that highly increases the system's probability to transition into state S-4 as depicted in Figure 6-5. The system's high rates transitioning to state S-4 is because the system accumulates unresolved faults at a much higher rate as time progresses. However, the nature of state interactions is the same for the simulated repair efficiency ($r_{eff}$) range. Figure 6-6 depicts the state probability of the system's availability and unavailability over 500-time steps as repair efficiency is varied from 5% to 100% at 99% system diagnostic coverage. It can be observed that the system's availability reduces to almost 0 in just over 50-time steps when the repair efficiency is 5%. It can also be observed in Figure 6-6 that the system is relatively sensitive at low repair efficiency levels, where the system's reliability performance seems to be impacted more than at higher repair efficiency levels.

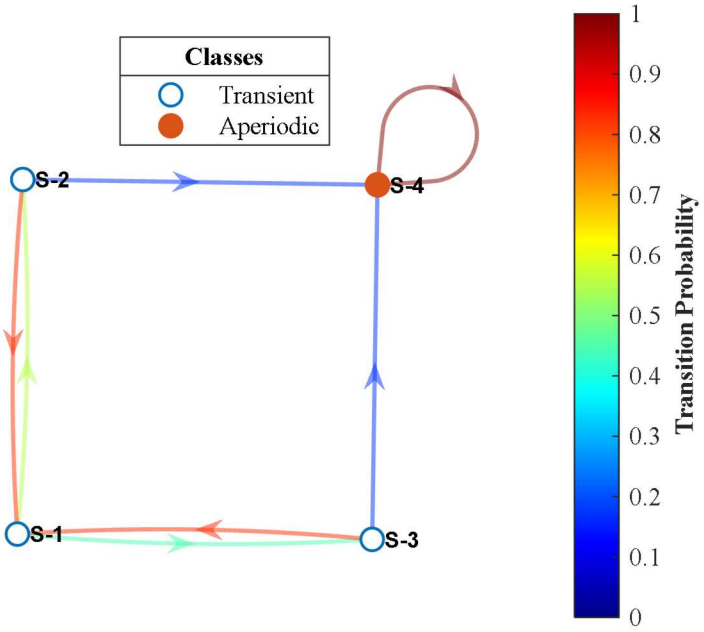


Figure 6-5: State transition probability diagram of 'one-out-of-two' IEC 61850 SCN at 99% diagnostic coverage and 5% repair efficiency.

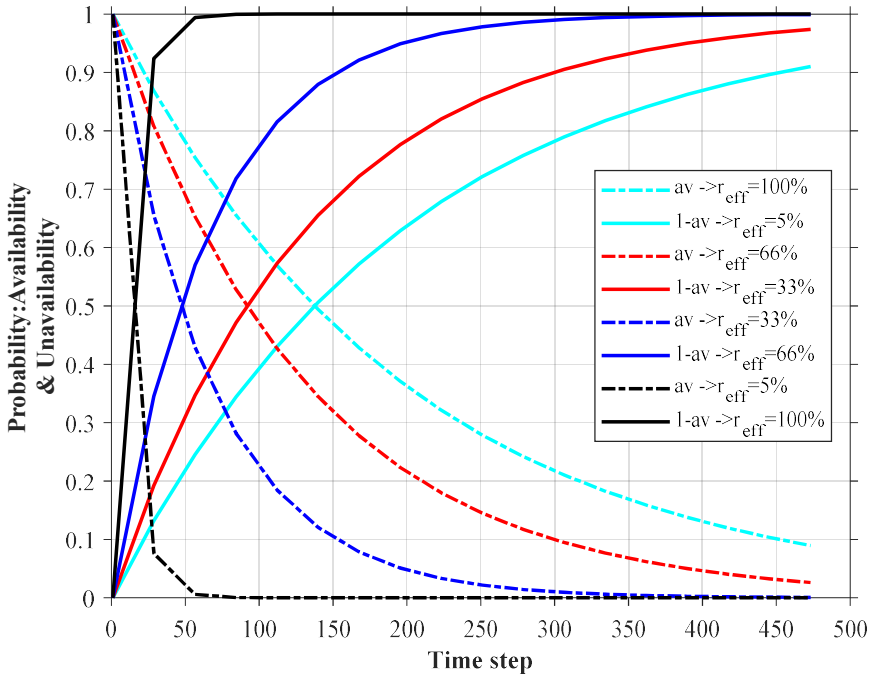


Figure 6-6: System probability – availability and unavailability with repair efficiency of 5% to 100% at 99% diagnostic coverage.

Figure 6-7 depicts the system state transitions for different repair efficiency levels at 99% system diagnostic coverage that appears consistent with the eigenvalue magnitudes and the

spectral gap in Figure 6-3. In Figure 6-3 and Figure 6-4, it was observed that the high repair efficiency level is associated with high eigenvalue magnitudes for all $|\gamma_i| < 1$, where a bigger spectral gap between the eigenvalue of magnitude 1 depicted by a unit circle in a complex plane and the second largest eigenvalue(s). Hence, the mean state transitions of the system before failure is high.

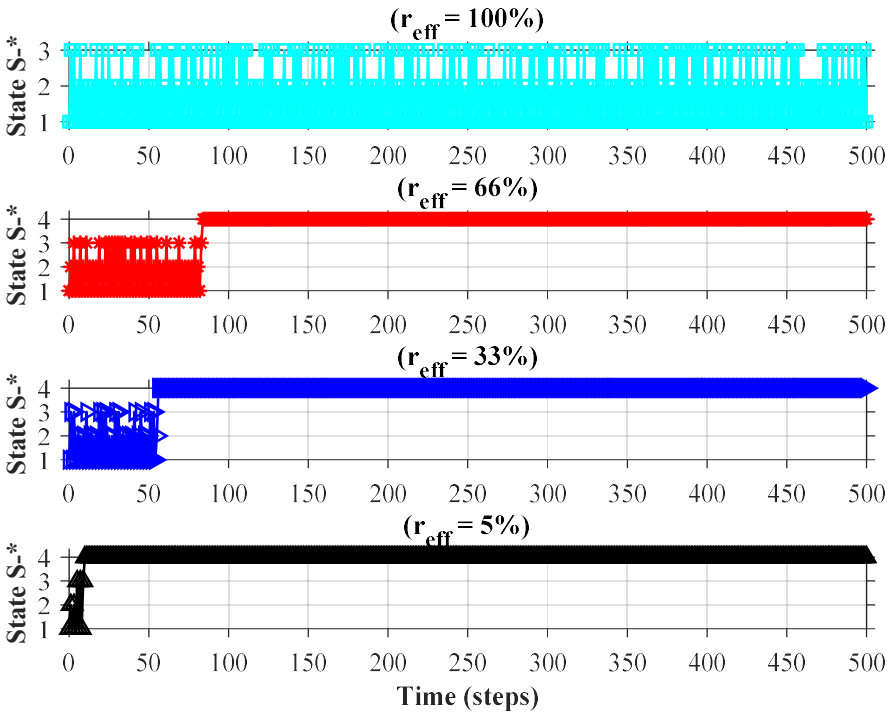


Figure 6-7: System state transition simulated at varying repair efficiency of 5% to 100% and 99% diagnostic coverage.

### 6.6.2 Medium diagnostic coverage level

In this case study, subsystems A and B are assumed to have 90% diagnostic coverage ($e_{dc}$) factors, while their failure and repair rates remain unchanged, as stated in subsection 6.3. As in the previous case study, the long-term dynamical impact of repair efficiency ($r_{eff}$) is examined by observing the magnitudes of the respective system eigenvalues ($\gamma_j$) under varying levels of repair efficiency ($r_{eff}$). Figure 6-8 depicts the magnitudes of the system eigenvalues ($\gamma_j$) under varying levels of repair efficiency ($r_{eff}$). Again, it can be observed in Figure 6-8 that only two eigenvalues are affected by the change in repair efficiency, while the other two remain constant at magnitudes 0 and 1, respectively. The system behaviour demonstrates that there is still one dominant state in the system as time $t \to \infty$. In addition, it is evident again that the increase in repair efficiency closer to 100% does not have a significant impact as in the lower efficiency range, even though the impact is relatively visible than when the diagnostic coverage is high.

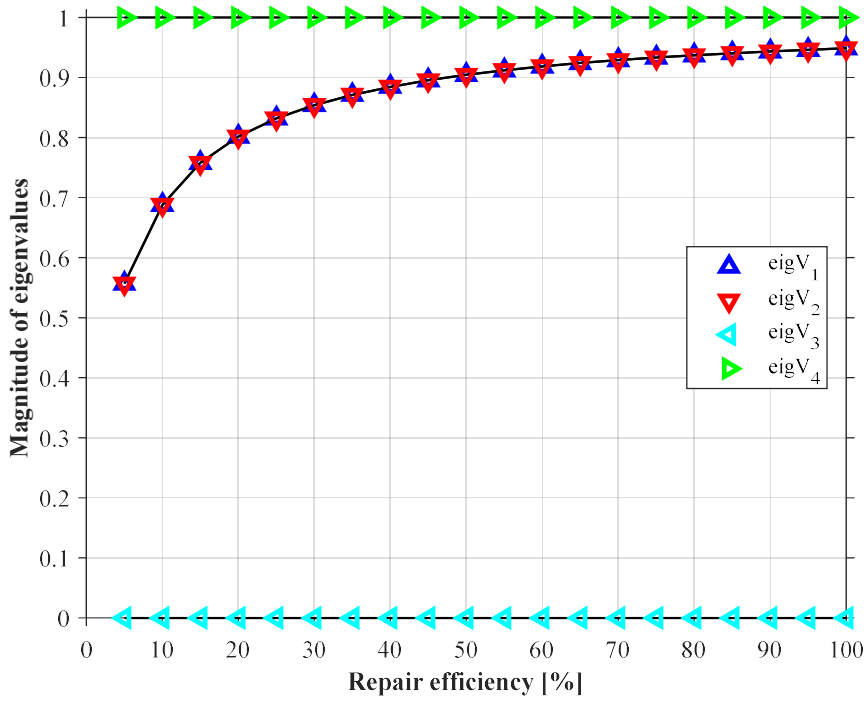


Figure 6-8: Eigenvalue magnitudes of 'one-out-of-two' IEC 61850 SCN at 90% diagnostic coverage

Compared to when the diagnostic coverage of the system was 99%, the reduced eigenvalue magnitudes result in an increased spectral gap between the unit circle and the second-largest eigenvalue (i.e., $max_{i:|\gamma_i|<1}|\gamma_i|$), indicating an increased rate of system convergence towards an absorbing state of the system represented by eigenvalue magnitude of 1-term in (6-15) or a limit cycle if multiple eigenvalues of the magnitude of 1 existed. Figure 6-9 depicts the system eigenvalues on a complex plane, where the system's dynamics can be determined; as well as how the spectral gap changes with different repair efficiency ($r_{eff}$) levels while diagnostic coverage ($e_{dc}$) is kept constant at 90%.

The layout formation of the eigenvalues is not being affected by the change in repair efficiency ($r_{eff}$) even though the diagnostic coverage of the system has reduced to 90%. However, it is noticeable that the spectral gap increases with lower diagnostic coverage values and repair efficiency as more system errors become undiscoverable, which affects the system's rate of convergence, as discussed earlier in subsection 6.6.1. In addition, the system does not become periodic at any level of repair efficiency while at 90% diagnostic coverage since only one eigenvalue has a magnitude of 1. In the system presented above, the spectral gap at 5% repair efficiency had increased than when the diagnostic coverage was 99%, implying that the system's mean state transition before failure is relatively lower.

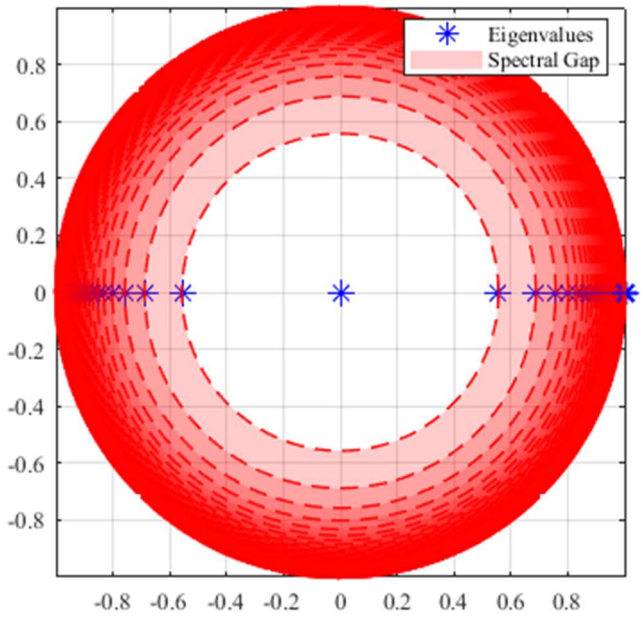


Figure 6-9: Eigenvalues of 'one-out-of-two' IEC 61850 SCN at 90% diagnostic coverage

Figure 6-10 depicts the system transition probability diagram with states grouped into classes according to their behavioural characteristics when the repair efficiency is 5%. It can be observed that states S-1, S-2 and S-3 still communicate in a transient dynamic manner as in the case where the diagnostic coverage was 99%, while state S-4 is still aperiodic and recurrent. The low transition probability of system state transitions from states S-2 and S-3 to state S-1 is due to the low repair efficiency at the specified system diagnostic coverage factor that highly increases the system's probability to transition into state S-4, as depicted in Figure 6-10.

However, the state transition probabilities from states S-2 and S-3 to state S-1 reduce when more system faults remain hidden, while the system's probability of entering state S-4 increases. The system's probability of transitioning to state S-4 is because it accumulates more unresolved errors as time progresses than when the diagnostic coverage is 99%. Even so, the nature of state interactions is the same for the simulated repair efficiency ($r_{eff}$) range. Figure 6-11 depicts the state probability of the system's availability and unavailability over 80-time steps as repair efficiency is varied from 5% to 100% at 90% system diagnostic coverage. Again, the system's availability reduces to almost 0 in 10-time steps when the repair efficiency is 5%, and in just over 80-time steps at repair efficiency of 100%.

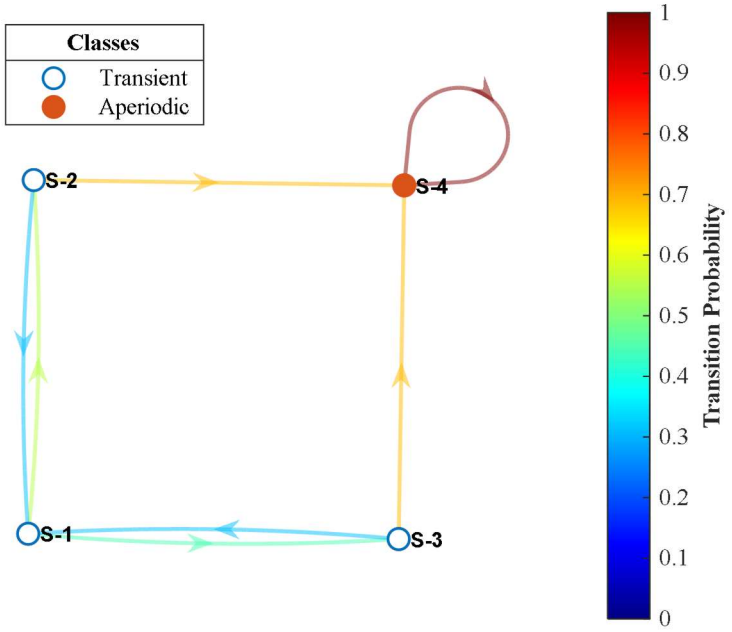


Figure 6-10: State transition probability diagram of 'one-out-of-two' IEC 61850 SCN at 90% diagnostic coverage and 5% repair efficiency.

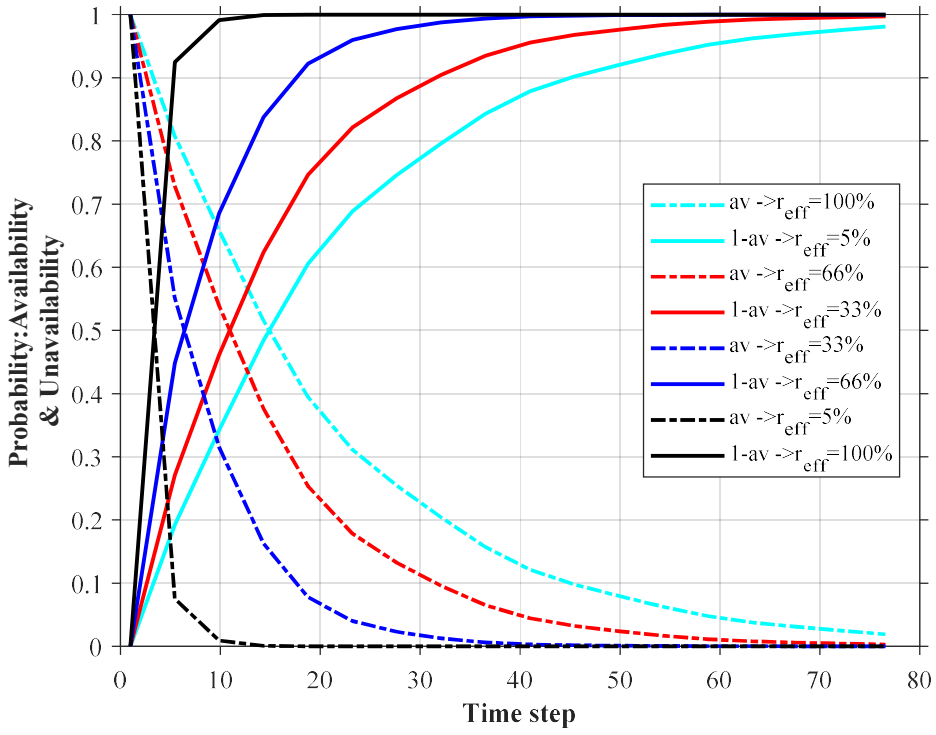


Figure 6-11: System probability – availability and unavailability with repair efficiency of 5% to 100% at 90% diagnostic coverage.

The system's availability relatively reduces because only 5% of repairs are executed when the repair efficiency is 5%, whereas only 90% of system errors are assumed to have been identified at this system diagnostic coverage level. The system's availability improves as repair efficiency increases to 100%, which is again expected since identified system errors are fully repaired at 100% repair efficiency. Figure 6-12 depicts the system state transitions for different repair efficiency levels at 90% system diagnostic coverage and is consistent with the eigenvalue magnitudes and the spectral gap depicted in Figure 6-9.

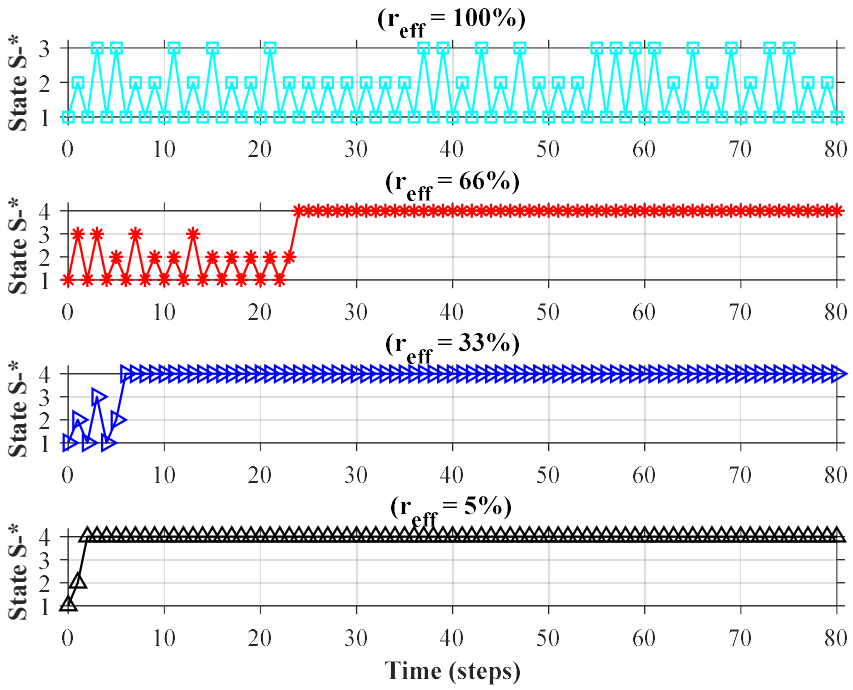


Figure 6-12: System state transition simulated at varying repair efficiency of 5% to 100% and 90% diagnostic coverage.

As was observed in Figure 6-8 and Figure 6-9, low repair efficiency level resulted in low eigenvalue magnitudes for all $|\gamma_i| < 1$ as in the case when the system was assumed to have 99%% diagnostic coverage. This condition results in a relatively lower spectral gap, hence the system's reduced mean state transitions before failure. However, the system's mean state transitions reduced when the system was assumed to have 99% diagnostic coverage.

### 6.6.3 Low diagnostic coverage level

Subsystems A and B are assumed to have 60% diagnostic coverage ($e_{dc}$) factors in this case study, while their failure and repair rates remain unchanged as stated in the previous case studies. As before, the long-term dynamical impact of the repair efficiency ($r_{eff}$) is examined by observing the magnitudes of the respective system eigenvalues ($\gamma_j$) under varying levels of repair efficiency. Figure 6-13 depicts the magnitudes of the system eigenvalues under

varying levels of repair efficiency. It can be observed in Figure 6-13 that only two eigenvalues are affected by the change in repair efficiency as in the cases of 99% and 90% diagnostic coverage factors, while the other two eigenvalues remain constant at magnitudes 0 and 1, respectively. It is also noticeable that the increase in repair efficiency closer to 100% does not significantly change the eigenvalue magnitudes, which is consistent with the observations made at diagnostic coverage factors of 99% and 90%. However, the impact is more visible than in the two previous case studies.

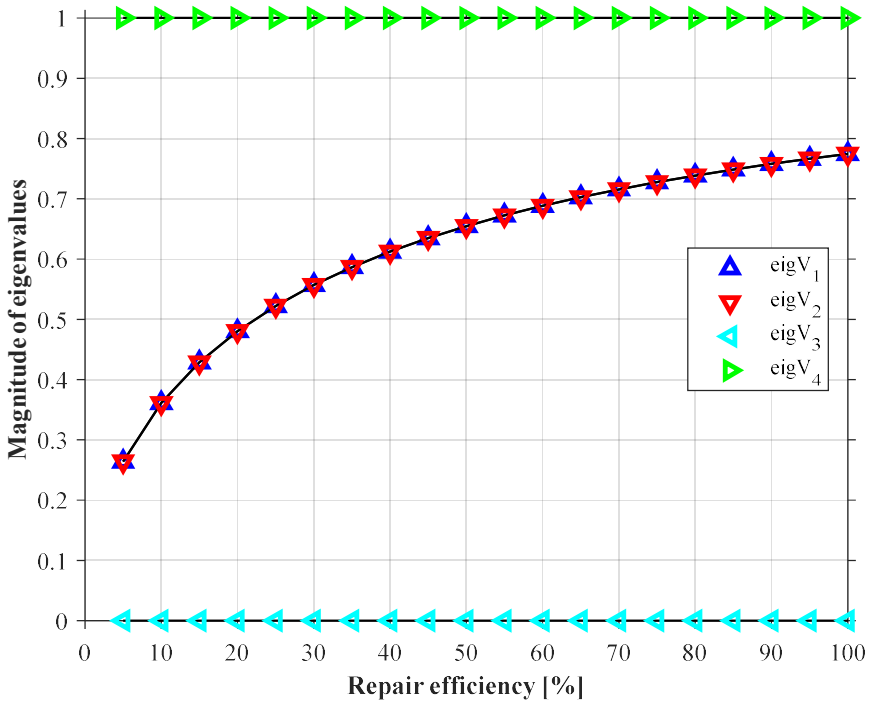


Figure 6-13: Eigenvalue magnitudes of 'one-out-of-two' IEC 61850 SCN at 60% diagnostic coverage

Again, compared to when the diagnostic coverage of the system was 99% and 90%, the lower eigenvalue magnitudes lead to a substantial spectral gap between the unit circle and the second-largest eigenvalue (i.e. $max_{i:|\gamma_i|<1}|\gamma_i|$), indicating an even much higher rate of system convergence towards an absorbing state of the system represented by eigenvalue magnitude of 1-term in (6-15) or a limit cycle if multiple eigenvalues of the magnitude of 1 existed. Figure 6-14 depicts the system eigenvalues on a complex plane, where the system dynamics can be determined; as well as how the spectral gap changes with different repair efficiency ($r_{eff}$) levels while diagnostic coverage ($e_{dc}$) is kept constant at 60%.

