THE UNIVERSITY OF HULL

SAFE-FLOW: A Systematic Approach for Safety Analysis of Clinical Workflows

being a Thesis submitted for the Degree of Doctor of Philosophy

in the University of Hull

by

Lamis Farah Al-Qora'n

B.Sc., Yarmouk University, Jordan, 2003

M.Sc., University of Hull, UK, 2006

March 2015

SAFE-FLOW: A Systematic Approach for Safety Analysis of Clinical Workflows

Abstract

The increasing use of technology in delivering clinical services brings substantial benefits to the healthcare industry. At the same time, it introduces potential new complications to clinical workflows that generate new risks and hazards with the potential to affect patients' safety. These workflows are safety critical and can have a damaging impact on all the involved parties if they fail.

Due to the large number of processes included in the delivery of a clinical service, it can be difficult to determine the individuals or the processes that are responsible for adverse events. Using methodological approaches and automated tools to carry out an analysis of the workflow can help in determining the origins of potential adverse events and consequently help in avoiding preventable errors. There is a scarcity of studies addressing this problem; this was a partial motivation for this thesis.

The main aim of the research is to demonstrate the potential value of computer science based dependability approaches to healthcare and in particular, the appropriateness and benefits of these dependability approaches to overall clinical workflows. A particular focus is to show that model-based safety analysis techniques can be usefully applied to such areas and then to evaluate this application.

This thesis develops the SAFE-FLOW approach for safety analysis of clinical workflows in order to establish the relevance of such application. SAFE-FLOW detailed steps and guidelines for its application are explained. Then, SAFE-FLOW is applied to a case study and is systematically evaluated. The proposed evaluation design provides a generic evaluation strategy that can be used to evaluate the adoption of safety analysis methods in healthcare.

It is concluded that safety of clinical workflows can be significantly improved by performing safety analysis on workflow models. The evaluation results show that SAFE-FLOW is feasible and it has the potential to provide various benefits; it provides a mechanism for a systematic identification of both adverse events and safeguards, which is helpful in terms of identifying the causes of possible adverse events before they happen and can assist in the design of workflows to avoid such occurrences. The clear definition of the workflow including its processes and tasks provides a valuable opportunity for formulation of safety improvement strategies.

To my beloved husband: Abdelsalam Alodat

To my children: Mahdi, Rama, Leen and Raya

To my great father

To the soul of my mother

Acknowledgement

Foremost, I would like to thank my supervisor, Dr. Neil Andrew Gordon, for his continuous support through my PhD study, for his patience, encouragement, keenness, and knowledge. I could not have imagined having a better supervisor and mentor for my PhD study.

I would like to extend my gratitude to Dr. Martin Walker, the technical expert and the second supervisor of the research, for his technical support, help and insightful comments on the thesis content. I also would like to thank the chair of my PhD committee, Dr. Darryl Davis, for monitoring my academic progress.

Special thanks go as well to Prof. Yiannis Papadopoulos and Dr. Septavera Sharvia for their support, comments and for reading parts of the thesis.

I am grateful to Philadelphia University, Jordan, which provided me with much appreciated financial support during my study period to make my dream come true.

I am also grateful to all the administrative staff in the department of Computer Science for their practical support throughout my PhD. I also thank my fellow lab mates in the department especially Dr. Ernest Edifor and Sohag Kabir; their support and friendship are much appreciated.

Thanks to my father, brothers and sisters for believing in my abilities and for encouraging me to start and continue this doctoral journey.

Finally, my deepest and massive thank you goes to my husband Abdelsalam and to my children Mahdi, Rama, Leen and Raya for their continuous love and support, and for allowing me time away from family to get my PhD completed.