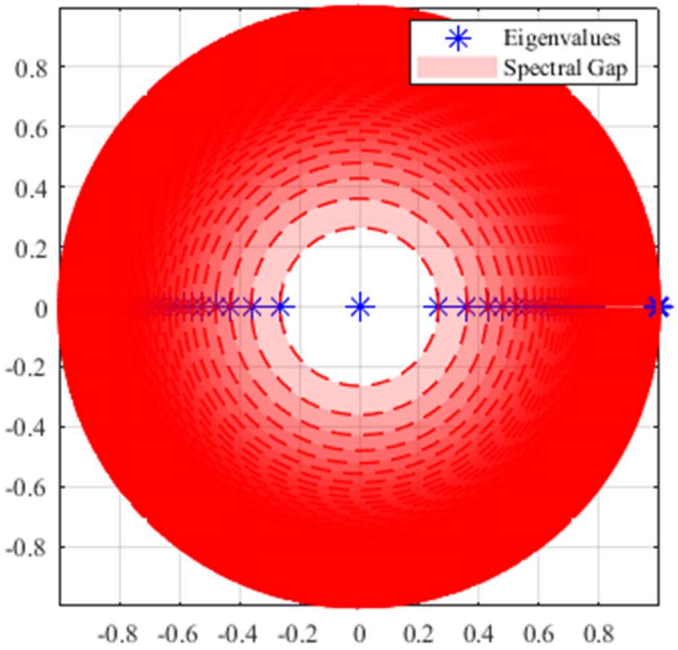


Figure 6-14: Eigenvalues of 'one-out-of-two' IEC 61850 SCN at 60% diagnostic coverage

As in the previous case studies, at 99% and 90% diagnostic coverage factors, the eigenvalues' formation is not affected by the change in repair efficiency even though the system's diagnostic coverage has reduced further to 60%. Nevertheless, it is noticeable that the spectral gap increases even more with lower diagnostic coverage values and repair efficiency. Expectedly so, more system errors remain hidden and unresolved, which increases the system's rate of convergence, as discussed earlier in subsections 6.6.1 and 5.6.2. In addition, the system does not become periodic at any repair efficiency level while at 60% diagnostic coverage since only one eigenvalue has a magnitude of 1. Hence, the spectral gap at 5% $r_{eff}$ had increased further than when the diagnostic coverage was 90%, implying that the system's mean state transition before failure is even much lower than before.

Figure 6-15 depicts the system transition probability diagram with states grouped into classes according to their behavioural characteristics when the repair efficiency is 5%. It can be observed that states S-1, S-2 and S-3 still communicate in a transient dynamic manner as in the case where the diagnostic coverage was 99% and 90%, respectively, whereas state S-4 is aperiodic and recurrent as before. In contrast to when the diagnostic coverage of the system is 99% or 90%, the probability of the system transitioning from states S-2 and S-3 to state S-1 significantly reduces as a result of the low diagnostic cover at 5% repair efficiency, and this is because more errors remain hidden and unresolved in the system.

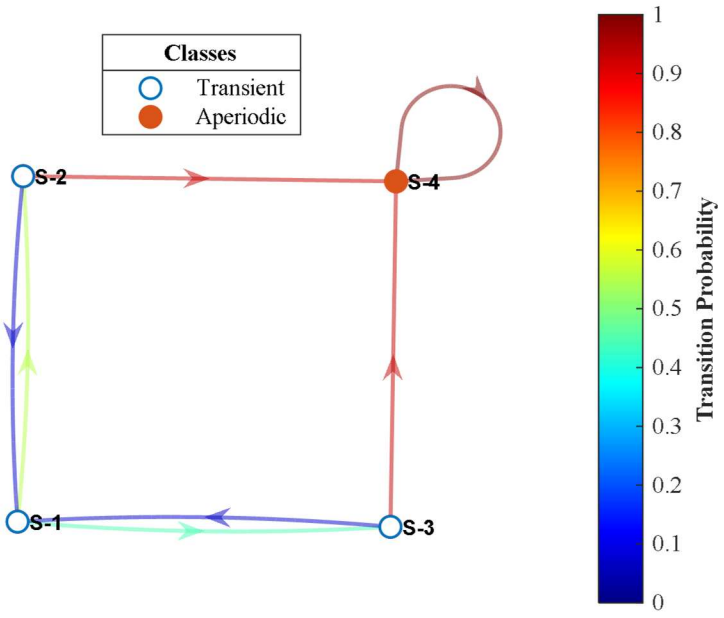


Figure 6-15: State transition probability diagram of 'one-out-of-two' IEC 61850 SCN at 60% diagnostic coverage and 5% repair efficiency.

The specified system diagnostic coverage ($e_{dc}$) factor of 60% increases the probability of the system transitioning into state S-4 as depicted in Figure 6-15 since almost all system errors are hidden and unresolved than when the diagnostic coverage is 99% or 90%, resulting in high system errors accumulating over time. Even so, the nature of state interactions remains for simulated repair efficiency ($r_{eff}$) range. Figure 6-16 depicts the state probability of the system's availability and unavailability over 35-time steps as repair efficiency is varied from 5% to 100% at 60% system diagnostic coverage. It can be observed that the system's availability reduces to almost 0 in just above 5-time steps when the repair efficiency is 5%, which represents a degradation in system performance than when the system is assumed to be at 99% and 90% diagnostic coverage.

Figure 6-17 depicts the system's state transitions for different repair efficiency levels at 60% system diagnostic coverage, consistent with the eigenvalue magnitudes and the spectral gap in Figure 6-13. The simulated states' transition results are consistent with the observations made when the system was assumed to be at 99% and 90% diagnostic coverage levels, highlighting the significance of the information derived by studying the system transition's eigenvalues probability matrix.

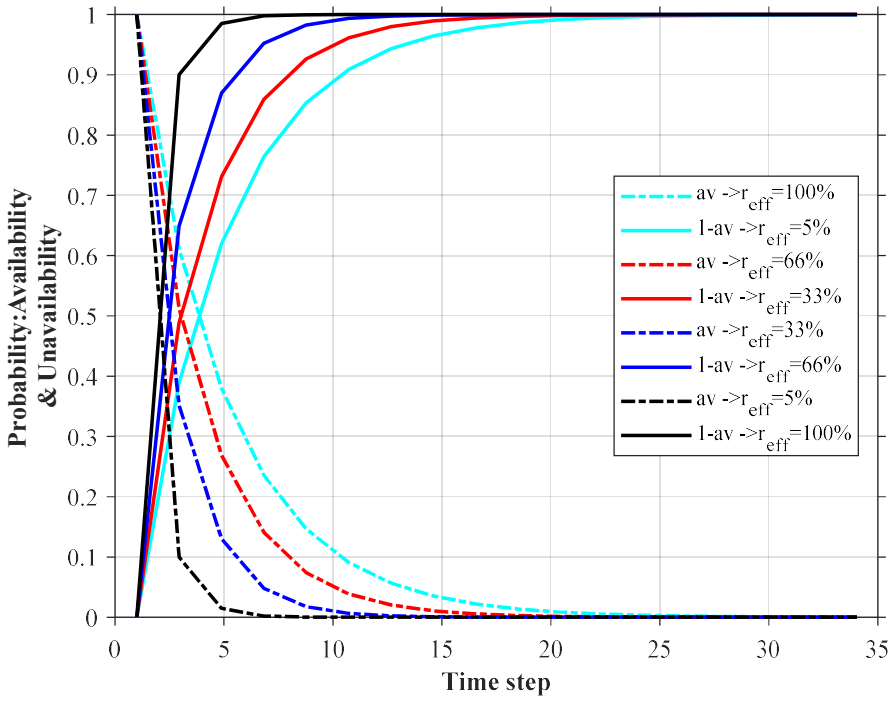


Figure 6-16: System probability – availability and unavailability with repair efficiency of 5% to 100% at 60% diagnostic coverage.

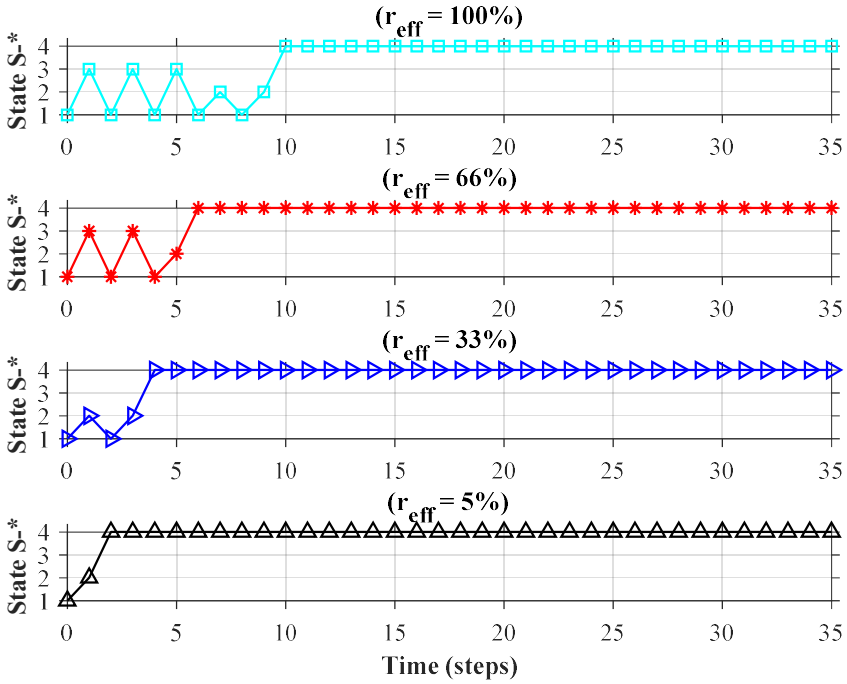


Figure 6-17: System state transition simulated at varying repair efficiency of 5% to 100% and 60% diagnostic coverage.

### 6.6.4 Mixed diagnostic coverage levels

This case study relaxes the assumption on the subsystems' diagnostic coverages and assumes that they have different diagnostic capabilities. The relaxation of the assumption is necessary because different system channels are often used to minimise the impact of CCFs. To investigate the impact of mixed subsystem diagnostic coverages, Table 6-1 presents three scenarios of individual subsystem diagnostic coverages that have been arbitrarily chosen to investigate the impact of mixed diagnostic coverages on the system performance and its dynamical behaviour. The combinations of subsystem diagnostic coverages investigated include 'medium and high', 'medium and low', as well as 'high and low', represented by scenarios C-1, C-2 and C-3, respectively. Figure 6-18 depicts the response of the transition probability matrix's eigenvalue magnitudes under different levels of repair efficiency for the case studies presented in Table 6-1.

Table 6-1: Case studies of mixed diagnostic coverage levels

| Case study | C-1 | C-2 | C-3 |
|---|---|---|---|
| Subsystem 'A' diagnostic coverage ($e_{dcA}$) | 90% | 90% | 99% |
| Subsystem 'B' diagnostic coverage ($e_{dcB}$) | 99% | 60% | 60% |

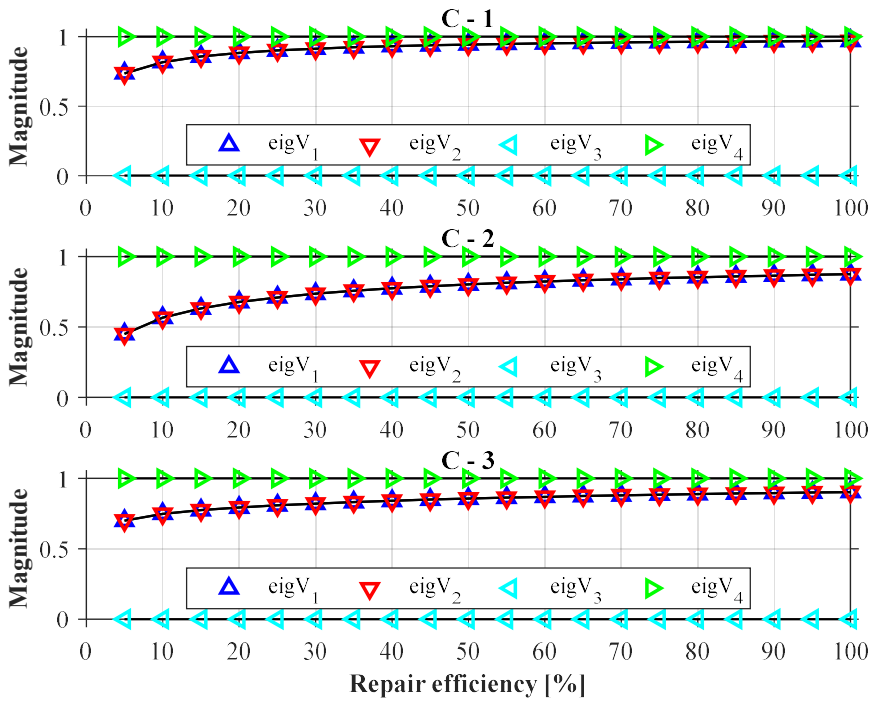


Figure 6-18: Case studies C-1, C-2 and C-3 of 'one-out-of-two' system-eigenvalue analysis

It is observable in Figure 6-18(C-1) that the spectral gap reduces with increasing repair efficiency, which implies that the mean system state transitions improve with increasing repair efficiency as in the previous case studies. Even so, the eigenvalue magnitudes have reduced

than when both subsystems have 99% diagnostic coverages. This trend is noticeable in the results of C-2 and C-3 case studies depicted in Figure 6-18(C-2) and Figure 6-18(C-3). Moreover, it is observable that the spectral gap increases with low system diagnostic coverages for a given level of repair efficiency. In addition, repair efficiencies closer to 100% do not significantly impact the eigenvalues' magnitudes, especially for systems with high diagnostic coverage presented by case study C-1 parameters.

### 6.6.5 Mixed repair efficiency and diagnostic coverage levels

This case study relaxes both the assumptions on the subsystems' repair efficiencies and diagnostic coverages and assumes that they have different repair efficiencies and diagnostic coverages. The relaxation of the assumptions is necessary because different teams can be used to maintain different system channels to minimise the impact of CCFs. It is also possible that the maintenance team does not have the same level of expertise on both subsystems. Table 6-2 presents three scenarios of individual system diagnostic coverages that have been arbitrarily chosen to investigate the impact of mixed repair efficiency and diagnostic coverages on the system performance and its dynamical behaviour. The combinations of subsystem diagnostic coverages investigated include ‘medium and high’, ‘medium and low’, as well as ‘low and low; represented by scenarios C-4, C-5 and C-6, respectively. Figure 6-19 depicts the response of the transition probability matrix's eigenvalue magnitudes under different levels of repair efficiency for the case studies presented in Table 6-2.

Table 6-2: Case studies of mixed repair efficiencies and diagnostic coverages

| Case study | C-4 | C-5 | C-6 |
|---|---|---|---|
| Subsystem A diagnostic coverage ($e_{dcA}$) | 90% | 90% | 60% |
| Subsystem B diagnostic coverage ($e_{dcB}$) | 99% | 60% | 60% |
| Subsystem A repair efficiency ($r_{effA}$) | 95% | 95% | 95% |
| Subsystem B repair efficiency ($r_{effB}$) | 5%-100% | 5%-100% | 5%-100% |

It is observable in Figure 6-19(C-4) that the spectral gap reduces with increasing repair efficiency of subsystem B. A similar response is noticeable in the results of C-5 and C-6 scenarios depicted in Figure 6-19(C-5) and Figure 6-19(C-6). However, subsystem B repair efficiency variations have an insignificant impact on the eigenvalue magnitudes while the repair efficiency of subsystem A is constant at 95%, particularly when the subsystems have medium to high diagnostic coverages.

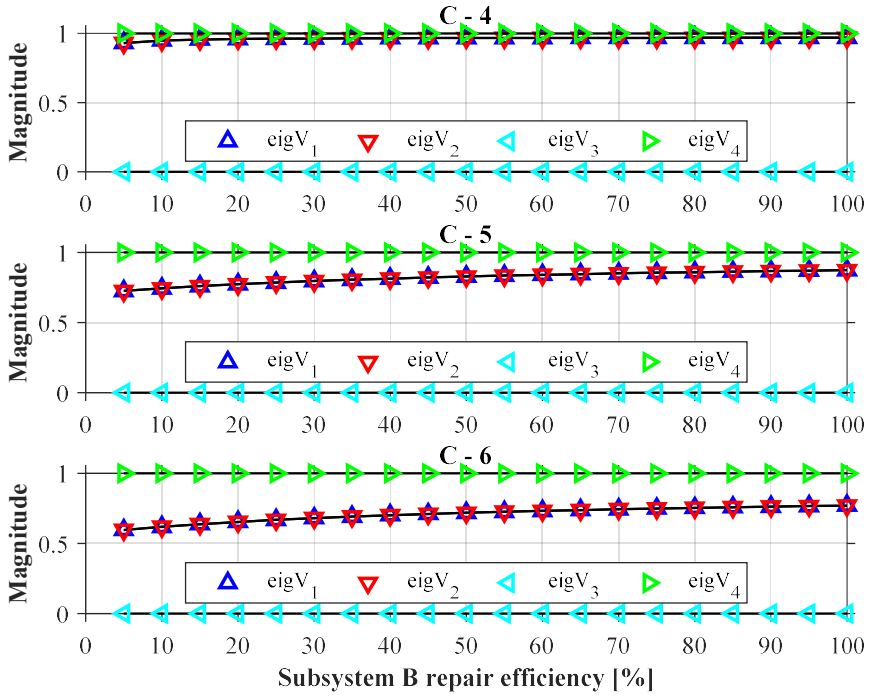


Figure 6-19: Case studies C-4, C-5 and C-6 of 'one-out-of-two' systems-eigenvalue analysis

Nevertheless, it is observable that the spectral gap increases further with low system diagnostic coverages at various repair efficiency levels. In addition, repair efficiencies closer to 100% do not significantly impact the eigenvalues' magnitudes, especially for systems with high diagnostic coverage presented by scenario C-4 parameters.

### 6.6.6 Impact of common cause failures in system dynamics and performance

This case study relaxes the assumption made earlier relating to the two subsystems A and B being entirely independent. The level of CCFs represented by the parameter β has been set to zero in previous case studies; this assumption is relaxed because it is almost impossible to have two entirely independent subsystems. The results presented in this section demonstrate the impact of CCFs on the system's dynamical behaviour and performance. The repair efficiency of the subsystems is considered 95%. The scenarios presented in this case study are also based on the ISO 849-1 diagnostic coverage levels.

#### 6.6.6.1 High diagnostic coverage level

Figure 6-20 depicts the transition matrix's eigenvalues plotted on a complex plane when the fault coverage level is 99%. Two sets of eigenvalues for β at 10% and 50% show that their layout formation does not change for different levels of CCFs. Nevertheless, the spectral gap between the second-largest eigenvalue and magnitude one increases as the level of CCFs increases, indicating a reduction in mean system state transitions. Figure 6-21 depicts the system's transition diagram when the CCF level is 50%. It is observable that the system can

quickly move to state S-4 from state S-1 based on the transition probabilities. Hence, the CCF level of CCFs impacts only how the system transitions from state S-1 and the rate of system convergence.

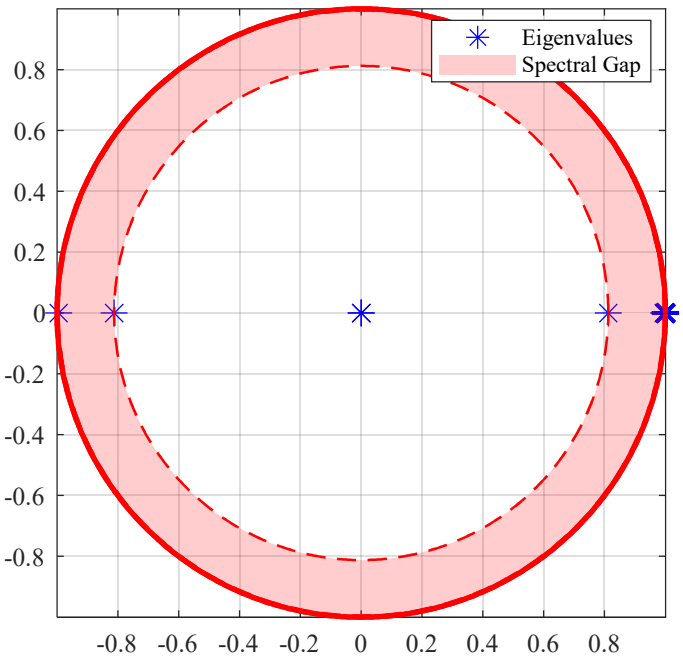


Figure 6-20: System eigenvalue layout formation and the spectral gap at 0% and 50% CCFs

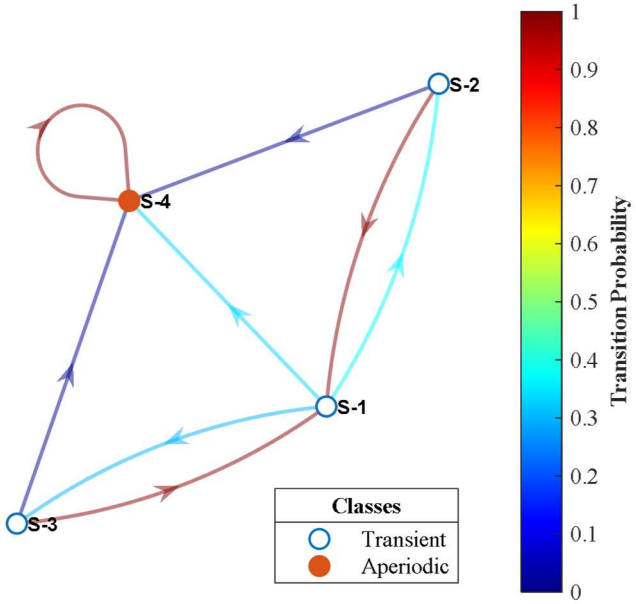


Figure 6-21: State transition probability diagram at 50% CCFs

### 6.6.6.2 Medium diagnostic coverage level

In this scenario, the system diagnostic coverage is assumed to be 90%. Figure 6-22 depicts the system eigenvalue layout formation on the complex plane.

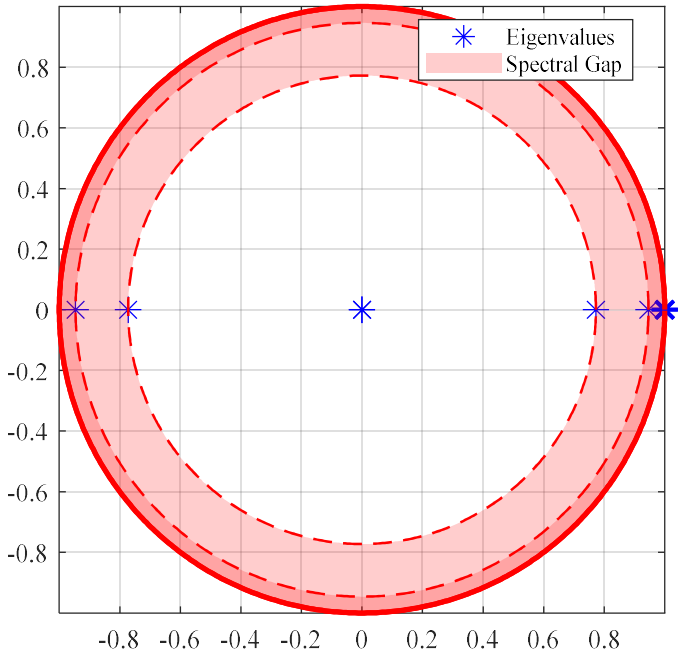


Figure 6-22: System eigenvalue layout formation and the spectral gap at 0% and 50% CCFs

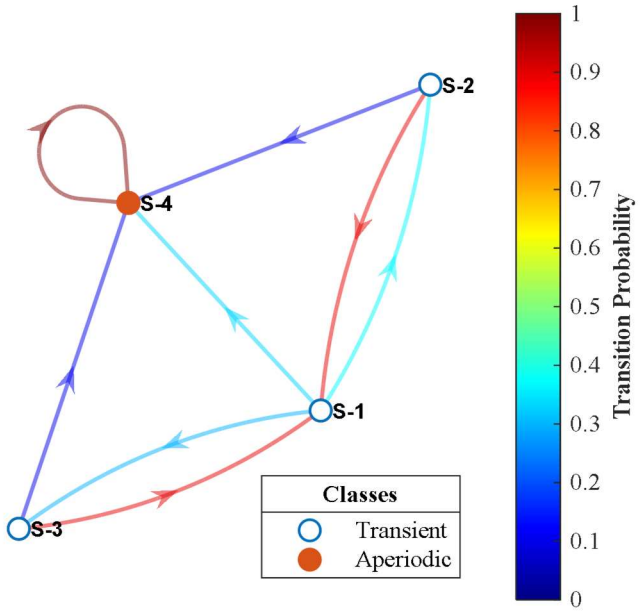


Figure 6-23: State transition probability diagram at 50% CCFs

It can be observed that the spectral gap between the second-largest eigenvalue and the unit circle has increased compared to the results of the previous scenario, which indicates a reduction in system performance considering the mean state transitions of the system. Even so, the eigenvalues' layout formation has not changed; and remains the same for different levels of β. Therefore, the system's dynamic behaviour has not changed even though the diagnostic coverage has been reduced. Figure 6-23 depicts the system probability transition diagram. In contrast to the results presented in the previous scenario, the probabilities of the system transitioning back to state S-1 from either states S-2 or S-3 have reduced, whereas the probabilities of the system transitioning to state S-4 remain the same; which results in lower transitions than when the system has 99% diagnostic coverage.

#### 6.6.6.3 Low diagnostic coverage level

Figure 6-24 and Figure 6-25 depict the eigenvalue layout formation and the system's transition probability diagram when its diagnostic coverage is 60%, respectively. It is noticeable that the spectral gap between the second-largest eigenvalue and the unit circle increases while the formation of the eigenvalues remains unchanged, indicating the stability of the 'one-out-of-two' system under different levels of diagnostic coverage levels and CCFs. The change in state transition probabilities resulting in the increased spectral gap is depicted in Figure 6-25. It is noticeable that the system's likelihood of moving back to state S-1 from either states S-2 or S-3 has decreased further while the system's likelihood of moving to state S-4 has increased.

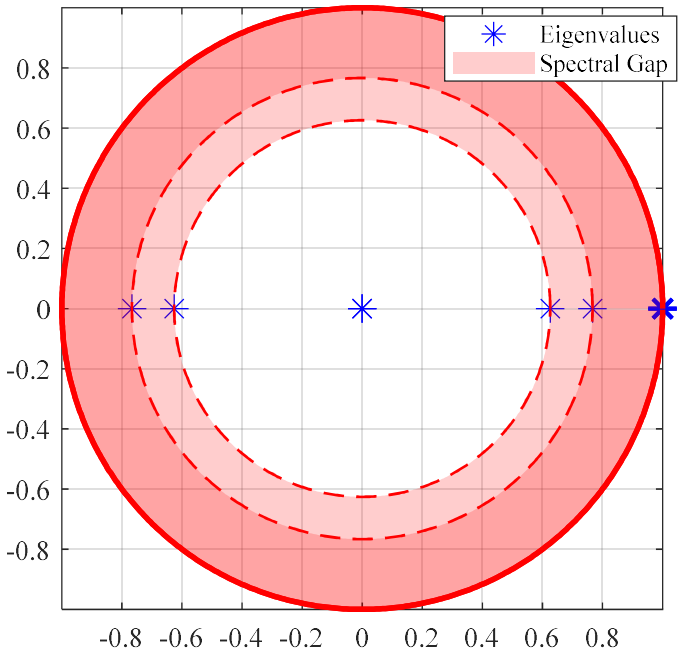


Figure 6-24: System eigenvalue layout formation and the spectral gap at 0% and 50% CCFs

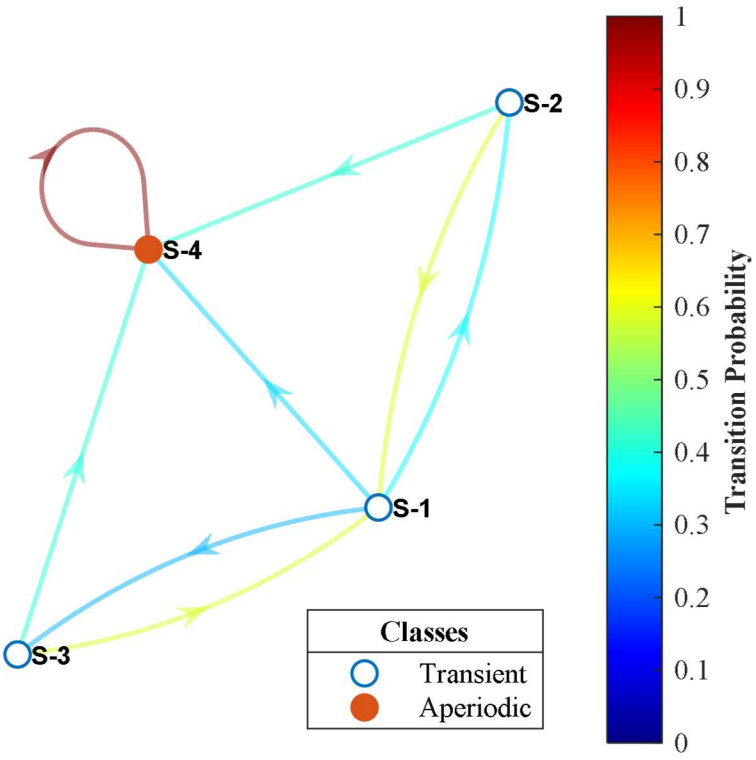


Figure 6-25: State transition probability diagram at 50% CCFs

## 6.7 Chapter conclusion

In this chapter, the impact of imperfect repairs and system diagnostic coverage on the dynamical behaviour of multi-state IEC 61850 based SCN was investigated using Markov partitions and symbolic dynamics. The most commonly referenced system diagnostic coverage levels in IEC 61508 were used to investigate the impact of different repair efficiency levels on the communication system. The investigation's proposed technique advances the Markov time series simulation's insights so far as the system's dynamics and performance are concerned. It is evident from the simulation results that the 'one-out-of-two' IEC 61850 based SCN is dynamically stable through design considerations, and therefore, suitable for implementing mission-critical applications. The significance of system repair efficiency $(r_{eff})$ and diagnostic coverage $(e_{dc})$ factors were highlighted and demonstrated, of which optimal selection of the respective factors is required.

Therefore, in context, the desired system dynamics are characterised by aperiodic behaviour and a clearly defined recurrent fail-safe state to ensure plant and personnel safety since any form of periodic system failures would indicate known failure modes on the system. The objective is to avoid failures modes through design considerations to ensure that the system does not become unmanageable. It is also a desirable property for the system to have

high mean state transitions before entering the failed state, of which the behaviour is characterised by a small spectral gap on the complex plane. Even so, the eigenvalue method does not provide transient system performance indicators to optimise the system objectively. Moreover, the individual factors' incremental effect on the mean system state transitions cannot be determined in total or percentages, optimising the various subsystem parameters even more challenging. Chapter 7 addresses the shortcomings of the eigenvalue analysis method based on its sensitivity and elasticity on the various system parameters.

# CHAPTER 7

# SENSITIVITY AND ELASTICITY OF SYSTEM RELIABILITY TO REPAIR AND COMMON CAUSE FAILURE FACTORS

## 7.1 Introduction

This chapter advances the eigenvalue analysis method presented in Chapter 6. The method presented in this chapter employs sensitivity and elasticity analysis of the mean system state transitions to repair efficiency, diagnostic coverage and Common Cause Failure (CCF) factors in determining their effect on the system performance [2]. The system's sensitivity and elasticity to the factors enable their effectiveness to be analysed at a much lower system abstraction than the eigenvalue analysis method. In contrast to sensitivity and elasticity analysis, the eigenvalue analysis method focuses on the system dynamical behaviour and the spectral gap of the second largest eigenvalue(s) as the indicators of system performance [95], [142], [143]. The drawback of only using the eigenvalue analysis method is that states interactions are described at a very high level, making it impossible to determine the mean number of states transitions between any two states because the focus is asymptotic and not transient. The analysis of lower-level system parameters impacting the system's performance enables the factors' optimisation at the subsystem level because regardless of how small the incremental system performance is, it can be evaluated, analysed, compared and adjusted for optimisation purposes [150].

Sensitivity and elasticity analysis enables accurate determination of the system's response based on the number of mean system state transitions to changes in the level of imperfect repairs and diagnostic coverage for all possible system initial conditions; which can be used to optimise the level of repair efficiency and system diagnostic coverage to achieve optimal system performance. Hence, using both analysis methods provide a comprehensive state of system behavioural dynamics and performance to enable system optimization [15], [16]. The main advancements of the chapter are the following:

- Demonstrate the significance of accurate and comprehensive system fault diagnostics and repairs to achieve high system reliability performance for mission-critical systems in power distribution centres.
- Provide complimentary analysis technique that advances the asymptotic eigenvalue analysis method based on absorbing Markov chain and matrix calculus to focus on the system's transient states.
- Analysis of system responsiveness to imperfect repairs (viz. repair efficiency and system diagnostic coverage factors) enabling objective optimisation of the system Mean Time To Failure (MTTF) based on the mean state transitions at the subsystem level.

The chapter's layout is as follows: The context of the sensitivity and elasticity analysis of the mean system state transitions to the repair and diagnostic coverage factors are presented in section 7.2. Section 7.3 presents the derivation of the absorbing Markov Chain fundamental matrix's sensitivity and elasticity, whereas section 7.4 presents the modelling of sensitivity and elasticity of a 'one-out-of-two' system to imperfect repair factors. The results and discussions of the case studies are presented in section 7.5. Section 7.6 highlights the findings of the case studies and observations and thus concludes the chapter.

## 7.2 Sensitivity and elasticity

The magnitudes of the eigenvalues of a transition probability matrix are dependent on both the repair efficiencies of the individual subsystems and their diagnostic coverages, as demonstrated in [8], [13]. The non-linear response of the eigenvalue magnitudes to incremental repair efficiencies and system diagnostic coverage factors raises the need to know how the system mean state transition responds in absolute quantity or percentage values when the individual factors are increased to improve the performance level of the system. In science, economics and financial studies, the concept of proportional sensitivity or elasticity is used to measure the responsiveness of a system when one or more dependent variables change. This concept is also applicable in engineering systems where the system's performance depends on various factors. Sensitivity measures the system's response when a dependent variable changes in total quantities, whereas elasticity measures the same using per unit or percentage quantities [150]–[152].

This chapter investigates the sensitivity and elasticity of the mean system state transitions on the repair efficiency, diagnostic coverage and CCF factors. The transition probability matrix's fundamental matrix is used to investigate the transient states' sensitivity and elasticity to the repair, diagnostic coverage and common causes of failure factors. Matrix calculus differential based Kronecker method is adopted in this research work because the focus is on the effect of one system input parameter at a time and not the interaction between input parameters since the diagnostic coverage of the system is embedded in the system design itself and cannot be changed with ease once the system is commissioned and running [75], [105], [153]. This approach makes it possible to determine whether adjusting the respective subsystems' factors is beneficial or not, given a specific system performance level [96], [101], [105], [106]. Thus, the optimisation of the system can be achieved at the subsystem level as desired. The following section presents the derivation of the fundamental matrix's sensitivity and elasticity.

### 7.3 Sensitivity and elasticity of the fundamental matrix

An absorbing Markov chain is characterised by at least one recurrent state in the system, of which the form of the state probability transition matrix is given by (7-1),

$$\boldsymbol{P} = \begin{bmatrix} (\boldsymbol{Q}) & (\boldsymbol{M}) \\ (\mathbf{0}) & (\boldsymbol{I}) \end{bmatrix} \tag{7-1}$$

Where $\boldsymbol{Q}$ is a $n\,x\,n$ transient probability matrix, $\boldsymbol{M}$ is an n $x\,m$ matrix of $m$ vectors comprising each of the transient states' probabilities to transit into the respective recurrent states in the system, and $m$ is the number of recurrent states. The matrix $\boldsymbol{I}$ is the identity matrix of the order $m$ representing the number of recurrent states in the system, whereas $\mathbf{0}$ is a zero matrix. As demonstrated in [8], [75], the mean number of states transitions of the system is given by the elements of the fundamental matrix $\boldsymbol{N}$ in (7-2) [75], [104], [153],

$$\boldsymbol{N} = (\boldsymbol{I} - \boldsymbol{Q})^{-1} \tag{7-2}$$

To derive the sensitivity of the fundamental matrix $\boldsymbol{N}$, it is considered that $\boldsymbol{N}$ satisfies the identity given by (7-3),

$$\boldsymbol{I} = \boldsymbol{N}\boldsymbol{N}^{-1} \tag{7-3}$$

Now, differentiating both sides of (7-3) gives (7-4),

$$\mathbf{0} = (d\boldsymbol{N})\boldsymbol{N}^{-1} + \boldsymbol{N}(d\boldsymbol{N}^{-\mathbf{1}}) \tag{7-4}$$

Reorganising (7-4), applying the vec operator and Roth's theorem leads to (7-5),

$$\text{vec}\,\mathbf{0} = [(\boldsymbol{N}^{-1})^{\mathrm{T}} \otimes \boldsymbol{I}]\; d\text{vec}\,\boldsymbol{N} + (\boldsymbol{I} \otimes \boldsymbol{N})\; d\text{vec}\,\boldsymbol{N}^{-1} \tag{7-5}$$

Solving (7-5) for $d\text{vec}\,\boldsymbol{N}$ simplifies to (7-6),

$$d\text{vec}\,\boldsymbol{N} = [(\boldsymbol{N}^{-1})^{\mathrm{T}} \otimes \boldsymbol{I}]^{-1}\,(\boldsymbol{I} \otimes \boldsymbol{N})\; d\text{vec}\,\boldsymbol{Q} \tag{7-6}$$

Applying the Kronecker product identity given by (7-7) and (7-8) simplifies to (7-9) provided that the dimensions of the matrices satisfy the operators [104], [154],

$$(\boldsymbol{A} \otimes \boldsymbol{B})^{-1} = \boldsymbol{A}^{-1} \otimes \boldsymbol{B}^{-1} \tag{7-7}$$

$$(\boldsymbol{A} \otimes \boldsymbol{B})(\boldsymbol{C} \otimes \boldsymbol{D}) = (\boldsymbol{A}\boldsymbol{C} \otimes \boldsymbol{B}\boldsymbol{D})` \tag{7-8}$$

$$d\text{vec}\,\boldsymbol{N} = (\boldsymbol{N}^{\mathrm{T}} \otimes \boldsymbol{N}) d\text{vec}\,\boldsymbol{Q} \tag{7-9}$$

Using the identification theorem, (7-9) can be written in the form of (7-10),

$$\frac{d\text{vec}\,\boldsymbol{N}}{d\text{vec}\,\boldsymbol{Q}^{\mathrm{T}}} = \boldsymbol{N}^{\mathrm{T}} \otimes \boldsymbol{N} \tag{7-10}$$

Thus, if $\boldsymbol{N}$ is a function of a vector $U$ of variables of interest, (7-10) can be extended to give (7-11) by using the chain rule, which is the sensitivity of $\boldsymbol{N}$ to vector $U$ [101], [104], [106],

$$\frac{d\text{vec}\,\boldsymbol{N}}{d\text{vec}\,U^{\mathrm{T}}} = (\boldsymbol{N}^{\mathrm{T}} \otimes \boldsymbol{N})\ \frac{d\text{vec}\,\boldsymbol{Q}}{d\text{vec}\,U^{\mathrm{T}}} \tag{7-11}$$

Since the proportional effectiveness (elasticity) of $y_i$ to $x_j$ is given by (7-12), the elasticity of vector $Y$ to $X$ is given by (7-13) [104], [155],

$$\frac{\varepsilon y_i}{\varepsilon x_j} = \frac{x_j}{y_i}\frac{dy_i}{dx_j} \tag{7-12}$$

$$\frac{\varepsilon Y}{\varepsilon X^{\mathrm{T}}} = \mathrm{D}(Y)^{-1}\ \frac{dY}{dX^{\mathrm{T}}}\ \mathrm{D}(X) \tag{7-13}$$

The notation $\mathrm{D}(X)$ is a square matrix with the elements of the vector $X$ on the diagonal of the matrix (i.e., $a_{ij} = 0$ for $i \neq j$). Consequently, the elasticity of the fundamental matrix $\boldsymbol{N}$ to vector $U$ comprising all lower-level parameters of interest is given by (7-14) [96], [104],

$$\frac{\varepsilon\text{vec}\,\boldsymbol{N}}{\varepsilon U^{\mathrm{T}}} = \mathrm{D}(\text{vec}\,\boldsymbol{N})^{-1}\ \frac{d\text{vec}\,\boldsymbol{N}}{dU^{\mathrm{T}}}\ \mathrm{D}(U) \tag{7-14}$$

The following section presents the lower-level parameter model of the state probability transition matrix of the 'one-out-of-two' protection system and the sensitivity and elasticity of the mean number of system state transitions to the repair efficiency and diagnostic coverage factors.

## 7.4 Modelling sensitivity and elasticity to repair factors: 'one-out-of-two' system

The state transition diagram of the 'one-out-of-two' system in Chapter 6 is depicted in Figure 7-1 for ease of reference. In order to model the proportional sensitivity of the system to repair and diagnostic coverage factors, the state transition probability matrix $\boldsymbol{P_s}$ describing the state transitions of the system is rewritten as a function of lower-level system parameters

of interest (i.e. repair efficiency, diagnostic coverage and CCF factors) in its stochastic form given by (7-15) [2], [75].

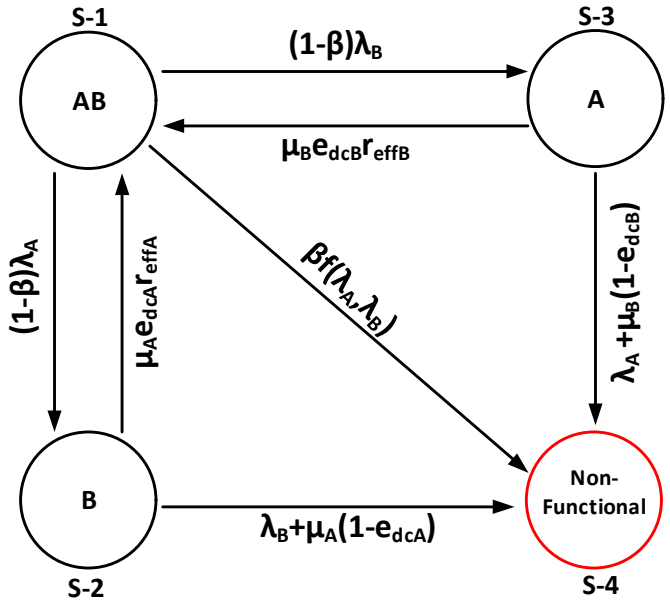


Figure 7-1: 'One-out-of-two' system state transition diagram incorporating quality of repairs

$$\boldsymbol{P_s} = \begin{bmatrix} \frac{1-\boldsymbol{P}_{12}-\boldsymbol{P}_{13}-\boldsymbol{P}_{14}}{(1-\beta)\lambda_A+(1-\beta)\lambda_B+\beta f(\lambda_A,\lambda_B)} & \frac{(1-\beta)\lambda_A}{(1-\beta)\lambda_A+(1-\beta)\lambda_B+\beta f(\lambda_A,\lambda_B)} & \frac{(1-\beta)\lambda_B}{(1-\beta)\lambda_A+(1-\beta)\lambda_B+\beta f(\lambda_A,\lambda_B)} & \frac{\beta f(\lambda_A,\lambda_B)}{(1-\beta)\lambda_A+(1-\beta)\lambda_B+\beta f(\lambda_A,\lambda_B)} \\ \frac{\mu_A e_{dcA} r_{effA}}{\mu_A e_{dcA} r_{effA}+(\lambda_B+\mu_A-\mu_A e_{edcA})} & \frac{1-\boldsymbol{P}_{21}-\boldsymbol{P}_{24}}{\mu_A e_{dcA} r_{effA}+(\lambda_B+\mu_A-\mu_A e_{edcA})} & 0 & \frac{\lambda_B+\mu_A(1-e_{edcA})}{\lambda_B+\mu_A(1-e_{edcA})+\mu_A e_{dcA} r_{effA}} \\ \frac{\mu_B e_{dcB} r_{effB}}{\mu_B e_{dcB} r_{effB}+(\lambda_A+\mu_B-\mu_B e_{edcA})} & 0 & \frac{1-\boldsymbol{P}_{31}-\boldsymbol{P}_{34}}{\lambda_A+\mu_B(1-e_{edcB})+\mu_B e_{dcB} r_{effB}} & \frac{\lambda_A+\mu_B(1-e_{edcB})}{\lambda_A+\mu_B(1-e_{edcB})+\mu_B e_{dcB} r_{effB}} \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (7\text{-}15)$$

The transient probability matrix $\boldsymbol{Q}$ of the system depicted in Figure 7-1 is given by (7-16) based on (7-15).

$$\boldsymbol{Q} = \begin{bmatrix} \frac{1-\boldsymbol{P}_{12}-\boldsymbol{P}_{13}-\boldsymbol{P}_{14}}{(1-\beta)\lambda_A+(1-\beta)\lambda_B+\beta f(\lambda_A,\lambda_B)} & \frac{(1-\beta)\lambda_A}{(1-\beta)\lambda_A+(1-\beta)\lambda_B+\beta f(\lambda_A,\lambda_B)} & \frac{(1-\beta)\lambda_B}{(1-\beta)\lambda_A+(1-\beta)\lambda_B+\beta f(\lambda_A,\lambda_B)} \\ \frac{\mu_A e_{dcA} r_{effA}}{\mu_A e_{dcA} r_{effA}+(\lambda_B+\mu_A-\mu_A e_{edcA})} & \frac{1-\boldsymbol{P}_{21}-\boldsymbol{P}_{24}}{\mu_A e_{dcA} r_{effA}+(\lambda_B+\mu_A-\mu_A e_{edcA})} & 0 \\ \frac{\mu_B e_{dcB} r_{effB}}{\mu_B e_{dcB} r_{effB}+(\lambda_A+\mu_B-\mu_B e_{edcA})} & 0 & \frac{1-\boldsymbol{P}_{31}-\boldsymbol{P}_{34}}{\lambda_A+\mu_B(1-e_{edcB})+\mu_B e_{dcB} r_{effB}} \\ 0 & 0 & 0 \end{bmatrix} \quad (7\text{-}16)$$

Hence, the vector arrangement of the transient matrix $\boldsymbol{Q}$ is given by (7-17),

$$\mathrm{vec}\boldsymbol{Q} = \begin{bmatrix} \frac{1-\boldsymbol{P}_{12}-\boldsymbol{P}_{13}-\boldsymbol{P}_{14}}{(1-\beta)\lambda_A+(1-\beta)\lambda_B+\beta f(\lambda_A,\lambda_B)} \\ \frac{\mu_A e_{dcA} r_{effA}}{\mu_A e_{dcA} r_{effA}+(\lambda_B+\mu_A-\mu_A e_{edcA})} \\ \frac{\mu_B e_{dcB} r_{effB}}{\mu_B e_{dcB} r_{effB}+(\lambda_A+\mu_B-\mu_B e_{edcA})} \\ \frac{(1-\beta)\lambda_A}{(1-\beta)\lambda_A+(1-\beta)\lambda_B+\beta f(\lambda_A,\lambda_B)} \\ \frac{1-\boldsymbol{P}_{21}-\boldsymbol{P}_{24}}{\mu_A e_{dcA} r_{effA}+(\lambda_B+\mu_A-\mu_A e_{edcA})} \\ 0 \\ \frac{(1-\beta)\lambda_B}{(1-\beta)\lambda_A+(1-\beta)\lambda_B+\beta f(\lambda_A,\lambda_B)} \\ 0 \\ \frac{1-\boldsymbol{P}_{31}-\boldsymbol{P}_{34}}{\lambda_A+\mu_B(1-e_{edcB})+\mu_B e_{dcB} r_{effB}} \end{bmatrix} \quad (7\text{-}17)$$