Table of Contents

Abstract **2**

Acknowledgement **4**

Table of Contents **5**

List of Figures **10**

List of Tables **12**

1 Introduction **13**

1.1 Research Motivation 14

1.2 Research Context and Scope 17

1.3 Research Questions 18

1.4 Aim and Objectives 19

1.5 Thesis Structure 20

1.6 Note on Publications 22

2 Background **24**

2.1 Introduction to Safety Analysis 24

2.2 Safety Analysis Methods 26

2.2.1 Fault Tree Analysis (FTA) 27

2.2.2 Failure Mode and Effect Analysis (FMEA) 29

2.2.3 Petri Nets 30

2.2.4 Bayesian Networks (BNs) 31

2.2.5 Simulation Based Verification and Formal Verification 33

2.2.6 Model-Based Safety Analysis (MBSA) 33

2.2.6.1 Behavioural MBSA Methods: Model Checking 34

2.2.6.2 Compositional MBSA Methods: Hierarchically-Performed Hazard Origin and Propagation Studies (HiP-HOPS) 35

2.2.7 Discussion 37

2.3 Patient Safety and Safety Analysis in Healthcare 42

2.4 Workflows and Clinical Workflows 46

2.5 Workflow Management and Workflow Modelling 47

2.6 Workflow Modelling in Healthcare 49

2.7 Challenges of Workflow Modelling in Healthcare in Comparison to Industry 59

2.8 Evaluation Background 61

2.8.1 Usability Testing 61

2.8.2 Evaluation Frameworks 62

3 SAFE-FLOW: A Systematic Approach for Safety Analysis of Clinical Workflows 63

3.1 Challenges in Safety Analysis of Clinical Workflows 63

3.2 SAFE-FLOW: A Systematic Approach for Safety Analysis of Clinical Workflow 67

3.2.1 Workflow Documentation (Step 1) 70

3.2.2 Workflow Modelling (Step 2) 73

3.2.3 Hazards Identification and Risk Assessment (Step 3) 80

3.2.4 Failure Annotation (Step 4) 84

3.2.5 Fault Tree and FMEA Synthesis and Analysis (Step 5) 88

3.2.6 Probability Analysis (Optional Step) 89

3.2.7 New Workflow Design (Optional Step) 91

3.2.8 Accepting the Workflow (Step 6) 91

3.3 Conclusion 92

4 Safety Analysis of the Workflow within a Radiology Department- Case Study 93

4.1 Why Use Radiology Workflow for a Case Study? 93

4.2 Applying SAFE-FLOW to the Radiology Workflow 97

4.2.1 Workflow Documentation (for the Main Workflow within the Department) 97

4.2.2 Workflow Modelling 106

4.2.3 Hazards Identification and Risk Assessment 109

4.2.4 Failure Annotation 110

4.2.5 Fault Tree and FMEA Synthesis and Analysis 114

4.2.6 Probability Analysis 117

4.2.7 New Workflow Design and Accepting the Workflow 117

4.3 Safety Analysis of RIS/PACS Workflow- Wrong Treatment Scenario 118

4.3.1 Workflow Scenario Documentation 118

4.3.2 Workflow Modelling 119

4.3.3 Hazards Identification and Risk Assessment 121

4.3.4 Failure Annotation 121

4.3.5 Fault Tree and FMEA Synthesis and Analysis 124

4.3.6 Probability Analysis 128

4.3.7 New Workflow Design and Accepting of the Workflow 128

4.4 Discussion of the Achieved Benefits 129

4.5 Conclusion 131

5 Evaluation..132

5.1 Evaluation Design 132

5.1.1 Usability Testing 132

5.1.2 The Application of the Evaluation Framework...134

5.1.3 Comparison with Other Methods for Analysing the Safety of Clinical Workflows...........152

5.2 Summary and Recommendations...155

6 Conclusion and Future Work 157

6.1 Summary of Key Findings 157

6.2 Contributions of the Research..162

6.3 Limitations of the Research 164

6.4 Future Work 165

6.4.1 Improving Workflow Modelling...166

6.4.2 Comprehensive Safety Analysis (Incorporating more Scenarios) 166

6.4.3 Incorporating Administrative Processes 166

6.4.4 Application of Probability Analysis...166

6.4.5 Considering the Order of Events...166

6.4.6 Usability of SAFE-FLOW 167

References..168

Appendix 1: List of Abbreviations 179

Appendix 2: Interviews Questions..182

First Set of Interview Questions...182

Interview Questions for Evaluating SAFE-FLOW (first group and second group) 183

Third Group Interview Questions with Answers 184

Appendix 3: Case Study: Analysis of a Tele Guideline based Decision support system for Generating Referral Recommendations using HiP-HOPS 188

Workflow Documentation..188

Workflow Modelling...190

Hazards Identification..192

Failure annotation 193

Fault Tree and FMEA Synthesis and Analysis 195

New Workflow Design and Accepting the Workflow..198

Limitation and assumptions: 199

List of Figures

Figure 1 Basic Fault Tree structure........27

Figure 2 Inductive FMEA and deductive FTA........29

Figure 3 A simple Petri net example........30

Figure 4 A simple Bayesian Network example........32

Figure 5 Overview of HiP-HOPS (Papadopoulos *et al.*, 2011, pg. 596)........37

Figure 6 Flowchart for modelling of clinical process modelling........51

Figure 7 RAD for modelling of clinical process (Patel, 2000)........53

Figure 8 DFD for modelling of clinical workflow (Jun *et al.*, 2009)........54

Figure 9 SAFE-FLOW: An approach for safety analysis of clinical workflows........69

Figure 10 Modelling the interaction between an information system and an actor........74

Figure 11 Modelling the interaction between an actor and a system........74

Figure 12 Modelling Parallel Processes........75

Figure 13 Modelling of conditional processes........76

Figure 14 The hierarchical representation of components........77

Figure 15 Modelling of a nurse collecting blood sample........78

Figure 16 Modelling of shared processes........79

Figure 17 HiP-HOPS failure editor........88

Figure 18 The Radiology workflow (HiP-HOPS snapshot)........107

Figure 19 The CM component (HiP-HOPS snapshot)........108

Figure 20 CMDoseCalculation Component (HiP-HOPS snapshot)........109

Figure 21 FTA result for the CT scan scenario........114

Figure 22 MCS result for the CT scan scenario........115

Figure 23 The Radiology workflow- treatment scenario........120

Figure 24 FTA- treatment scenario 125

Figure 25 Evaluation design: Evaluation over three levels 132

Figure 26 CDC's Framework for Program Evaluation in Public Health (U.S. Department of Health and Human Services, 1999) 135