In order to simplify the equations and the computation effort, the following expressions are defined:

$$P_{21}NM = \mu_A e_{dcA} r_{effA} \quad (7\text{-}18)$$

$$P_{21}DN = \mu_A e_{dcA} r_{effA} + (\lambda_B + \mu_A - \mu_A e_{edcA}) \quad (7\text{-}19)$$

$$P_{31}NM = \mu_B e_{dcB} r_{effB} \quad (7\text{-}20)$$

$$P_{31}DN = \mu_B e_{dcB} r_{effB} + (\lambda_A + \mu_B - \mu_B e_{edcB}) \tag{7-21}$$

$$Qdn = (1-\beta)\lambda_A + (1-\beta)\lambda_B + \beta f(\lambda_A, \lambda_B) \tag{7-22}$$

Delimitate vector $U$ to comprise the factors of interest to which the sensitivity and elasticity of the mean number of state transitions represented by the transient state matrix $\boldsymbol{Q}$ are analysed [104], [155], given by (7-23),

$$U = \begin{bmatrix} r_{effA} \\ r_{effB} \\ e_{dcA} \\ e_{dcB} \\ \beta \end{bmatrix} \tag{7-23}$$

Thus, the sensitivity of the transient state matrix to the elements of vector $U$ (i.e. $\frac{d\mathrm{vec}\,\boldsymbol{Q}}{dU^T}$) is given by (7-24) – (7-28),

$$\frac{d vec \boldsymbol{Q}}{dU_1} = \begin{bmatrix} 0 \\ \frac{\mu_A e_{dcA}(P_{21}DN - P_{21}NM)}{P_{21}DN^2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{7-24}$$

$$\frac{d vec \boldsymbol{Q}}{dU_2} = \begin{bmatrix} 0 \\ 0 \\ \frac{\mu_B e_{dcB}(P_{31}DN - P_{31}NM)}{P_{31}DN^2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{7-25}$$

$$\frac{d\mathrm{vec}\boldsymbol{Q}}{dU_3} = \begin{bmatrix} 0 \\ \frac{\mu_A(P_{21}DNr_{effA} - P_{21}NM(r_{effA}-1))}{P_{21}DN^2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{7-26}$$

$$\frac{d\mathrm{vec}\boldsymbol{Q}}{dU_4} = \begin{bmatrix} 0 \\ 0 \\ \frac{\mu_B(P_{31}DNr_{effB} - P_{31}NM(r_{effB}-1))}{P_{31}DN^2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{7-27}$$

$$\frac{d\mathrm{vec}\boldsymbol{Q}}{dU_5} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{-\lambda_A Q_{dn} + \lambda_A(1-\beta)(\lambda_A + \lambda_B - f(\lambda_A,\lambda_B)}{{Q_{dn}}^2} \\ 0 \\ 0 \\ \frac{-\lambda_B Q_{dn} + \lambda_B(1-\beta)(\lambda_A + \lambda_B - f(\lambda_A,\lambda_B)}{{Q_{dn}}^2} \\ 0 \\ 0 \end{bmatrix} \tag{7-28}$$

The complete matrix for the sensitivity of the transient matrix $\boldsymbol{Q}$ to the elements of vector $U$ comprising (7-24) to (7-28) is given by (7-29). Substituting (7-29) into (7-13) and (7-14) enables determining the system's reliability performance based on sensitivity and elasticity to CCFs. Therefore, (7-24) to (7-28) represent the sensitivity of the transient matrix $\boldsymbol{Q}$ to the individual factors of interest contained in $U$. The preliminaries of matrix calculus methods used in this chapter are discussed in Chapter 3 [15], [16], [104]. The following section presents case studies, results, and a discussion of the system's sensitivity and elasticity mean state transitions to repair efficiency, diagnostic coverage, and CCF factors.

$$\frac{dvec\boldsymbol{Q}}{dU}=\begin{bmatrix} 0 & 0 & 0 \\ \frac{\mu_A e_{dcA}(P_{21}DN-P_{21}NM)}{P_{21}DN^2} & 0 & \frac{\mu_A(P_{21}DNr_{effA}-P_{21}NM(r_{effA}-1))}{P_{21}DN^2} \\ 0 & \frac{\mu_B e_{dcB}(P_{31}DN-P_{31}NM)}{P_{31}DN^2} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \cdots \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ \frac{\mu_B(P_{31}DNr_{effB}-P_{31}NM(r_{effB}-1))}{P_{31}DN^2} & 0 \\ 0 & \frac{-\lambda_A Q_{dn}+\lambda_A(1-\beta)(\lambda_A+\lambda_B-f(\lambda_A,\lambda_B)}{{Q_{dn}}^2} \\ 0 & 0 \\ 0 & 0 \\ 0 & \frac{-\lambda_B Q_{dn}+\lambda_B(1-\beta)(\lambda_A+\lambda_B-f(\lambda_A,\lambda_B)}{{Q_{dn}}^2} \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \quad (7\text{-}29)$$

## 7.5 Results and discussion

The system diagnostic coverage levels based on ISO 13849-1, as presented in Chapter 4 and Chapter 5, form the basis of the case studies. Table 4-4 presents the system diagnostic coverage levels according to their denotation [118]–[120].

The following assumptions are made to gain insights into the behaviour of the system while easing the analysis effort:

a) Subsystems A and B are of the same technology. Hence, the subsystems have the same diagnostic coverage levels; this assumption is relaxed later.
b) The resources used to support and maintain subsystems A and B are not the same. Hence, the subsystem's repair efficiencies are not identical. The repair efficiency is 90% for subsystem A, whereas that of subsystem B is 50%. The individual repair efficiencies are chosen to enable the system's responsiveness to be analysed at different repair levels. This assumption is maintained in all study cases presented in this chapter.
c) Subsystems A and B are assumed to be entirely independent of each other, making the CCF factor level zero. This assumption is relaxed at a later stage.
d) The system is fully functional at the beginning of the simulation.

The choice of repair efficiency levels is informed by the eigenvalue analysis results and is meant to observe the system response at different repair factors levels. This approach also demonstrates that the proposed method can compute individual repair efficiencies. Although the subsystems are assumed to have the same diagnostic coverage by being of the same technology, individual diagnostic coverage factors can be computed if required; this aspect is demonstrated later in the case studies. The system state transitions are depicted by $S_{xy}$, where $x$ represent the initial condition of the system and $y$ is the state into which the system transitioned. Full initial system functionality is represented by state S-1 and depicted by $S_{1y}$ in the results presented in this chapter.

### 7.5.1 High diagnostic coverage

In this case study, the individual subsystems' diagnostic coverage factors are assumed to be 99%. The analysis presented below relates to a fully functional system initial condition depicted by $S_{1y}$. Figure 7-2(a) depicts the sensitivity of the system to the repair efficiency factors. It can be observed that the system is more sensitive to the repair efficiency of subsystem B, which is 50% compared to that of subsystem A at 90%. The incremental change in $r_{effB}$ causes the mean system state transition to increase by 76, 42 and 34, respectively; of which the total is the sum of transitions in states $S_{1y}$. Thus, it is more beneficial to increase

the repair efficiency of subsystem B than that of subsystem A since it could only improve the state transitions by 29, 16 and 13.

In addition, it is noticeable that the mean system state transitions are less impacted by the increase of repair efficiency factors of magnitudes closer to 100% because the magnitudes of the eigenvalues remain relatively constant closer to 100%. Hence, subsystem B's repair efficiency would have a high impact on the system eigenvalues' magnitudes. The high number of system state transitions into state S-2 compared to S-3 is expected since subsystem A has a higher failure rate than subsystem B and a higher repair efficiency factor considering that the subsystems' diagnostic coverages are identical.

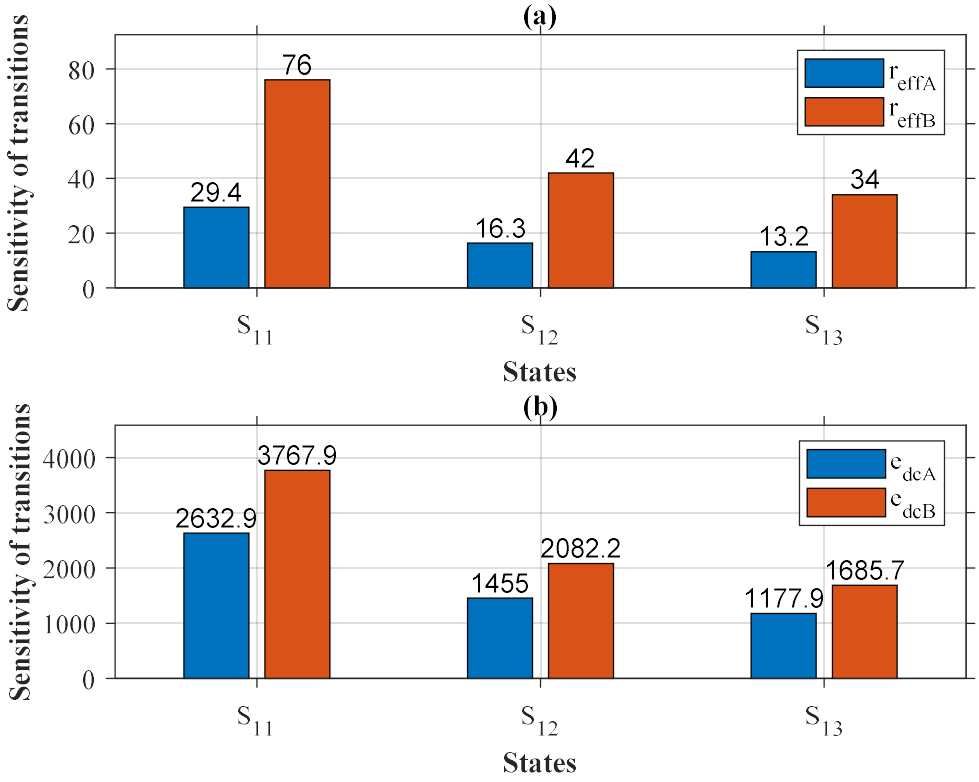


Figure 7-2: Sensitivity analysis of repair and diagnostic coverage factors (99%)

In contrast, the diagnostic coverage factors significantly impact the mean system state transitions as observed from the system's sensitivity depicted in Figure 7-2(b) to repair efficiency factors. The incremental change in $e_{edcB}$ causes the mean system state transitions to increase by 3768, 2082 and 1686, respectively; of which the total is the sum of transitions into states $S_{1y}$. Again, the system's sensitivity to the factors indicates that diagnostic coverage is a critical factor in determining system performance.

Figure 7-3 depicts the elasticities of the system to both the repair and diagnostic coverage factors. The magnitude of elasticities of the repair efficiency factors $r_{effA}$ and $r_{effB}$ are inelastic, as depicted in Figure 7-3(a). It can be observed that improving the repair efficiency

of subsystem B is proportionally beneficial than improving that of subsystem A since the elasticity of the mean system state transition is 0.6 for subsystem B, whereas that of subsystem A is 0.4.

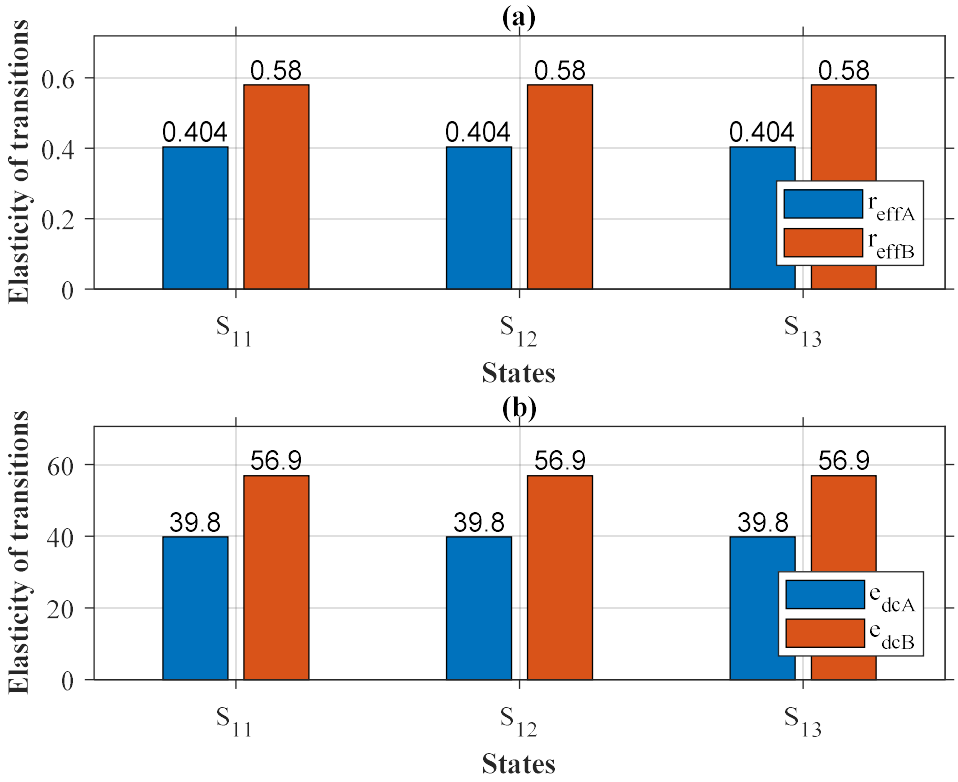


Figure 7-3: Elasticity analysis of repair and diagnostic coverage factors (99%)

Figure 7-3(b) depicts the elasticity of the system to the diagnostic coverage factors. The diagnostic coverage factors are perfectly elastic at around 40 for subsystem A and under 60 for subsystem B. Thus, it is again beneficial to improve subsystem B's diagnostic coverage factor because of its low repair efficiency factor. In context, the system's mean state transitions can be improved by focusing on subsystem B's performance because it is clear that the diagnostic coverage is the most critical factor to improve, and then the system's low repair efficiencies.

### 7.5.2 Medium diagnostic coverage

The diagnostic coverage factors of the individual subsystems are assumed to be 90% in this case study. As before, the analysis presented below is for a fully functional system initial condition depicted by $S_{1y}$. Figure 7-4(a) depicts the sensitivity of the system to the repair efficiency factors. The system is more sensitive to subsystem B's repair efficiency, which is lower by 40% than that of subsystem A. The incremental change in $r_{effB}$ causes the mean system state transition to increase by 7, 4 and 3, respectively; of which the total is the sum of

transitions in states $S_{1y}$. The individual subsystem failure rates maintain their influence regardless of the reduced system diagnostic coverage at 90%. Nevertheless, the system's sensitivity to the repair efficiency factors has significantly reduced, which signifies the level of impact imposed by the system's diagnostic coverage.

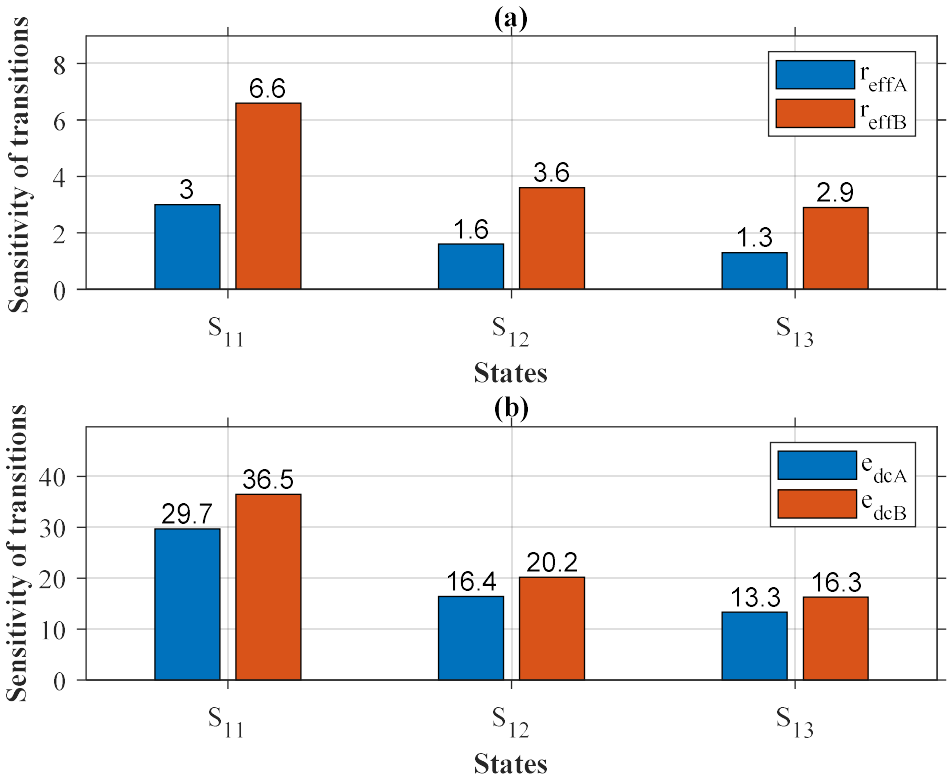


Figure 7-4: Sensitivity analysis of repair and diagnostic coverage factors (90%)

The incremental change in $e_{edcA}$ causes the mean system state transitions to increase by only 30, 16 and 13, respectively; which is the sum of transitions in states $S_{1y}$. Contrasting the incremental change of $e_{edcA}$, the incremental change of $e_{edcB}$ causes the mean system state transitions to increase by only 37, 20 and 16, respectively. The difference in the subsystems' repair efficiencies and their failure rates causes the difference in the two diagnostic coverage factors' effectiveness. Again, the system's sensitivity to the factors indicates that diagnostic coverage is a critical factor in determining system performance.

Figure 7-5 depicts the elasticities of the system to both the repair and diagnostic coverage factors. The magnitude of the elasticity of both the repair factors ($r_{effA}$ and $r_{effB}$) indicate that the factors are inelastic, as depicted in Figure 7-5(a). Once again, improving the repair efficiency of subsystem B is proportionally beneficial than improving that of subsystem A since the elasticity of the mean system state transition is 0.5 for subsystem B, whereas that of subsystem A is 0.4. Figure 7-5(b) depicts the elasticity of the system to the diagnostic coverage factors. The diagnostic coverage factors are perfectly elastic at 4 for subsystem A and 5 for

subsystem B. Thus, it is again beneficial to improve subsystem B's diagnostic coverage factor because of its low repair efficiency factor.

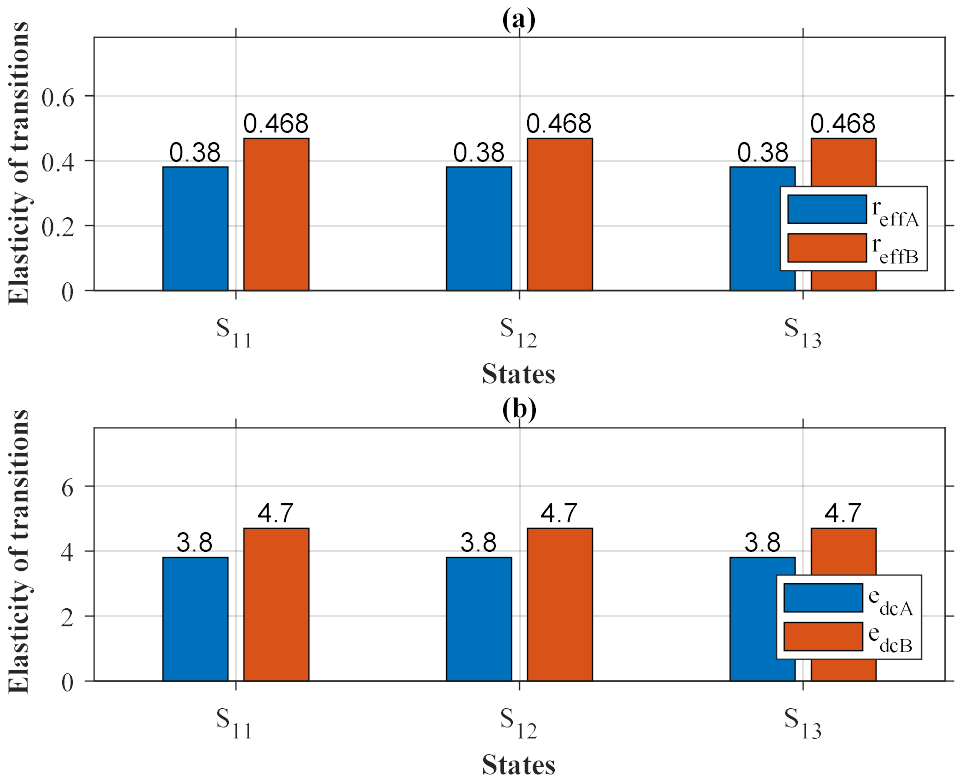


Figure 7-5: Elasticity analysis of repair and diagnostic coverage factors (90%)

Further, the incremental effectiveness of diagnostic coverage factors had significantly reduced compared to when the system was operating at 99% for both the subsystems. Hence, the mean state transitions of the system can be improved by focusing on the performance of subsystem B because it is clear that the diagnostic coverage is the most critical factor to improve, after which the low repair efficiencies in the system can be considered to improve the performance of the system further.

### 7.5.3 Low diagnostic coverage

This case study assumes that the diagnostic coverage factor of the individual subsystems is 60%. As in the two previous case studies, the analysis presented below is for a fully functional system initial condition depicted by $S_{1y}$. Figure 7-6(a) depicts the sensitivity of the system to the repair efficiency factors. In contrast to the high and medium diagnostic coverage level case studies, the incremental change in repair efficiency factors does not affect the mean system state transitions. Further, even though subsystem A has a higher repair efficiency than subsystem B, the responsiveness of the two subsystems is identical at just under magnitude one for $S_{11}$ and $S_{12}$. This observation suggests that the level of unidentified system faults is

very high for the repairs to be significant regardless of repair efficiency level. Hence the increase of the repair efficiency factors is not useful, and therefore not beneficial.

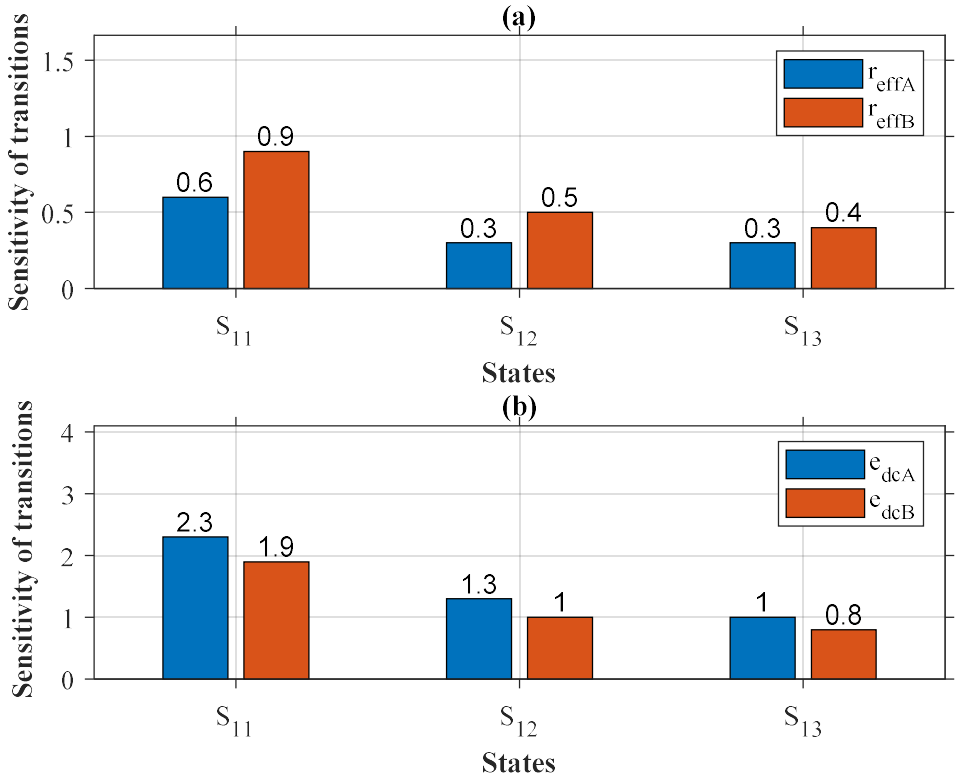


Figure 7-6: Sensitivity analysis of repair and diagnostic coverage factors (60%)

The incremental change in $e_{edcA}$ causes the mean system state transitions to increase by only 2, 1 and 0.8, respectively; of which the total is the sum of transitions in states $S_{1y}$ as before. Similarly, the incremental change of $e_{edcB}$ causes the mean system state transitions to increase by only 2, 1 and 1, respectively. The subsystems' behaviour is similar to the subsystems' low diagnostic coverage, which accounts for a high level of unidentified system faults. Thus, the diagnostic coverages of the subsystems significantly influence the performance of the system.

Figure 7-7 depicts the elasticities of the system to both the repair and diagnostic coverage factors. As before, the elasticity magnitude of both the repair factors ($r_{effA}$ and $r_{effB}$) indicate that the factors are inelastic, as depicted in Figure 7-7(a). In contrast to the two previous case studies, improving the repair efficiency of subsystem A is proportionally beneficial than improving that of subsystem B since the elasticity of the mean system state transition is 0.3 for subsystem A, whereas that of subsystem B is 0.2. The change in system behaviour is attributed to the higher repair efficiency of subsystem A than that of subsystem B, given the subsystems' low diagnostic coverages.

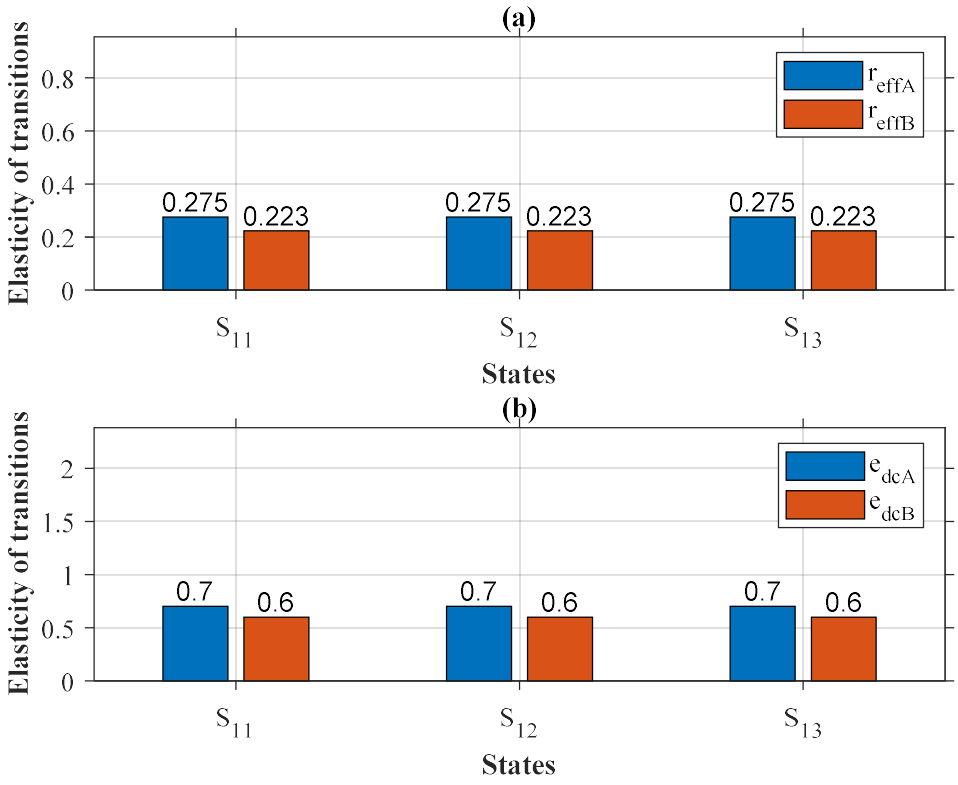


Figure 7-7: Elasticity analysis of repair and diagnostic coverage factors (60%)

Figure 7-7(b) depicts the elasticity of the system to the diagnostic coverage factors. The diagnostic coverage factors are no longer perfectly elastic for subsystem A and subsystem B. Consequently, it is equally beneficial to improve the diagnostic coverage factors of both subsystems. The much-reduced effectiveness of the factors is attributed to the much lower diagnostic coverage of 60% on the individual subsystems.

### 7.5.4 Mixed diagnostic coverages

This case study relaxes the assumption made earlier where the subsystem's diagnostic coverages were considered identical and investigate the system's responsiveness when the subsystems have different diagnostic coverages. The following assumptions remain unchanged:

a) The resources used to support and maintain subsystems A and B are not the same. However, subsystem A's repair efficiency is assumed to be 95%, while subsystem B's repair efficiency is considered 70%. The increase in the subsystems' repair efficiency factors is meant to investigate the system at different repairs levels than the three case studies above.

b) Subsystems A and B are assumed to be entirely independent of each other, making the CCF factor level zero as in the previous case studies. This assumption is relaxed in the following case study.

c) The system is fully functional at the beginning of the simulation.

Table 7-1 presents the diagnostic coverage levels of the scenarios considered in this case study. The selection of diagnostic coverage factors is informed by the previous case studies results and is intended to observe the system's response at different subsystem diagnostic capabilities levels. The various factors also demonstrate that the method used in this research can compute different repair efficiency factors and diagnostic coverage levels.

Table 7-1: Denotation of subsystem diagnostic coverage levels

| Scenario | C-1 | C-2 | C-3 |
|---|---|---|---|
| Subsystem A diagnostic coverage ($e_{dcA}$) | 90% | 90% | 60% |
| Subsystem B diagnostic coverage ($e_{dcB}$) | 99% | 60% | 60% |

#### 7.5.4.1 Scenario C-1

In this scenario, the individual subsystems' diagnostic coverage factors are assumed to be 90% and 99% for subsystem A and subsystem B, respectively. The system's sensitivity to the repair efficiency factors is depicted in Figure 7-8(a). It is noticeable that the system is more sensitive to the repair efficiency of subsystem A, which has a lower system diagnostic coverage compared to subsystem B, even though the repair efficiency of subsystem A is 95%. The incremental change of subsystem A repair efficiency ($r_{effA}$) causes the mean system state transition to increase by 13, 7 and 6, for transitions into states S-1, S-2 and S-3, respectively; of which the total is the sum of transitions in states $S_{1y}$. Hence, it is more beneficial to increase the repair efficiency of subsystem A than that of subsystem B since it could only improve the state transitions by 2, 1 and 1, for transitions into states S-1, S-2 and S-3, respectively. The high number of system state transitions into state S-2 compared to S-3 is expected since subsystem A has a higher failure rate than subsystem B and a higher repair efficiency factor considering that their diagnostic capabilities are relatively high.

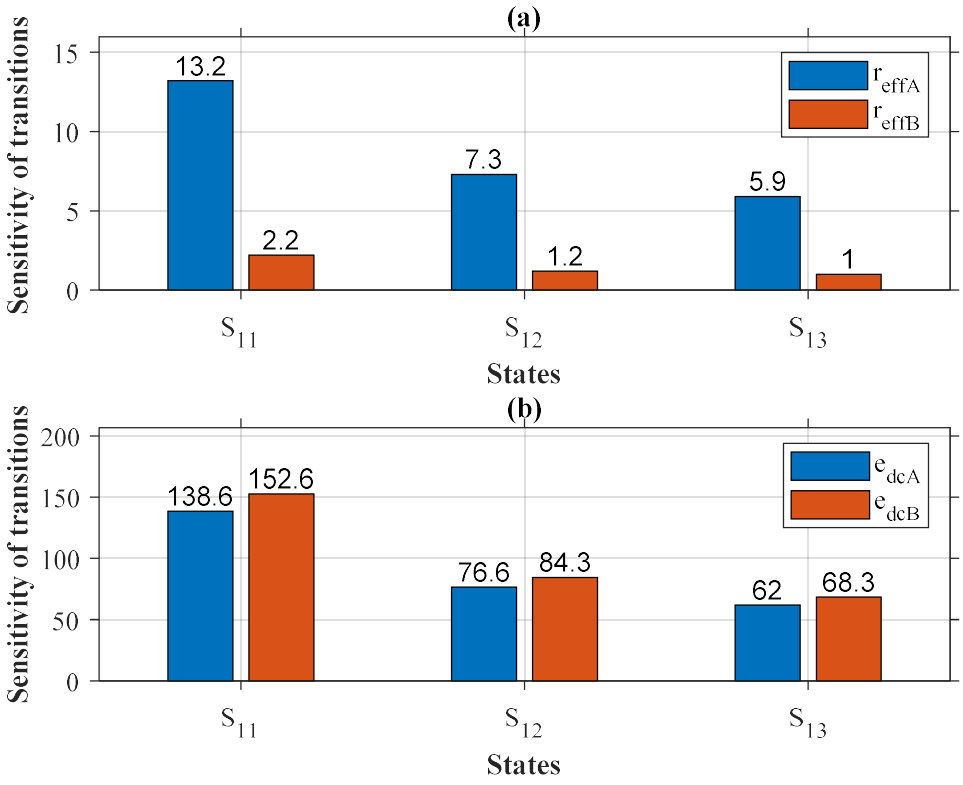


Figure 7-8: Sensitivity analysis of repair and diagnostic coverage factors of case study C-1

In contrast, the diagnostic coverage factors significantly impact the mean system state transitions, as depicted in Figure 7-8(b). The incremental change in diagnostic coverage of the subsystem ($e_{edcB}$) causes the mean system state transitions to increase by 153, 84 and 68 transitions into states S-1, S-2 and S-3, respectively, which is the sum of transitions given that the initial state is S-1. The system's sensitivity to the factors indicates that diagnostic coverage is a critical factor in determining system reliability performance.

Figure 7-9 depicts the system state transitions' elasticities to repair efficiency and system diagnostic coverage factors. The elasticity magnitudes of the repair efficiency factors $r_{effA}$ and $r_{effB}$ are inelastic, as depicted in Figure 7-9(a). It is noticeable that improving the repair efficiency of subsystem A is beneficial than that of subsystem B since the elasticity of the mean system state transition is 0.8 for subsystem A, whereas that of subsystem B is 0.1.

Figure 7-9(b) depicts the elasticity of the system to the diagnostic coverage factors. The diagnostic coverage factors are perfectly elastic at around 8 for subsystem A and 9.7 for subsystem B. Thus, it is beneficial to increase the diagnostic coverage factor of subsystem B because of its low repair efficiency factor. In context, the system's reliability can be improved by focusing on subsystem B's performance because it has the most elastic factor with the highest overall incremental system state transitions.

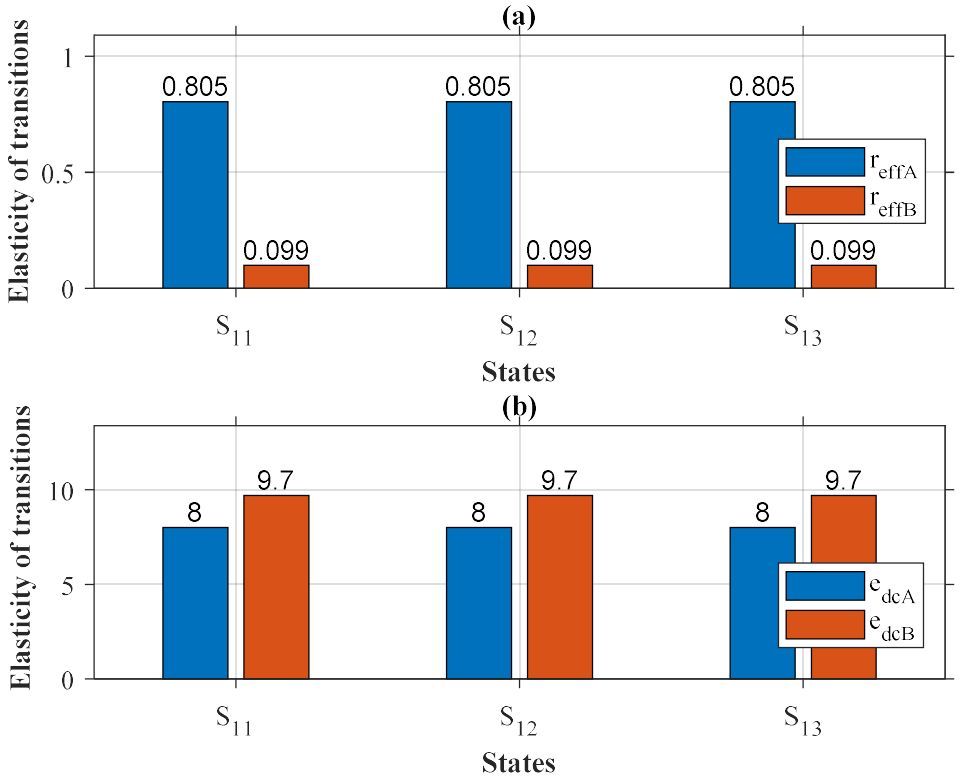


Figure 7-9: Elasticity analysis of repair and diagnostic coverage factors of case study C-1

### 7.5.4.2 Scenario C-2

The individual subsystem A and subsystem B's diagnostic coverage factors are assumed to be 90% and 60%, respectively. Figure 7-10(a) depicts the sensitivity of the system reliability to the repair efficiency factors. It is noticeable that the system is more sensitive to subsystem B's repair efficiency, which is lower by 25% than that of subsystem A at 95%. The incremental change in repair efficiency of subsystem B ($r_{effB}$) causes the mean system state transition into states S-1, S-2 and S-3 to increase by 2, 1 and 1, respectively, which is the sum of states transitions given that the initial system state is S-1. Hence, the individual subsystem failure rates maintain their influence regardless of the reduced system diagnostic coverage of 60% for subsystem B. Nevertheless, the system's sensitivity to the system repair efficiency factors has significantly reduced, which signifies the level of impact imposed by the system's diagnostic coverage.

The incremental change in subsystem A diagnostic coverage ($e_{edcA}$) causes the mean system state transitions to increase by 7, 4 and 3 in states S-1, S-2 and S-3. Contrasting the incremental change of subsystem A diagnostic coverage ($e_{edcA}$), the incremental change of subsystem B diagnostic coverage ($e_{edcB}$) causes the mean system state transitions to increase by 6, 3 and 3, respectively. The difference in the subsystems' repair efficiencies and their failure rates causes the difference in the two diagnostic coverage factors' effectiveness. Again,

the system's sensitivity to the factors indicates that diagnostic coverage is the most critical factor in determining system performance.

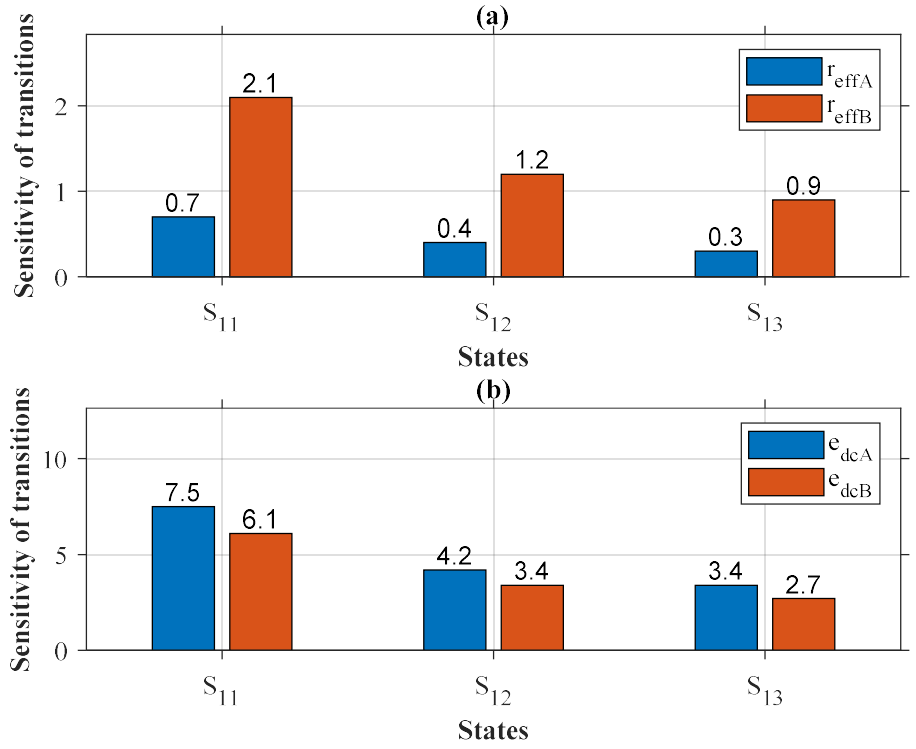


Figure 7-10: Sensitivity analysis of repair and diagnostic coverage factors of case study C-2

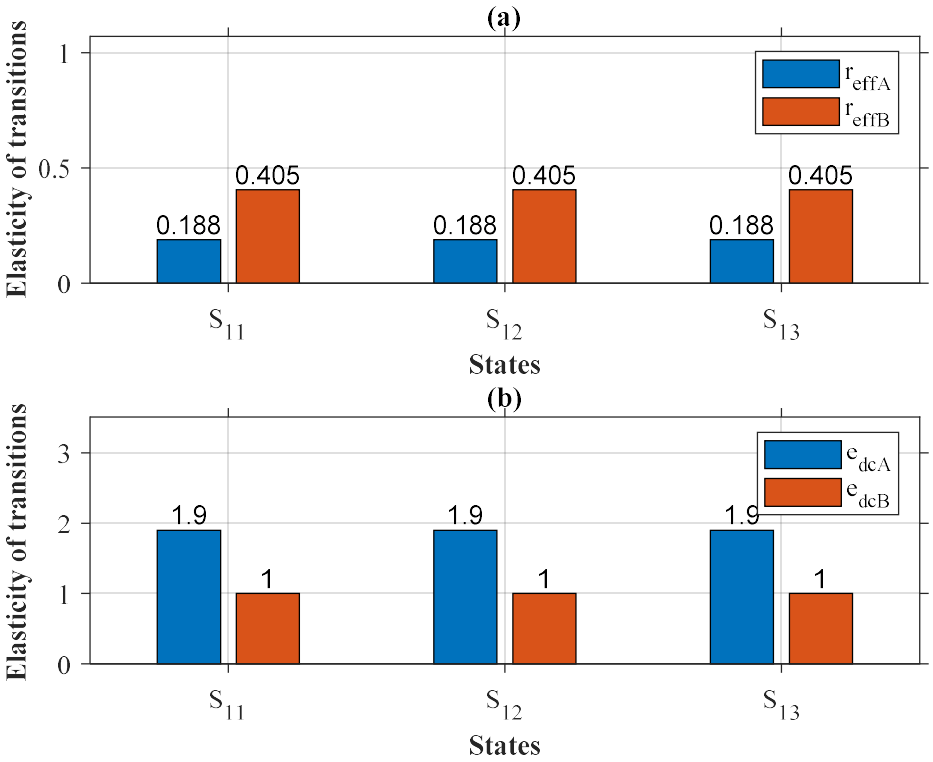


Figure 7-11: Elasticity analysis of repair and diagnostic coverage factors of case study C-2

Figure 7-11 depicts the system's elasticities to both the repair efficiency and diagnostic coverage factors. The magnitude of the elasticity of both the repair efficiency factors $r_{effA}$ and $r_{effB}$ indicate that the factors are inelastic, as depicted in Figure 7-11(a). Even so, improving the repair efficiency of subsystem B is proportionally beneficial than that of subsystem A since the elasticity of the mean system state transition is 0.4 for subsystem B, whereas that of subsystem A is 0.2. Figure 7-11(b) depicts the elasticity of the system to the diagnostic coverage factors. The diagnostic coverage factors are elastic at 2, 3, and 2 transitions for states S-1, S-2 and S-3 in subsystem A, respectively and 1, 1 and 2 for states S-1, S-2 and S-3 for subsystem B. Thus, it is again beneficial to improve the diagnostic coverage factor of subsystem A because of its high repair efficiency factor.

#### 7.5.4.3 Scenario C-3

This case study assumes that the diagnostic coverage factor of the individual subsystems is 60%. This scenario is similar to the low diagnostic coverage case study presented earlier. However, the individual subsystem's repair efficiencies have been increased to investigate the impact of high repair efficiency at low system diagnostic coverage. Figure 7-12(a) depicts the sensitivity of the system to the repair efficiency factors. In contrast to C-1 and C-2 case studies' diagnostic coverage levels, the incremental change in repair efficiency factors does not affect the mean system state transitions.

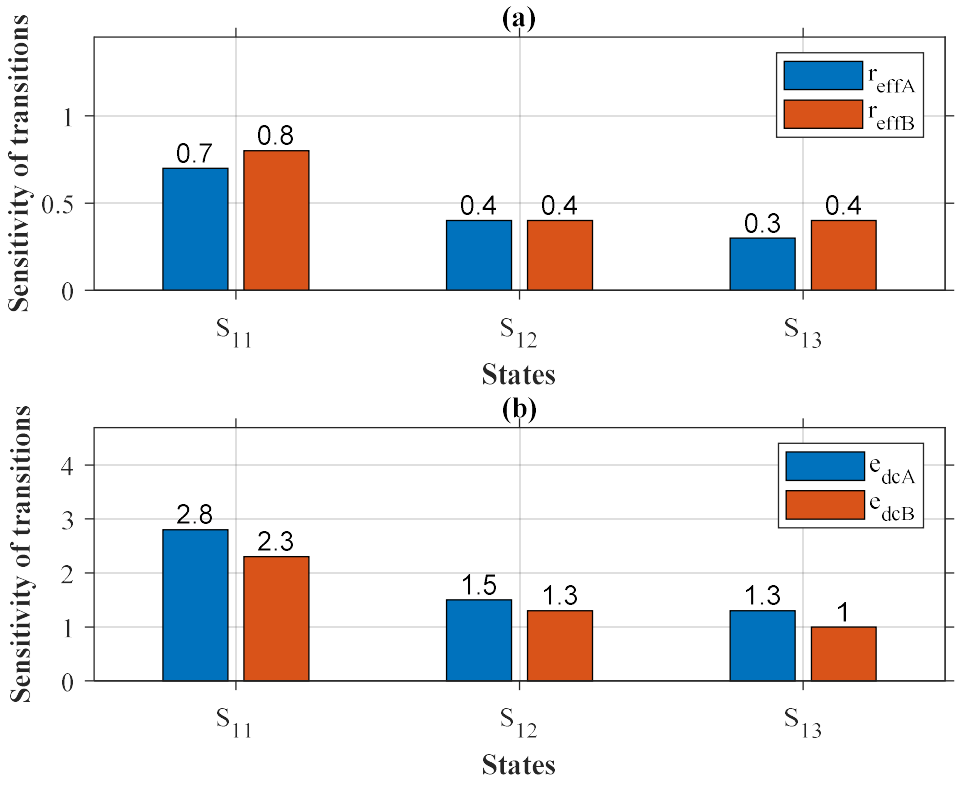


Figure 7-12: Sensitivity analysis of repair and diagnostic coverage factors of case study C-3

Moreover, even though subsystem A has a higher repair efficiency than subsystem B, the two subsystems' responsiveness is relatively identical because of the low system diagnostic coverage level. This observation suggests that the unidentified system faults are very high for the repairs to be significant regardless of repair efficiency level. Hence the increase of the repair efficiency factors is not useful, and therefore not beneficial.

The incremental change in subsystem A diagnostic coverage causes the mean system state transitions to increase by only 3, 1 and 1, respectively. In contrast, the incremental change of subsystem B diagnostic coverage causes the mean system state transitions to increase by only 2, 1 and 1, respectively. The similarity in the subsystems' response is attributed to the subsystems' low diagnostic coverage, which accounts for a high level of unidentified system faults. Hence, the diagnostic coverages of the subsystems highly influence the performance of the system. The system's elasticities to both the repair and diagnostic coverage factors are depicted in Figure 7-13.

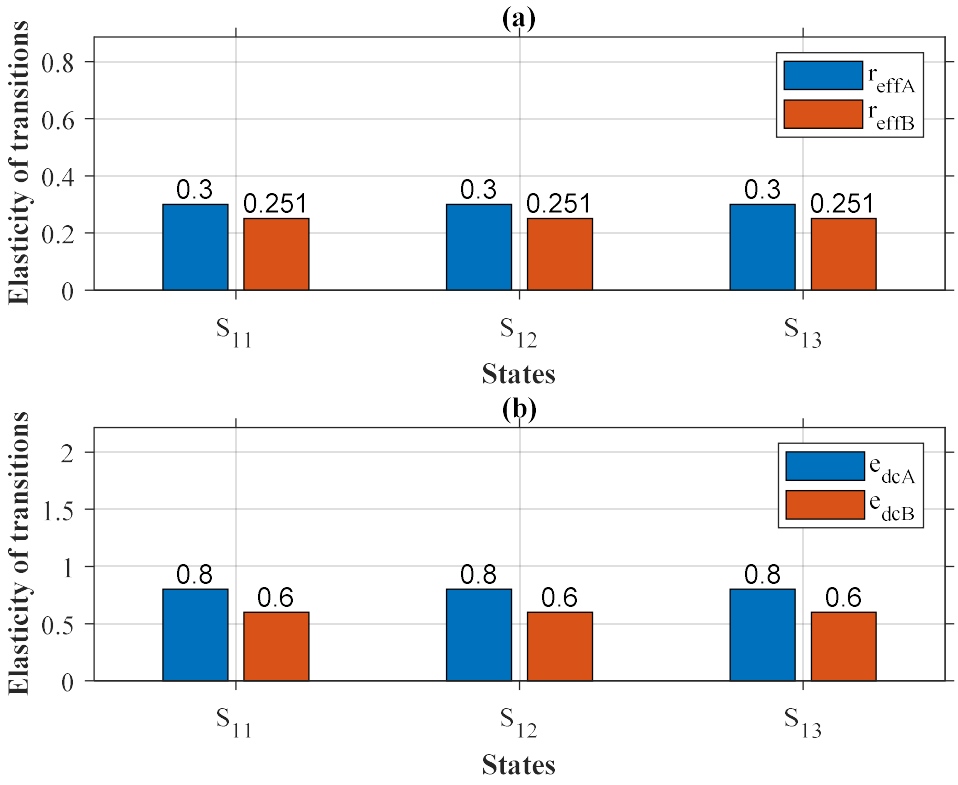


Figure 7-13: Elasticity analysis of repair and diagnostic coverage factors of case study C-3

The magnitude of the elasticity of both the repair factors of subsystems A and B ($r_{effA}$ and $r_{effB}$) indicate that the factors are inelastic, as depicted in Figure 7-13(a). Improving the repair efficiency of subsystem A yields similar results as that of subsystem B since the elasticities of the mean system state transition for subsystem A are relatively equal to that of subsystem B, given the equally low diagnostic coverages of the subsystems at 60%.

Figure 7-13(b) depicts the elasticity of the system to the diagnostic coverage factors. The diagnostic coverage factors are no longer elastic for both subsystem A and subsystem B. Consequently, it is equally beneficial to improve the diagnostic coverage factors of both subsystems. The much-reduced effectiveness of the factors is attributed to the much-lower diagnostic coverage of 60% on the individual subsystems.

### 7.5.5 Sensitivity and elasticity to common causes of failure

This case study relaxes the assumption made earlier where the subsystems were considered entirely independent from each other. The following assumptions are made to ease the results analysis effort required:

a) Subsystems A and B are of the same technology. Hence the subsystems have the same diagnostic coverage levels.

b) The resources used to support and maintain subsystems A and B are the same. Subsystem A and B's repair efficiencies are assumed to be 95%.

c) The system is fully functional at the beginning of the simulation.

#### 7.5.5.1 High diagnostic coverage

Figure 7-14 depicts the system's responsiveness to CCFs based on sensitivity and elasticity when the coverage is 99% for β = 0.1 and β = 0.5. It can be observed that the system state mean transitions into state S-1 is the most sensitive at -139 in Figure 7-14(a) when the level of CCF level is 10%.

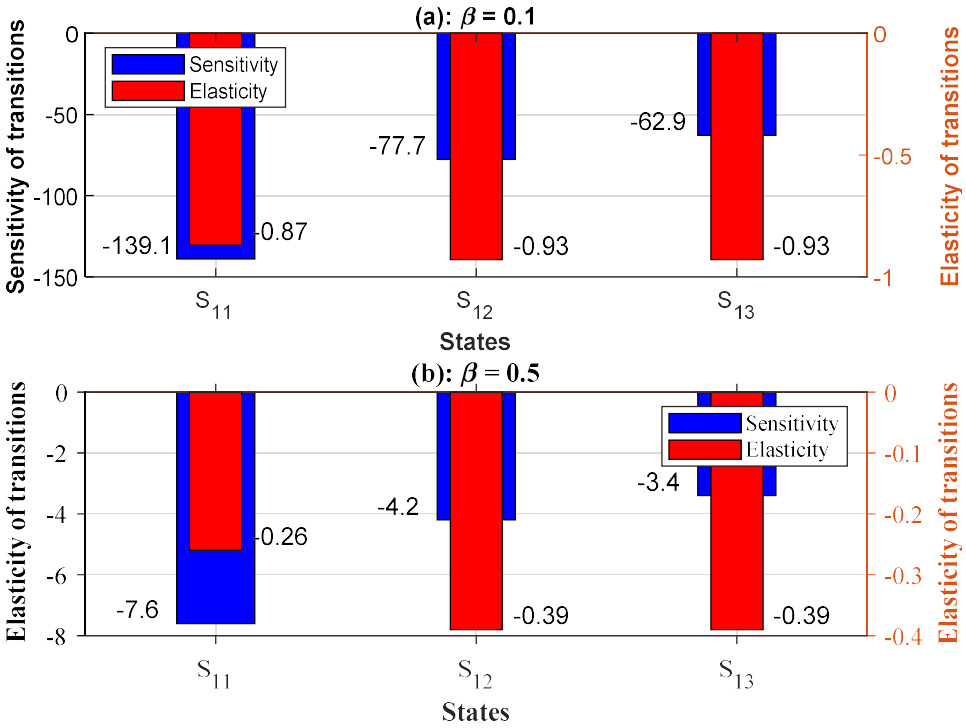


Figure 7-14: Sensitivity and elasticity of system to CCFs - High diagnostic coverage

The negative magnitude indicates that the incremental change in the CCF level causes the system's mean state transitions to decrease, which implies that the system's reliability performance decreases. It is also noticeable that state S-1 is the most sensitive when β = 0.5, as depicted in Figure 7-14(b). However, the magnitude of the state transition sensitivity has reduced to -7.6. Although state S-1 has the highest sensitivity, its elasticity is the least than moving into S-2 and S-3. This observation is similar for the two system CCF levels. Nevertheless, the results depicted in Figure 7-14 confirms that the system performance is most sensitive to low β-factor levels when the diagnostic coverage is high.

#### 7.5.5.2 Medium diagnostic coverage

Figure 7-15 depicts the system's responsiveness to CCFs based on sensitivity and elasticity when the coverage is 90% for β = 0.1 and β = 0.5. It can be observed that the system state mean transitions into state S-1 is the most sensitive at -21.5 in Figure 7-15(a) when β = 0.1. As before, the negative magnitude indicates that the incremental change in the CCF level causes the mean system state transitions to decrease, which implies that the system's reliability performance decreases when the level of CCFs increases. Similarly to the previous scenario, it is noticeable that state S-1 remains sensitive when β = 0.5 even though the diagnostic coverage has reduced, as depicted in Figure 7-15(b). However, the magnitude of the state transition sensitivity has reduced to -4.9.

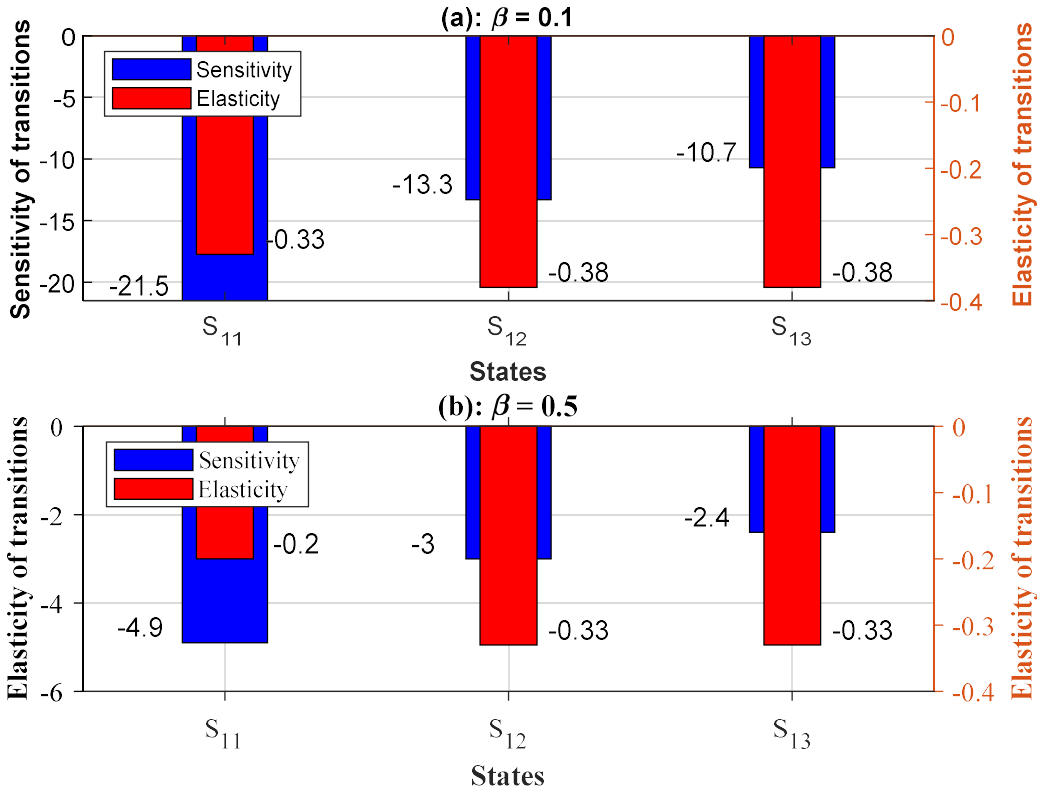


Figure 7-15: Sensitivity and elasticity of system to CCFs - Medium diagnostic coverage

The elasticity of state S-1 transitions is the least than moving into S-2 and S-3. This observation is similar for the two CCF levels at β = 0.1 and β = 0.5. The results confirm that the system performance is most sensitive to low β-factor levels when the diagnostic coverage is medium.

#### 7.5.5.3 Low diagnostic coverage

Figure 7-16 depicts the system's responsiveness to CCFs based on sensitivity and elasticity when the coverage is 60% for β = 0.1 and β = 0.5. The system state mean transitions into state S-1 is the most sensitive at -1.7 when β = 0.1, as depicted in Figure 7-16(a). As before, the system's reliability performance decreases when the level of CCFs increases. Similarly, to the two previous scenarios, it is noticeable that state S-1 remains sensitive when β = 0.5 even though the diagnostic coverage has reduced further to 60%, as depicted in Figure 7-16(b).

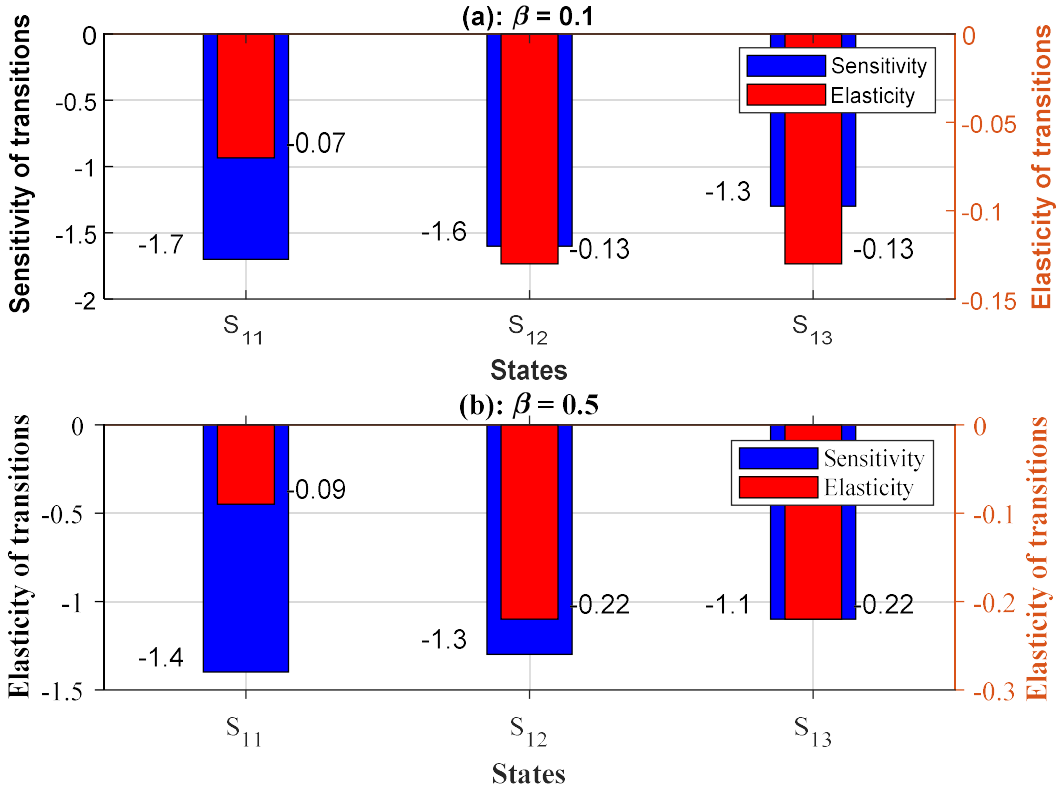


Figure 7-16: Sensitivity and elasticity of system to CCFs - Low diagnostic coverage

However, the magnitude of the state transition sensitivity has marginally reduced to -1.4. The state S-1 transitions' elasticity is consistently the least compared to moving into S-2 and S-3. This observation is the same for the two CCF levels at β = 0.1 and β = 0.5. Once again, the results confirm that the system performance is most sensitive to low β-factor levels.

## 7.6 Chapter conclusion

The system's responsiveness to incremental repair efficiency and diagnostic coverage factors can be precisely determined using sensitivity and elasticity analysis, as demonstrated in the case studies. This approach enables the effect of the individual factors on the system reliability to be investigated based on the mean system state transitions, enabling the system's performance to be optimised at the subsystem level. The case studies results demonstrate the significance of accurate system fault diagnostics and repairs to achieve high system reliability performance for mission-critical systems in power distribution centres. Notably, the results show that the elasticity of the system reliability is inelastic to the repair efficiency factors, which indicates that the benefits as a result of increasing the repair factors are not significant for a given level of system performance; while the diagnostic coverage of the system is the most critical of the two factors with higher elasticity as the factor approaches 100%. Moreover, the increase of repair efficiency in small magnitudes proved ineffective at low system diagnostic coverage level due to the high number of unidentified faults in the system. Therefore, the results indicate that system performance is very dependent on the diagnostic coverage of the individual subsystems compared to their repair efficiencies, particularly for high diagnostic coverages at 99% and 90% based on ISO 13849-1 for subsystems A and B in a ‘one-out-of-two’ system configuration.

The case studies results also demonstrated the importance of maintaining a low level of CCFs, where the most impact on system reliability is observed. The characteristic impact of CCFs is relatively similar for a given level of system diagnostic coverage and repair efficiency demonstrated by the case studies results. Nevertheless, it is concluded that the severity of CCFs highly depends on system diagnostic coverage level than the repair efficiency, even though both factors impact the system's overall performance. Hence, the impact of CCFs must be considered in developing reliability models of mission-critical systems to determine the system's performance accurately. Hence, the results indicate that emphasis should be more on the system diagnostic coverage because it is embedded in the system design itself that cannot easily be changed later, considering that it would be too expensive and require plant downtime for implementation and testing as well.

# CHAPTER 8

## SUMMARY OF CONCLUSIONS AND FUTURE RECOMMENDED RESEARCH

This chapter presents a summary of research findings, conclusions and recommendations for future research work.

### 8.1 Summary of conclusions

The research work presented in the thesis investigated the methods and considerations of evaluating the reliability performance of IEC 61850 based SCN, the basis for parameter optimisation and its stability for executing safety-related mission-critical functions based on the IEC 61508 standard for safety-related systems. The research work also investigated the responsiveness of the SCN reliability performance to repair factors, diagnostic coverage and common causes of failure to enable parameter selection to attain the desired system performance. Hence, the scope of the work presented in the thesis fulfils the set objectives of the research. The reliability of a repairable multi-channel IEC 61850 based SCN is modelled using structure-function and Markov process. Imperfect repair factors were integrated into the quantitative analysis model using Systems Thinking, enabling a holism approach to studying the system's behaviour. Thereafter, a novel eigenvalue analysis method based on Markov partitions and symbolic dynamics in the context of linear dynamical systems was used to investigate the impact of imperfect repairs on the system's reliability based on the number of mean state transitions and dynamical behaviour. The eigenvalue method was then advanced by a complimentary analysis technique based on absorbing Markov Chain and matrix calculus methods to determine the system's responsiveness to repair factors.

The impact and significance of both the system diagnostic coverage and repair efficiency on the system's reliability performance were demonstrated considering IEC 61850 based SCN interfacing to IEC 61508 system in a power distribution centre, where the case studies were based on ISO 13849-1 diagnostic coverage levels, the standard for Safety of Machinery. The investigation outcome shows that the Markov process and mathematical expectation can be used to study the reliability and availability of systems with imperfect repairs (viz. repair efficiency and diagnostic coverage). The studies results show that combinatorial analysis methods do not produce realistic results for multi-channel systems such as the repairable IEC 61850 SCN, mainly used for implementing mission-critical safety-related protection systems in power distribution centres within industrial facilities. Their lack of comprehensiveness is due to their failure to consider the low quality of repairs caused by imperfect repairs and low system diagnostic coverage, whereas the IEC 61508 standard requires considering the factors.

Even though CCFs can be modelled using combinatorial methods, their impact at the different quality of repair levels cannot be accurately determined due to the methods' inability to incorporate low-quality repairs. Integrating the CCFs into the Markov reliability model

enhances the model's flexibility to investigate various system case studies, enabling the impact of common causes of failure to be comprehensively studied. The case studies results indicate that the existence of CCFs significantly reduces the system's reliability performance, where the highest system sensitivity is observed at low levels of CCFs and high system diagnostic coverage of 99% based on ISO 13849-1 and reduces as the level of diagnostic coverage reduces. Therefore, reliability models of mission-critical systems must incorporate CCFs to determine the system's performance accurately.

The research also investigated the impact of imperfect repairs, system diagnostic coverage and CCFs on the dynamical behaviour of multi-channel IEC 61850 based SCN using Markov partitions and symbolic dynamics based on linear dynamical systems. The investigation's proposed technique advances the Markov time series simulation's insights regarding the system's dynamics and performance. The 'one-out-of-two' IEC 61850 based SCN is dynamically stable and suitable to implement mission-critical functions based on the layout formation of the transition probability matrix's eigenvalues. The spectral gap between the eigenvalue magnitude one and the second largest eigenvalue(s) indicates the system's convergence rate towards the fail-safe recurrent state, whereas multiple eigenvalues of magnitude one indicates the system's periodicity. Moreover, the eigenvalues' magnitudes can be used to determine the various system factors' effectiveness (viz. repair efficiency and CCFs) for optimisation purposes. The desired system dynamics are characterised by aperiodic behaviour and a clearly defined recurrent fail-safe state to ensure plant and personnel safety, as per the IEC 61508 safety-related standard requirements. In addition, a single point of failure should not render the system non-functional. The eigenvalue method's drawback is that it does not provide transient system performance indicators to optimise the system objectively at the subsystem level. Moreover, the individual factors' incremental effect on the mean system state transitions cannot be accurately determined.

The eigenvalue analysis method was advanced by sensitivity and elasticity analysis methods to determine the system's responsiveness to parameter changes accurately at the subsystem level. The method enables the effect of the individual system parameters of interest on the system reliability to be analysed by observing the mean system state transitions, thus allowing parameter optimisation at the subsystem level. The results show that the elasticity of the system reliability is inelastic to the repair efficiency factors. This finding reveals that the benefits of increasing the system repairs level are insignificant for a given level of system performance than the system diagnostic coverage. The diagnostic coverage is the most critical of the two factors, with higher elasticity when the factor approaches 100%.

In contrast, increasing repair efficiency in small magnitudes is ineffective at low system diagnostic coverage levels due to many unrevealed system faults. Therefore, the results

indicate that system performance is very dependent on the diagnostic coverage of the individual subsystems than their repair efficiencies, particularly for high diagnostic coverages at 99% and 90% based on ISO 13849-1 for subsystems A and B in a 'one-out-of-two' system configuration. Hence, the results indicate that emphasis should be more on the system diagnostic coverage because it is embedded in the system design itself that cannot easily be changed at a later stage considering that it would be too expensive and require plant downtime for implementation and testing as well once the system is commissioned and operational.

Hence, the main contributions of the research as discussed in chapter one can be summarised as follows:

a) The research models the quality of repairs (viz. repair efficiency and diagnostic coverage) impacting the reliability performance of IEC 61850 based SCN architecture using the Markov process and symbolic dynamics in the context of Linear Dynamical Systems. This approach enables the determination of system parameter optimisation basis.
b) Sensitivity and elasticity analysis of IEC 61850 based SCN architecture to the quality of repairs (viz. repair efficiency and diagnostic coverage) is modelled to enable effective system parameter adjustment for optimisation purposes using the Markov process and Matrix Calculus methods.

Therefore, the following research questions have been answered by the investigations presented in the thesis:

a) Whether combinatorial reliability analysis methods are suitable for evaluating IEC 61850 based Substation Communication Networks (SCNs) for mission-critical applications, with specific reference to IEC 61508, the standards for safety-related systems?
b) What would be considered a safety-related mission-critical SCN architecture's desired characteristics considering reliability in a power distribution centre within industrial facilities?
c) Whether the quality of repairs can be optimised for best performance, and what would be the basis for optimisation?
d) What would be considered the most critical factor to consider for archiving high-reliability performance, and at what system level?

The proposed model in this research proved to be very effective in investigating the effectiveness of the quality of repairs and CCF, and hence it would apply to more complex systems with many subsystems depending on the modelling approach applied. A system with four subsystems and ten possible states has been modelled in "Publication 7" as detailed in the thesis' "Declaration 2" section. However, careful modelling of parameters of interest is necessary to keep the model complexity at its lowest level possible.

In summary, the proposed modelling technique reveals that the system performance is mainly affected by the diagnostic coverage factors, especially at 90% and below to 60%. In contrast, repair efficiencies closer to 100% do not seem very effective except in cases where the diagnostic coverage is far less than 90%. In addition, the proposed method can be used to investigate the behavioural dynamics of a system, all of which are not possible to determine and quantify using combinatorial analysis methods. Lastly, transient system analysis based on state transition matrix and matrix calculus methods enhances the modelling method's effectiveness to quantify even the most minor changes in system performance through the system's mean state transitions when the system parameters are adjusted for optimisation purposes. Thus, the proposed method is superior to combinatorial analysis methods.

The following section presents the future recommended research work to improve and expand the results contained in this thesis.

## 8.2 Future recommended research work

The following future research work is suggested:

a) It is acknowledged that failures due to varying failure rates may occur during the infancy stage or late in the system's life due to system components' ageing. Nevertheless, failures due to varying components failure rates do not form part of the research's scope because it is usual practice that proven protection systems are employed to execute protection functions. Even so, safety-related system replacements are often made towards the end of the system's useful life, where components failure rates can be considered non-constant. Hence, a system can operate while its failure rate is characterised by the bathtub infancy stage or system components' ageing stage. It is recommended that the research work presented can be expanded to cover all regions of the component's failure rate life-cycle based on the bathtub concept.

b) The proportions of the individual subsystems contributing to common causes of failure are modelled using a single β parameter to demonstrate the analysis approach. This approach assumes that the proportions of the individual system's common causes of failure are identical. Even though the approach demonstrated that the system's reliability performance's responsiveness could be determined, this assumption would generally not be valid in many cases. It is recommended that a multiple beta factor model or similar be considered to investigate the impact of CCF at the subsystem level. The approach will enable various case studies to provide more insight into the impact of CCFs, considering systems with low-quality repairs for executing safety-related functions.

c) The basis for parameter optimisation has been established in the research work presented in the thesis using eigenvalue magnitudes and sensitivity and elasticity studies, considering repair efficiency, diagnostic coverage and common causes of failure. It is

recommended that global optimisations methods be considered to optimise the various system parameters while integrating cost as an additional input parameter.

d) In determining sensitivity and elasticity, the case studies assume that only one system parameter can change at a given point in time. It is suggested that the study be expanded using global sensitivity analysis methods to investigate conditions where multiple parameters can change at a given point in time to improve the result's accuracy.

## REFERENCES


[1] Xin Yang, N. Das, and S. Islam, "Analysis of IEC 61850 for a reliable communication system between substations," in *2013 Australasian Universities Power Engineering Conference (AUPEC)*, 2014, no. October, pp. 1–6, doi: 10.1109/aupec.2013.6725482.

[2] V. C. Mathebula and A. K. Saha, "Mission Critical Safety Functions in IEC-61850 Based Substation Automation System - A Reliability Review," *Int. J. Eng. Res. Africa*, vol. 48, pp. 149–161, 2020, doi: 10.4028/www.scientific.net/jera.48.149.

[3] K. P. Brand, M. Ostertag, and W. Wimmer, "Safety related, distributed functions in substations and the standard IEC 61850," in *2003 IEEE Bologna PowerTech - Conference Proceedings*, 2003, vol. 2, no. July, pp. 260–264, doi: 10.1109/PTC.2003.1304319.

[4] M. C. Magro, P. Pinceti, and L. Rocca, "Can we use IEC 61850 for safety related functions?," in *EEEIC 2016 - International Conference on Environment and Electrical Engineering*, 2016, pp. 1–6, doi: 10.1109/EEEIC.2016.7555402.

[5] M. Caserza Magro, P. Pinceti, L. Rocca, and G. Rossi, "Safety related functions with IEC 61850 GOOSE messaging," *Int. J. Electr. Power Energy Syst.*, vol. 104, no. November 2017, pp. 515–523, 2019, doi: 10.1016/j.ijepes.2018.07.033.

[6] M. H. Lloyd and P. J. Reeve, "IEC 61508 and IEC 61511 assessments - some lessons learned," *4th IET International Conference on Systems Safety 2009. Incorporating the SaRS Annual Conference*. IET, London, UK, UK, 2009, doi: 10.1049/cp.2009.1540.

[7] Y. Zhang, A. Sprintson, and C. Singh, "An integrative approach to reliability analysis of an IEC 61850 digital substation," *IEEE Power Energy Soc. Gen. Meet.*, pp. 1–8, 2012, doi: 10.1109/PESGM.2012.6345699.

[8] V. C. Mathebula and A. K. Saha, "Reliability and Availability of Multi-Channel IEC-61850 Substation Communication Networks for Mission-Critical Applications," *Int. J. Eng. Res. Africa*, vol. 51, pp. 199–216, 2020, doi: 10.4028/www.scientific.net/JERA.51.199.

[9] S. K. Kim and Y. S. Kim, "Evaluation Process for the Hardware Safety Integrity Level," *World Acad. Sci. Eng. Technol. Int. J. Mech. Aerospace, Ind. Mechatron. Manuf. Eng.*, vol. 7, no. 4, pp. 293–297, 2013.

[10] H. Gall, "Functional Safety IEC 61508 / IEC 61511 The Impact to Certification and the User." IEEE, Doha, Qatar, pp. 1027–1031, 2008, doi: 10.1109/AICCSA.2008.4493673.

[11] K. Kaneda, S. Tamura, N. Fujiyama, Y. Arata, and H. Ito, "IEC61850 based substation automation system," *2008 Jt. Int. Conf. Power Syst. Technol. POWERCON IEEE Power India Conf. POWERCON 2008*, 2008, doi: 10.1109/ICPST.2008.4745296.

[12] V. C. Mathebula and A. K. Saha, “Impact of Quality of Repairs and Common Cause Failures on the Reliability Performance of Intra-Bay IEC 61850 Substation Communication Network Architecture based on Markov and Linear Dynamical Systems,” *IEEE Access*, vol. 9, pp. 112805–112820, 2021, doi: 10.1109/ACCESS.2021.3104020.

[13] V. C. Mathebula and A. K. Saha, “Impact of Imperfect Repairs and Diagnostic Coverage on the Reliability of Multi-Channel IEC-61850 Substation Communication Network,” *IEEE Access*, vol. 9, pp. 2758–2769, 2021, doi: 10.1109/ACCESS.2020.3047781.

[14] V. C. Mathebula and A. K. Saha, “Multi-state IEC-61850 Substation Communication Network based on Markov partitions and Symbolic Dynamics,” *Sustain. Energy, Grids Networks*, 2021, doi: 10.1016/j.segan.2021.100466.

[15] V. C. Mathebula and A. K. Saha, “Responsiveness of Multi-Channel IEC-61850 Substation Communication Network Reliability Performance to Changes in Repair Factors,” *IEEE Access*, vol. 9, pp. 789–800, 2021, doi: 10.1109/ACCESS.2020.3046950.

[16] V. C. Mathebula and A. K. Saha, “Sensitivity and Elasticity of Multi-Channel IEC-61850 Substation Communication Networks to Imperfect Repairs,” *Sustain. Energy, Grids Networks*, vol. 26, 2021, doi: https://doi.org/10.1016/j.segan.2021.100443.

[17] R. Gore, H. Satheesh, M. Varier, and S. Valsan, “Analysis of an IEC 61850 based Electric Substation Communication Architecture,” in *Proceedings - International Conference on Intelligent Systems, Modelling and Simulation, ISMS*, 2017, pp. 388–393, doi: 10.1109/ISMS.2016.85.

[18] I. Xyngi and M. Popov, “IEC61850 overview - where protection meets communication,” *10th IET International Conference on Developments in Power System Protection (DPSP 2010). Managing the Change*. IET, Manchester, pp. 1–5, 2010, doi: 10.1049/cp.2010.0321.

[19] S. Roostaee, R. Hooshmand, and M. Ataei, “Substation automation system using IEC 61850,” in *2011 5th International Power Engineering and Optimization Conference, PEOCO 2011 - Program and Abstracts*, 2011, no. June, pp. 393–397, doi: 10.1109/PEOCO.2011.5970443.

[20] L. Ding, H. Wang, J. Jiang, and A. Xu, “SIL verification for SRS with diverse redundancy based on system degradation using reliability block diagram,” *Reliab. Eng. Syst. Saf.*, vol. 165, no. 114, pp. 170–187, 2017, doi: 10.1016/j.ress.2017.03.005.

[21] S. Nsaibi, L. Leurs, and H. D. Schotten, “Formal and simulation-based timing analysis of industrial-ethernet sercos III over TSN,” *Proc. - 2017 IEEE/ACM 21st Int. Symp. Distrib. Simul. Real Time Appl. DS-RT 2017*, vol. 2017-Janua, pp. 1–8, 2017, doi:

10.1109/DISTRA.2017.8167670.

[22] A. Elia, L. Ferrarini, C. Veber, and P. Milano, “Analysis of Ethernet-based safe automation networks according to IEC 61508,” in *2006 IEEE Conference on Emerging Technologies and Factory Automation*, 2006, pp. 333–340.

[23] V. C. Mathebula and A. K. Saha, “Development of In-Phase Bus Transfer Scheme Using Matlab Simulink,” *Proceedings - 2019 Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa, SAUPEC/RobMech/PRASA 2019*, no. 6. IEEE, Bloemfontein, South Africa, pp. 275–280, 2019, doi: 10.1109/RoboMech.2019.8704815.

[24] V. C. Mathebula and A. K. Saha, “Coal Fired Power Plant In-Phase Bus Transfer Simulation of Forced and Induced Draught Fan Motors,” *Proceedings - 2019 Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa, SAUPEC/RobMech/PRASA 2019*. IEEE, Bloemfontein, South Africa, pp. 293–298, 2019, doi: 10.1109/RoboMech.2019.8704820.

[25] V. C. Mathebula, “Application of Bus Transfer Schemes of Stabilise Power Supply in a Coal Fired Power Plant Unit Auxiliary Reticulation,” Durban, South Africa, SE-08, 2019. [Online]. Available: https://researchspace.ukzn.ac.za/handle/10413/17029.

[26] B. Falahati and E. Chua, “Failure modes in IEC 61850-enabled substation automation systems,” *Proc. IEEE Power Eng. Soc. Transm. Distrib. Conf.*, vol. 2016-July, 2016, doi: 10.1109/TDC.2016.7520066.

[27] M. S. Thomas and I. Ali, “Reliable, fast, and deterministic substation communication network architecture and its performance simulation,” *IEEE Trans. Power Deliv.*, vol. 25, no. 4, pp. 2364–2370, 2010, doi: 10.1109/TPWRD.2010.2042824.

[28] S. Gupta, “Reliability Analysis of IEC 61850 Substation Communication Network Architectures,” *Adv. Res. Electr. Electron. Eng.*, vol. 3, no. 2, pp. 93–98, 2016.

[29] F. Tilaro, B. Copy, and M. Gonzalez-Berges, “IEC-61850 Industrial Communication Standards Under Test,” *Proc. ICALEPCS2013, San Fr. CA, USA*, 2014.

[30] J. C. Tan and W. Luan, “IEC 61850 based substation automation system architecture design,” in *IEEE Power and Energy Society General Meeting*, 2011, pp. 1–6, doi: 10.1109/PES.2011.6039814.

[31] S. Roostaee, S. Mehfuz, and M. S. Thomas, “Reliability Comparison of Various Power Substation Automation based on IEC61850,” *Int. J. Ser. Eng. Sci.*, vol. 3, pp. 15–26, 2017, [Online]. Available: http://ijseries.com/.

[32] N. Das and S. Islam, “Analysis of power system communication architectures between substations using IEC 61850,” in *5th Brunei International Conference on Engineering*

*and Technology (BICET 2014)*, 2015, pp. 1.06 (6 .)-1.06 (6 .), doi: 10.1049/cp.2014.1060.

[33] R. Mackiewicz, "Overview of IEC 61850," in *Proceedings of Power Systems Computations Conference*, 2006, vol. 57, no. 57, pp. 1–40, doi: 10.1021/la500336c.

[34] B. E. M. Camachi, O. Chenaru, L. Ichim, and D. Popescu, "A practical approach to IEC 61850 standard for automation, protection and control of substations," *Proc. 9th Int. Conf. Electron. Comput. Artif. Intell. ECAI 2017*, vol. 2017-Janua, pp. 1–6, 2017, doi: 10.1109/ECAI.2017.8166471.

[35] I. Ali and M. S. Thomas, "Substation communication networks architecture," *2008 Joint International Conference on Power System Technology POWERCON and IEEE Power India Conference, POWERCON 2008*. IEEE, New Delhi, India, 2008, doi: 10.1109/ICPST.2008.4745218.

[36] S. M. Suhail Hussain, M. A. Aftab, and I. Ali, "A novel PRP based deterministic, redundant and resilient IEC 61850 substation communication architecture," *Perspect. Sci.*, vol. 8, pp. 747–750, 2016, doi: 10.1016/j.pisc.2016.06.077.

[37] A. Khavnekar, S. Wagh, and A. More, "Comparative Analysis of IEC 61850 Edition-I and II Standards for Substation Automation," *2015 IEEE Int. Conf. Comput. Intell. Comput. Res.*, no. Iccic, pp. 1–6, 2015, doi: 10.1109/ICCIC.2015.7435756.

[38] A. Ingalalli, K. S. Silpa, and R. Gore, "SCD based IEC 61850 traffic estimation for substation automation networks," *IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA*, pp. 1–8, 2018, doi: 10.1109/ETFA.2017.8247596.

[39] N. Liu, M. Panteli, and P. A. Crossley, "Reliability evaluation of a substation automation system communication network based on IEC 61850," in *12th IET International Conference on Developments in Power System Protection (DPSP 2014)*, 2014, no. April, pp. 1–6, doi: 10.1049/cp.2014.0057.

[40] S. Gupta, "Performance analysis of substation communication network architectures in OPNET," *Int. J. Res. Adv. Eng. Technol.*, vol. 3, no. 2, pp. 40–47, 2017.

[41] J. Burger and C. Sufana, "Application Considerations of IEC 61850 / UCA 2 for Substation Ethernet Local Area Network Communication for Protection and Control," *Int. Electr. Test. Assoc. J.*, Art. no. Report No. WGH6, 2005, [Online]. Available: https://www.pes-psrc.org/kb/published/reports/H6Paper-App Consider of IEC61850&UCA_072205_083105.pdf.

[42] IEEE Power System Relaying Committee WG K15 Report, "Centralized Substation Protection and Control." pp. 1–76, 2015.

[43] G. Antonova, L. Frisk, and J. C. Tournier, "Communication redundancy for substation automation," *2011 64th Annu. Conf. Prot. Relay Eng.*, pp. 344–355, 2011, doi: 10.1109/CPRE.2011.6035636.

[44] I. Ali, M. S. Thomas, S. Gupta, and S. M. S. Hussain, “IEC 61850 Substation Communication Network Architecture for Efficient Energy System Automation,” *Energy Technol. Policy*, pp. 82–91, 2015, doi: 10.1080/23317000.2015.1043475.

[45] M. Kumar, A. Kabra, G. Karmakar, and P. P. Marathe, “A review of defences against common cause failures in reactor protection systems,” *2015 4th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2015*. IEEE, Noida, India, pp. 1–6, 2015, doi: 10.1109/ICRITO.2015.7359232.

[46] P. Zhang, L. Portillo, and M. Kezunovic, “Reliability and Component Importance Analysis of All-Digital Protection Systems,” in *2006 IEEE PES Power Systems Conference and Exposition*, 2006, pp. 1380–1387, doi: 10.1109/PSCE.2006.296504.

[47] J. Jayaprakash, D. Neil Jim Eliot, A. Shakilabanu, and S. Kasi Viswanath, “Protection and interlocks of critical equipment in power stations using PLC,” in *Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016*, 2016, pp. 1–8, doi: 10.1109/ISCO.2016.7726881.

[48] P. Wang, X. Chen, and L. Yu, “Application of functional safety theories in furnace safety supervisory system,” in *Proceedings - 9th International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2017*, 2017, pp. 164–167, doi: 10.1109/ICMTMA.2017.0048.

[49] J. V. Bukowski and W. M. Goble, “Properly crediting diagnostics in safety instrumented functions for high demand processes,” *2017 Annual Reliability and Maintainability Symposium (RAMS)*. IEEE, Orlando, FL, USA, pp. 1–6, 2017, doi: 10.1109/RAM.2017.7889648.

[50] O. Gorgies and L. Reindl, “Fail-safe protection Circuit for industrial safety applications,” in *2015 25th International Conference on Information, Communication and Automation Technologies, ICAT 2015 - Proceedings*, 2015, pp. 1–5, doi: 10.1109/ICAT.2015.7340521.

[51] S. Sekiou, Z. Chiremsel, S. Drid, and R. Nait Said, “Failures diagnostic of safety instrumented system: Simulation and experimental study,” in *2013 International Conference on Control, Decision and Information Technologies, CoDIT 2013*, 2013, pp. 776–781, doi: 10.1109/CoDIT.2013.6689641.

[52] F. Redmill, “An introduction to the safety standard IEC 61508,” *Hazard Prev.*, vol. 35, no. 1, pp. 20–25, 1999, [Online]. Available: http://www.csr.ncl.ac.uk/FELIX_Web/4B.IEC 61508 Intro.pdf.

[53] R. Bell, “Introduction & revision of IEC 61508,” *Meas. Control*, vol. 42, no. 6, pp. 174–179, 2009, doi: 10.1177/002029400904200603.

[54] A. Gabriel, C. Ozansoy, and J. Shi, “Developments in SIL determination and calculation,” *Reliab. Eng. Syst. Saf.*, vol. 177, no. April, pp. 148–161, 2018, doi: 10.1016/j.ress.2018.04.028.

[55] A. Gabriel, “Design and Evaluation of Safety Instrumented Systems: A Simplified and Enhanced Approach,” *IEEE Access*, vol. 5, pp. 3813–3823, 2017, doi: 10.1109/ACCESS.2017.2679023.

[56] T. Fujiwara, M. Kimura, Y. Satoh, and S. Yamada, “A method of calculating safety integrity level for IEC 61508 conformity software,” in *Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC*, 2011, pp. 296–301, doi: 10.1109/PRDC.2011.50.

[57] P. B. Ladkin, “An Overview of IEC 61508 on E/E/PE Functional Safety,” *Causalis Ltd. Univ. Bielefeld*, pp. 1–33, 2008.

[58] M. Catelani, L. Ciani, and V. Luongo, “A new proposal for the analysis of safety instrumented systems,” in *2012 IEEE I2MTC - International Instrumentation and Measurement Technology Conference, Proceedings*, 2012, no. May, pp. 1612–1616, doi: 10.1109/I2MTC.2012.6229556.

[59] J. R. Müller, T. Ständer, and E. Schnieder, “Improving system safety modelling in accordance to IEC 61508 by using Monte Carlo simulations,” *IFAC Proc. Vol.*, vol. 2, no. PART 1, pp. 193–197, 2009, doi: 10.3182/20090610-3-IT-4004.00038.

[60] J. V. Bukowski and I. Van Beurden, “Impact of proof test effectiveness on safety instrumented system performance,” in *Proceedings - Annual Reliability and Maintainability Symposium*, 2009, pp. 157–163, doi: 10.1109/RAMS.2009.4914668.

[61] N. Das, W. Ma, and S. Islam, “Analysis of end-to-end delay characteristics for various packets in IEC 61850 substation communications system,” *2015 Australasian Universities Power Engineering Conference (AUPEC)*. IEEE, Wollongong, NSW, Australia, 2015, doi: 10.1109/AUPEC.2015.7324831.

[62] S. Mnukwa and A. K. Saha, “SCADA and substation automation systems for the port of durban power supply upgrade,” *2020 International SAUPEC/RobMech/PRASA Conference, SAUPEC/RobMech/PRASA 2020*. IEEE, Cape Town, South Africa, South Africa, 2020, doi: 10.1109/SAUPEC/RobMech/PRASA48453.2020.9041078.

[63] A. Albarakati *et al.*, “Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management,” 2019, doi: 10.1109/SmartGridComm.2019.8909710.

[64] A. T. A. Pereira, L. A. C. Lisboa, and A. M. N. Lima, “Strategies and techniques applied to IEC 61850 based DSAS architectures,” 2016, doi: 10.1049/cp.2016.0009.

[65] J. Stark, W. Wimmer, and K. Majer, “Switchgear Optimization Using IEC 61850-9-2,” 2013.

[66] M. L. De Klerk and A. K. Saha, “A Review of the Methods Used to Model Traffic Flow in a Substation Communication Network,” *IEEE Access*, vol. 8, pp. 204545–204562, 2020, doi: 10.1109/access.2020.3037143.

[67] R. M. Rahat, M. H. Imam, and N. Das, “Comprehensive Analysis of Reliability and Availability of Sub-Station Automation System with IEC 61850,” 2019, doi: 10.1109/ICREST.2019.8644416.

[68] S. Kumar, N. Das, and S. Islam, “High performance communication redundancy in a digital substation based on IEC 62439-3 with a station bus configuration,” 2015, doi: 10.1109/AUPEC.2015.7324838.

[69] T. J. Wong and N. Das, “Modelling and analysis of IEC 61850 for end-to-end delay characteristics with various packet sizes in modern power substation systems,” 2014, doi: 10.1049/cp.2014.1073.

[70] S. Kumar, N. Das, and ; Syed Islam, “Performance Analysis of Substation Automation Systems Architecture Based on IEC 61850,” 2014, doi: 10.1109/AUPEC.2014.6966532.

[71] J. Á. Araujo, J. Lázaro, A. Astarloa, A. Zuloaga, and J. I. Gárate, “PRP and HSR for high availability networks in power utility automation: A method for redundant frames discarding,” *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2325–2332, Sep. 2015, doi: 10.1109/TSG.2014.2387474.

[72] M. G. Kanabar and T. S. Sidhu, “Reliability and availability analysis of IEC 61850 based substation communication architectures,” in *2009 IEEE Power and Energy Society General Meeting*, 2009, pp. 1–8, doi: 10.1109/PES.2009.5276001.

[73] B. Yunus, A. Musa, H. S. Ong, A. R. Khalid, and H. Hashim, “Reliability and Availability Study on Substation Automation System based on IEC 61850,” 2008, doi: 10.1109/PECON.2008.4762462.

[74] M. Mekkanen, R. Virrankoski, M. Elmusrati, and E. Antila, “Reliability evaluation and comparison for next-generation substation function based on IEC 61850 using Monte Carlo simulation,” 2013, doi: 10.1109/ICCSPA.2013.6487306.

[75] R. Billinton and R. N. Allan, *Reliability Evaluation of Power Systems*, 2nd ed. New York: Plenum Publishing Corporation, 1984.

[76] H. Ngo *et al.*, “An improved High-availability Seamless Redundancy (HSR) for dependable Substation Automation System.pdf,” 2014, doi: 10.1109/ICACT.2014.6779094.

[77] W. R. Wessels, “Use of the Weibull versus exponential to model part reliability,” in *2007 Proceedings - Annual Reliability and Maintainability Symposium*, 2007, no. 2, pp. 131–135, doi: 10.1109/RAMS.2007.328115.

[78] J. F. Kitchin, “Practical Markov modeling for reliability analysis,” in *1988 Proceedings Annual Reliability and Maintainability Symposium*, 1988, pp. 290–296, doi: 10.1109/arms.1988.196463.

[79] G. Gupta, R. P. Mishra, and P. Jain, “Reliability analysis and identification of critical components using Markov model,” in *IEEE International Conference on Industrial Engineering and Engineering Management*, 2016, vol. 2016-Janua, pp. 777–781, doi: 10.1109/IEEM.2015.7385753.

[80] B. O. Mkandawire, N. Ijumba, and A. K. Saha, “Transformer risk modelling by stochastic augmentation of reliability-centred maintenance,” *Electr. Power Syst. Res.*, vol. 119, pp. 471–477, 2015, doi: 10.1016/j.epsr.2014.11.005.

[81] T. C. Sharma and I. Bazovsky, “Reliability analysis of large system by Markov techniques,” in *1993 PROCEEDINGS Annual RELIABILITY AND MAINTAINABILITY Symposium*, 1993, pp. 260–267, doi: 10.1109/rams.1993.296845.

[82] G. F. M. Souza and C. A. Gabe, “Reliability modeling of partially repairable systems applied on electrical power system,” *Proc. - Annu. Reliab. Maintainab. Symp.*, pp. 1–6, 2017, doi: 10.1109/RAM.2017.7889685.

[83] P. M. Anderson, G. M. Chintaluri, S. M. Magbuhat, and R. F. Ghajar, “An improved reliability model for redundant protective systems - Markov models,” *IEEE Trans. Power Syst.*, vol. 12, no. 2, pp. 573–578, 1997, doi: 10.1109/59.589606.

[84] A. Hildebrandt, “Calculating the ‘probability of failure on demand’ (PFD) of complex structures by means of Markov Models,” *4th Pet. Chem. Ind. Conf. Eur. Instrum. Appl. PCIC Eur.*, pp. 1–5, 2007, doi: 10.1109/PCICEUROPE.2007.4353993.

[85] D. J. Smith, *Maintainability and Risk:Practical Methods for Engineers*, 8th ed. London, UK: Butterworth-Heinemann, 2011.

[86] S. Asgarpoor and M. J. Mathine, “Reliability Evaluation of Distribution Systems with Non-Exponential Down Times,” *IEEE Trans. Power Syst.*, vol. 12, no. 2, pp. 579–584, 1997, doi: 10.1109/59.589607.

[87] H. Mo, W. Wang, M. Xie, and J. Xiong, “Modeling and analysis of the reliability of digital networked control systems considering networked degradations,” *IEEE Trans. Autom. Sci. Eng.*, vol. 14, no. 3, pp. 1491–1503, 2017, doi: 10.1109/TASE.2015.2443132.

[88] N. Isaac and A. K. Saha, “Analysis of refueling behavior of hydrogen fuel vehicles through a stochastic model using Markov Chain Process,” *Renew. Sustain. Energy Rev.*, vol. 141, no. October 2020, p. 110761, 2021, doi: 10.1016/j.rser.2021.110761.

[89] C. L. M. Belusso, S. Sawicki, F. Roos-frantz, and R. Z. Frantz, “A Study of Petri Nets, Markov Chains and Queueing Theory as Mathematical Modelling Languages Aiming at the Simulation of Enterprise Application Integration Solutions : a first step,”

*Procedia - Procedia Comput. Sci.*, vol. 100, pp. 229–236, 2016, doi: 10.1016/j.procs.2016.09.147.

[90] D. H. Meadows, *Thinking in Systems*. Earthscan, 2009.

[91] B. O. Mkandawire, N. M. Ijumba, and A. K. Saha, "Component Risk Trending Based on Systems Thinking Incorporating Markov and Weibull Inferences," *IEEE Syst. J.*, vol. 9, no. 4, pp. 1185–1196, 2015, doi: 10.1109/JSYST.2014.2363384.

[92] M. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein, "A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability," *IEEE Commun. Surv. Tutorials*, vol. 11, no. 2, pp. 106–124, 2009, doi: 10.1109/SURV.2009.090208.

[93] J. R. Belland, "Modeling common cause failures in diverse components with fault tree applications," *2017 Proceedings - Annual Reliability and Maintainability Symposium (RAMS)*. IEEE, Orlando, FL, USA, 2017, doi: 10.1109/RAM.2017.7889659.

[94] D. Kumar, G. L. Pahuja, and J. K. Quamara, "Chemical reactor safety system reliability under common cause failure," *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, Bangalore, India, India, pp. 2534–2537, 2018, doi: 10.1109/RTEICT42901.2018.9012319.

[95] E. R. Scheinerman, *Invitation To Dynamical Systems*. Dover Publications, 2013.

[96] H. Caswell, "Sensitivity analysis of discrete Markov chains via matrix calculus," *Linear Algebra Appl.*, vol. 438, no. 4, pp. 1727–1745, 2013, doi: 10.1016/j.laa.2011.07.046.

[97] A. Kaufmann, D. Grouchko, and R. Cruon, *Mathematical Models for the Study of the Reliability of Systems*, vol. 124. London: Academin Press, Inc., 1977.

[98] T. Winkovich and D. Eckardt, "Reliability analysis of safety systems using Markov-chain modelling," *2005 European Conference on Power Electronics and Applications*. IEEE, Dresden, Germany, Germany, 2005, doi: 10.1109/epe.2005.219620.

[99] W. Hu, "Dynamical systems," *Vertical Integration of Research and Education (VIGRE)*. University of Chicago, Chicago, pp. 1–15, 2009, [Online]. Available: https://math.uchicago.edu/~may/VIGRE/VIGRE2009/REUPapers/Hu.pdf.

[100] D. Margalit and J. Rabinoff, "Interactive Linear Algebra," Georgia Institute of Technology, Atlanta, Georgia, 2019. [Online]. Available: https://textbooks.math.gatech.edu/ila/subspaces.html.

[101] M. R. Spiegel, *Advanced Mathematics for Engineers and Scientists*, S.I.ed. Singapore: Schaum's Outline Series, 1983.

[102] D. G. Nel, "On matrix differentiation in statistics," *South African Stat. J.*, vol. 14, pp. 137–193, 1980.

[103] H. Caswell, “Sensitivity analysis of transient population dynamics,” *Ecol. Lett.*, vol. 10, no. 1, pp. 1–15, 2007, doi: 10.1111/j.1461-0248.2006.01001.x.

[104] H. Caswell, *Sensitivity analysis : matrix methods in demography and ecology*. Switzerland: Springer, 2019.

[105] J. R. Magnus and H. Neudecker, *Matrix differential calculus with applications in statistics and econometrics*. New York: John Wiley and Sons, 1988.

[106] Erwin Kreyszig, *Advanced Engineering Mathematics*, 8th ed. Singapore: John Wiley & Sons, Inc., 1999.

[107] L. Andersson, K. P. Brand, C. Brunner, and W. Wimmer, “Reliability investigations for SA communication architectures based on IEC 61850,” in *2005 IEEE Russia Power Tech, PowerTech*, 2005, pp. 1–7, doi: 10.1109/PTC.2005.4524707.

[108] E. Zaitseva and V. Levashenko, “Construction of a Reliability Structure Function Based on Uncertain Data,” *IEEE Trans. Reliab.*, vol. 65, no. 4, pp. 1710–1723, 2016, doi: 10.1109/TR.2016.2578948.

[109] C. B. Keating and A. V. Gheorghe, “Systems thinking: Foundations for enhancing system of systems engineering,” in *2016 11th Systems of Systems Engineering Conference, SoSE*, 2016, pp. 1–6, doi: 10.1109/SYSOSE.2016.7542957.

[110] D. R. Padhi, P. Chavan, and R. Mitra, “Understanding systems thinking from the perspectives of experience and diversity,” in *Proceedings - IEEE 9th International Conference on Technology for Education, T4E 2018*, 2018, pp. 122–125, doi: 10.1109/T4E.2018.00033.

[111] R. D. Arnold and J. P. Wade, “A definition of systems thinking: A systems approach,” *Procedia Comput. Sci.*, vol. 44, no. C, pp. 669–678, 2015, doi: 10.1016/j.procs.2015.03.050.

[112] C. W. Caulfield and S. P. Maj, “A case for systems thinking and system dynamics,” in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics. e-Systems and e-Man for Cybernetics in Cyberspace (Cat.No.01CH37236)*, 2001, vol. 5, pp. 2793–2798, doi: 10.1109/icsmc.2001.971932.

[113] L. Assidmi, “Education dynamics: A systems thinking perspective,” in *Proceedings - 2015 5th International Conference on e-Learning, ECONF 2015*, 2015, pp. 188–194, doi: 10.1109/ECONF.2015.29.

[114] D. H. Kim, “Guidelines for Drawing Causal Loop Diagrams,” *Syst. Thinker*, vol. 3, no. 1, pp. 5–6, 1992.

[115] A. Avižienis, J. C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” *IEEE Trans. Dependable Secur. Comput.*, vol. 1, no. 1, pp. 11–33, 2004, doi: 10.1109/TDSC.2004.2.

[116] F. E. Nadir, I. H. Baraka, M. Bsiss, and B. Amami, “Influence of failure modes and

effects analysis on the average probability of failure on demand for a safety instremented system," *Colloq. Inf. Sci. Technol. Cist*, pp. 867–871, 2017, doi: 10.1109/CIST.2016.7805010.

[117] David Smith, *Reliability, Maintainability and Risk*, 9th ed. Butterworth-Heinemann: Elsevier, 2017.

[118] A. Porras-Vázquez and J. A. Romero-Pérez, "A new methodology for facilitating the design of safety-related parts of control systems in machines according to ISO 13849:2006 standard," *Reliab. Eng. Syst. Saf.*, vol. 174, pp. 60–70, 2018, doi: 10.1016/j.ress.2018.02.018.

[119] T. Fukuda, M. Hirayama, N. Kasai, and K. Sekine, "Evaluation of operative reliability of safety-related part of control system of machine and safety level," in *Proceedings of the SICE Annual Conference*, 2007, pp. 2480–2483, doi: 10.1109/SICE.2007.4421406.

[120] P. Lerévérend, "Inside the standardization jungle: IEC 62061 and ISO 13849-1, complementary or competing?," *2008 5th Petroleum and Chemical Industry Conference Europe - Electrical and Instrumentation Applications*. IEEE, Weimar, Germany, 2008, doi: 10.1109/PCICEUROPE.2008.4563534.

[121] J. V. Bukowski and R. Chalupa, "Calculating an appropriate multiplier for βλ when modeling common cause failure in triplex systems," *Proceedings - Annual Reliability and Maintainability Symposium (RAMS)*. San Jose, CA, USA, 2010, doi: 10.1109/RAMS.2010.5447996.

[122] L. Xing and W. Wang, "Probabilistic Common-Cause Failures analysis," *2008 Proceedings - Annual Reliability and Maintainability Symposium*. IEEE, Las Vegas, NV, USA, 2008, doi: 10.1109/RAMS.2008.4925821.

[123] Q. Muhammad, N. Amjad, and M. Zubair, "Modeling Of Common Cause Failures (CCFs) by using Beta Factor Parametric Model." IEEE, Islamabad, Pakistan, 2014, doi: 10.1109/ICESP.2014.7347004.

[124] M. Pourali, "Incorporating common cause failures in mission-critical facilities reliability analysis," *IEEE Trans. Ind. Appl.*, vol. 50, no. 4, pp. 2883–2890, 2014, doi: 10.1109/TIA.2013.2295472.

[125] J. Qin, R. Gu, and G. Li, "Reliability modeling of incomplete common cause failure systems subject to two common causes," *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. IEEE, Singapore, Singapore, pp. 1906–1910, 2017, doi: 10.1109/IEEM.2017.8290223.

[126] P. Hokstad and M. Rausand, *Common Cause Failure Modeling : Status and Trends*. London: Springer, 2008.

[127] Q. Shao, S. Yang, C. Bian, and X. Gou, "Formal Analysis of Repairable Phased-

Mission Systems With Common Cause Failures," *IEEE Trans. Reliab.*, pp. 1–12, 2020, doi: 10.1109/tr.2020.3032178.

[128] R. Smith and M. Modarres, "A physics of failure approach to common cause failure considering component degradation," *2020 Proceedings - Annual Reliability and Maintainability Symposium*. IEEE, Palm Springs, CA, USA, pp. 1–6, 2020, doi: 10.1109/RAMS48030.2020.9153651.

[129] Kathleen T. Alligood, Tim D. Sauer, and J. A. Yorke, *An introduction to dynamical systems and chaos*. New York: Springer-Verlag, Inc., 1996.

[130] D. Rickles, P. Hawe, and A. Shiell, "A simple guide to chaos and complexity," *J. Epidemiol. Community Health*, vol. 61, no. 11, pp. 933–937, 2007, doi: 10.1136/jech.2006.054254.

[131] N. Karcanias and A. G. Hessami, "Complexity and the notion of system of systems: part (I): general systems and complexity."

[132] N. Karcanias and A. G. Hessami, "Complexity and the notion of system of systems: Part (II): Defining the notion of system of systems," in *2010 World Automation Congress, WAC 2010*, 2010, no. I.

[133] M. J. Berryman and P. Campbell, "Some complex systems engineering principles," *Aust. Preeminent Syst. Eng. Test Eval. Conf.*, 2010, [Online]. Available: http://ro.uow.edu.au/smartpapers/1/.

[134] A. Hessami, "A framework for characterising complex systems and system of systems," in *Proceedings - 2013 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2013*, 2013, pp. 1702–1708, doi: 10.1109/SMC.2013.293.

[135] S. Effah-Poku, W. Obeng-Denteh, and I. K. Dontwi, "A Study of Chaos in Dynamical Systems," *J. Math.*, vol. 2018, no. 1, pp. 0–5, 2018, doi: 10.1155/2018/1808953.

[136] E. M. Bollt and joe D. Skufca, "Markov Parititions," 2002. https://webspace.clarkson.edu/~ebollt/Papers/MarkovPartitionsNonlinearEncyclopedia.pdf (accessed Mar. 06, 2020).

[137] D. M. Curry, "Practical application of Chaos Theory to systems engineering," *Procedia Comput. Sci.*, vol. 8, pp. 39–44, 2012, doi: 10.1016/j.procs.2012.01.011.

[138] T. Li and J. A. Yorke, "Period Three Implies Chaos," *Am. Math. Mon.*, vol. 82, no. 10, pp. 985–992.

[139] C. Nicolis, "Chaotic dynamics, Markov processes and climate predictability," *Tellus, Ser. A*, vol. 42 A, no. 4, pp. 401–412, 1990, doi: 10.3402/tellusa.v42i4.11886.

[140] M. D. Richard, "Properties and Discrimination of Chaotic Maps," in *1993 IEEE International Conference on Acoustics, Speech, and Signal Processing*, 1993, pp. 141–144, doi: 10.1109/ICASSP.1993.319455.

[141] A. Boyarsky and P. Góra, *Probability and Its Applications - Laws of Chaos - Invariant*

*Measures and Dynamical Systems in One Dimension*. Birkhäuser, 1997.

[142] R. G. Gallager, *Stochastic Processes Theory for applications*. United Kingdom: Cambridge University Press, 2013.

[143] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed. UK: Cambridge University Press, 2013.

[144] J. H. Hubbard and B. H. West, *Linear Dynamical Systems*. Berlin, Heidelberg: Springer-Verlag, Inc., 1993.

[145] G. J. Olsder, "Max Algebra Approach to Discrete Event Systems," 1993.

[146] F. W. Roush, "Applied Mathematical Modeling: A Multidisciplinary Approach," *Math. Soc. Sci.*, vol. 17, no. 2, p. 203, 1989, doi: 10.1016/0165-4896(89)90010-3.

[147] M. L. Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. John Wiley & Sons, Inc., 2005.

[148] J. M. Cargal, *Discrete Mathematics for Neophytes: Number Theory, Probability, Algorithms, and Other Stuff*. 1988.

[149] R. L. Tweedie, "Criteria for Classifying General Markov Chains," *Adv. Appl. Probab.*, vol. 8, no. 4, pp. 737–771, 1976.

[150] K. W. Yun, "Application of the Economic Elasticity Concept to Compressor Performance Parameters," in *International Compressor Engineering Conference*, 1992, pp. 1315–1321, [Online]. Available: https://docs.lib.purdue.edu/icec/926.

[151] P. Mohr and L. Fourie, *Economics for South African Students*, 3rd Editio. South Africa: Van Schaik Publishers, 2004.

[152] E. F. Brigham and M. C. Ehrhardt, *Financial Management*. London, UK: Thomson Learning, 2007.

[153] O. C. Ibe, "Markov Processes for Stochastic Modeling," 2nd Ed., London, UK: Elsevier, 2013, pp. 49–57.

[154] W. E. Roth, "On direct product matrices," *Bull. Am. Math. Soc.*, vol. 40, no. 6, pp. 461–468, 1934, doi: 10.1090/S0002-9904-1934-05899-3.

[155] A. A. Van Raalte and H. Caswell, "Perturbation Analysis of Indices of Lifespan Variability," *Popul. Assoc. Am.*, vol. 50, no. 5, pp. 1615–1640, 2013, doi: 10.1007/s13524-013-0223-3.

# APPENDIX A

Scripts included for demonstration purposes.

## APPENDIX A-1

The MATLAB programme presented in this section eigenvalues of the transition probability for various factors of repair efficiency, diagnostic coverage and common causes of failures the sensitivity and elasticity of the fundamental matrix.

```
clear;
%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//
%//Subsystem A: cascaded (CCDD)//
lambda_a = 0.13999;   %failure rate of subsystem A
mu_a = 730;           %repair rate of subsystem A
edcA = 0.99;          %system A diagnostic coverage
%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//
%Subsystem B: Star-ring (SR)
lambda_b = 0.11333;   %failure rate of subsystem B
mu_b = 730;           %repair rate of subsystem B
edcB = 0.78;          %system B diagnostic coverage
%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//
%//CCF//
lambda_ccf = (lambda_a+lambda_b)/2;
beta = 0;
%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//
pgraphNoPl = 20; %Number of times to adjust "edc" and or
%"reff" and plot graph
i=1;
eigenVs_1 = zeros(pgraphNoPl,1);
eigenVs_2 = zeros(pgraphNoPl,1);
eigenVs_3 = zeros(pgraphNoPl,1);
eigenVs_4 = zeros(pgraphNoPl,1);
y = zeros(pgraphNoPl,1);
reff = 1:-(1/pgraphNoPl):0;
 for graphNo=1:length(reff)
        reffA = reff(i);
```

```
        reffB = reff(i);

    %//Transition probability matrix of 'one-out-of-two'
system with transition

%//parameters lambda_*, mu_*, edc*, reff* and beta

P = [0 ((1-beta)*lambda_a/(((1-beta)*lambda_a)+((1-
beta)*lambda_b)+(beta*lambda_ccf))) ((1-beta)*lambda_b)/(((1-
beta)*lambda_a+((1-beta)*lambda_b)+(beta*lambda_ccf)))
((beta*lambda_ccf)/(((1-beta)*lambda_a)+((1-
beta)*lambda_b)+(beta*lambda_ccf)));

    ((mu_a*edcA*reffA)/(mu_a*edcA*reffA+(lambda_b+(mu_a*(1-
edcA))))) 0 0 ((lambda_b+(mu_a*(1-edcA)))/((lambda_b+(mu_a*(1-
edcA)))+mu_a*edcA*reffA));

    (mu_b*edcB*reffB/(mu_b*edcB*reffB+lambda_a+(mu_b*(1-
edcB)))) 0 0 (lambda_a+mu_b*(1-edcB))/((lambda_a+mu_b*(1-
edcB))+mu_b*edcB*reffB);

    0 0 0 1];

mc = dtmc(P, 'StateNames',["S-1" "S-2" "S-3" "S-4"]);

numSteps = 100;

%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++//

figure(1)

[eVals,~] = eigplot(mc);

hold on

 y(i)=reffA;

eigenVs_1(i) = abs(eVals(1));

eigenVs_2(i) = abs(eVals(2));

eigenVs_3(i) = abs(eVals(3));

eigenVs_4(i) = abs(eVals(4));

 i=i+1;

end
```

**APPENDIX A-2**

The MATLAB programme presented in this section determines the sensitivity and elasticity of the fundamental matrix. The programme requires "vec.m" MATLAB function, which is a vector operator function defined by (:) in MATLAB programming.

```
%//Definition of subsystems reliability parameters//
%//Subsystem A: cascaded (CCDD)//
lambda_a = 0.13999;         %// Failure rate of subsystem A//
mu_a = 730;                 %//Repair rate of subsystem A//
edcA = 0.60;                %//System A diagnostic coverage//
reffA = 0.95;               %//System A repair efficiency//
%//Subsystem B: Star-ring (SR)//
lambda_b = 0.11333;         %//Failure rate of subsystem B//
mu_b = 730;                  %//Repair rate of subsystem B//
edcB = 0.60;                %//System B diagnostic coverage//
reffB = 0.70;               %//System B repair efficiency//
%//+++++++++++++++++++++++++++++++++++++++++++++++++++++++++//
%//CCF
lambda_ccf = (lambda_a+lambda_b)/2;
beta = 0;
%//+++++++++++++++++++++++++++++++++++++++++++++++++++++++++//
%//System low level parameters//
R = [reffA reffB edcA edcB beta];
%//Low-level transition probability matrix P//
P = [0 ((1-beta)*lambda_a/(((1-beta)*lambda_a)+((1-
beta)*lambda_b)+(beta*lambda_ccf))) ((1-beta)*lambda_b)/(((1-
beta)*lambda_a+((1-beta)*lambda_b)+(beta*lambda_ccf)))
((beta*lambda_ccf)/(((1-beta)*lambda_a)+((1-
beta)*lambda_b)+(beta*lambda_ccf)));
    ((mu_a*edcA*reffA)/(mu_a*edcA*reffA+(lambda_b+(mu_a*(1-
edcA))))) 0 0 ((lambda_b+(mu_a*(1-edcA)))/((lambda_b+(mu_a*(1-
edcA)))+mu_a*edcA*reffA));
    (mu_b*edcB*reffB/(mu_b*edcB*reffB+lambda_a+(mu_b*(1-
edcB)))) 0 0 (lambda_a+mu_b*(1-edcB))/((lambda_a+mu_b*(1-
edcB))+mu_b*edcB*reffB);
    0 0 0 1];
%//Transient state matrix Q//
```

```
Q = P;

Q(4,:)=[];

Q(:,4)=[];

[~,s]=size(Q);

%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//

%//P21nm is the numerator of element P21//

P21nm = mu_a*edcA*reffA;

%//P31nm is the numerator of element P31//

P31nm = mu_b*edcB*reffB;

%//P21dn is the denominator of element P21//

P21dn = (mu_a*edcA*reffA+(lambda_b+(mu_a*(1-edcA))));

%//P31dn is the denominator of element 31//

P31dn = (mu_b*edcB*reffB+lambda_a+(mu_b*(1-edcB)));

%//P11dn is the denominator of element 11//

P11dn = (lambda_a*(1-beta))+(lambda_b*(1-
beta))+(beta*lambda_ccf);

 %//The derivatives of fundamental matrix with respect to
%repair efficiency

%//and diagnostic coverage factors: dvecQdp

%//dvecQdp(1) ->reffA//

%//Page 1//

dvecQdp(:,:,1) = zeros(s);

dvecQdp(2,1,1) = ((mu_a*edcA*(P21dn - P21nm))/(P21dn^2));

%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//

%//dvecQdRT(2) ->reffB//

%//Page 2//

dvecQdp(:,:,2) = zeros(s);

dvecQdp(3,1,2) = ((mu_b*edcB*(P31dn - P31nm))/(P31dn^2));

%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//

%//dvecQdRT(3) ->edcA//

%//Page 3//

dvecQdp(:,:,3) = zeros(s);

dvecQdp(2,1,3) = (mu_a*(P21dn*reffA - P21nm*(reffA-
1)))/(P21dn^2);
```

```
%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//

%//dvecQdRT(4) ->edcB//

%//Page 4//

dvecQdp(:,:,4) = zeros(s);

dvecQdp(3,1,4) = (mu_b*(P31dn*reffB - P31nm*(reffB-
1)))/(P31dn^2);

%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//

%//dvecQdRT(5) ->beta//

%//Page 5//

dvecQdp(:,:,5) = zeros(s);

dvecQdp(1,2,5) = (-lambda_a*P11dn - ((lambda_a*(1-beta)*(-
lambda_a-lambda_b+lambda_ccf))))/(P11dn^2);

dvecQdp(1,3,5) = (-lambda_b*P11dn - ((lambda_b*(1-beta)*(-
lambda_a-lambda_b+lambda_ccf))))/(P11dn^2);

%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//

%//Fundamental matrix N

I = eye(s); %//Identity matrix of size Q given by s//

N = (I - Q)^(-1);

%//Transposed fundamental matrix N -> NT//

NT = N';

%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//

%//Create matrix dvecQdRT//

%//Define size of dvecQdRT//

dvecQdRT = zeros([(s^2),length(R)]);

for i = 1:length(R)

dvecQdRT(:,i)= vec(dvecQdp(:,:,i));

end

%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//

%//Sensitivity of repair efficiency and diagnostic capability
%to system

%//states transitions (i.e. elements of the fundamental matrix
%N//

dNdvecRT = (kron(NT,N))*dvecQdRT;

%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//

%//Elasticities of repair efficiency and diagnostic capability
%factors
```

```
%//Rearrange N to a vector using vector operator//
vecN = vec(N);
%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//
%//Convert vectors to diagonal matrices//
DgvecN = diag(vecN);
DgR = diag(R);
%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//
%//Calculate elasticities//
EdNdvecRT = (DgvecN^(-1))*dNdvecRT*DgR;
%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//
%//Sensitivity of fundamental matrix N//
%//Repair efficiency on subsystem A//
SS_reffA = dNdvecRT(:,1);
%//Repair efficiency on subsystem B//
SS_reffB = dNdvecRT(:,2);
%//Diagnostic capability on subsystem A//
DG_edcA = dNdvecRT(:,3);
%//Diagnostic capability on subsystem B//
DG_edcB = dNdvecRT(:,4);
%//CCF//
DG_CCF = dNdvecRT(:,5);
%//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++//
%//Elasticity of fundamental matrix N//
%//Repair efficiency on subsystem A//
E_reffA = EdNdvecRT(:,1);
%//Repair efficiency on subsystem B//
E_reffB = EdNdvecRT(:,2);
%//Diagnostic capability on subsystem A//
E_edcA = EdNdvecRT(:,3);
%//Diagnostic capability on subsystem B//
E_edcB = EdNdvecRT(:,4);
%//CCF on Subsystem//
E_CCF = EdNdvecRT(:,5);
```

```
%//Programme does not include plotting of results, which will
%depend
%// on the intended use//
```