Figure 27 Sources of information for evaluating SAFE-FLOW 136

Figure 28 the interviews' main sections 141

Figure 29 Characteristics that contribute to improving clinical workflows 146

Figure 30 Decision Tree (Mohktar *et al.*, 2010) 189

Figure 31 Architecture of the System 191

Figure 32 Architecture of the GBDSS after decomposition 192

List of Tables

Table 1 Positive and negative points of safety analysis methods 41

Table 2 Organising a human component example 72

Table 3 Workflow Safety Levels 83

Table 4 organising the components of the radiology workflow 105

Table 5 Failure information for the CT scan scenario 112

Table 6 FMEA of direct and further effects 115

Table 7 Failure information- treatment scenario 123

Table 8 MCS- treatment scenario 126

Table 9 FMEA direct effects- treatment scenario 126

Table 10 FMEA of further effects- treatment scenario 127

Table 11 Participants' opinions regarding the usability of the models 142

Table 12 Participants' opinions regarding the ability of the models to represent clinical workflow concepts 143

Table 13 Participants' opinions about improving clinical workflows and their safety through using SAFE-FLOW 146

Table 14 Participants' concerns about the application of SAFE-FLOW 148

Table 15 MCSs for the home telemonitoring system 195

Table 16 FMEA direct effects 197

Table 17 (FMEA Table with component failures having direct effects towards false negative error) 198

1 Introduction

Despite the complexity of healthcare, in common with many other industries it is adopting an Information Technology (IT) infrastructure (Reid *et al.*, 2005; Chiasson and Davidson, 2004). This IT infrastructure has the potential to bring substantial benefits to the healthcare industry and to patients, such as increasing the efficiency and the quality of care. However, it can cause complexities and technical hitches in delivering clinical services (Kaplan, 1987; Bates, 2002; Kaplan and Harris-Salamone, 2009). It can also bring significant risks that threaten **patient safety** and can have devastating consequences if errors occur (Crane, 2012). Moreover, many of the non-technical processes and activities involved in delivering a **clinical service**, no matter how routine or common, can endanger patient safety.

The process of delivering a clinical service can involve numerous constituents that can be difficult to manage and control. Those constituents, including the involved processes, humans, activities, information systems and data flows are together termed as a **clinical workflow**.

It has been widely reported that different healthcare errors, including those in medical treatment processes and workflows, are a major cause of death and suffering (Starfield, 2000; Green, 2013). Research carried out in the United Kingdom, Australia and the United States showed that 1 in 10 patients admitted to hospitals suffers an **adverse event** (Emslie *et al.*, 2002). An adverse event is assumed to have occurred when a patient suffers unpredicted harm which is unrelated to the patient’s underlying medical condition (Kruskal *et al.*, 2008). Due to the large number of processes, people and information systems included in the delivery of a clinical service, it can be difficult, in general, to determine the individuals or the processes that are responsible for adverse events.

Patient safety has come to be an international priority (Battles and Lilford, 2003). Therefore, guaranteeing the safety of patients who are seeking clinical services is considered one of the most important issues in healthcare and finding effective methods to reduce medical errors and their contribution to adverse events is required (Murff *et al.*, 2003; Battles and Lilford, 2003).

One important stage of research initiatives in patient safety is the identification of risks and hazards (Battles and Lilford, 2003). Using technical tools to do so has the potential to help in determining the root causes of the possible adverse events and has the potential to enable the redesign of the processes and tasks that are accountable for such events; consequently, this may improve the reliability of the workflow through designing more reliable and non-faulty workflows.

To conclude, there are often no formal methods for analysing workflows, and such tasks are often done ad-hoc by people. Taking lessons from the dependability field and applying some of the same techniques may yield improvements in the safety of those workflows.

1.1 Research Motivation

Designing and implementing a clinical service usually comprises many tasks to be performed by many people, and increasingly by information systems. It also has numerous administration and diagnostic procedures and variations of these, providing many opportunities for error. Having these constituents included within the care process has the potential to create complex workflows and can introduce new concerns.

Producing the right clinical service without having any unexpected conditions and side effects is the ideal aim, although in practice the complexities preclude this beyond very simple scenarios. Such complex workflows and care flows can affect patient safety by omitting a clinical service, producing the wrong clinical service or producing the right clinical service whilst having side effects.

Accordingly, the different processes and systems that are involved in producing a clinical service can place the service in hazardous circumstances. Moreover, the adoption of new applications has the potential to affect the whole workflow design and can introduce new failure modes or bring hidden failure modes that have the potential to lead to catastrophic consequences or loss of human lives. Those workflows must be given attention and analysed for their safety early during their design and before they are put into operation. In addition, they should be analysed when new systems are installed in order to reduce the risks that they may cause and to achieve benefits from their involvement.

A **hazard** is a set of conditions within the system state from which there is a path to a disaster. Undetected errors that may happen in any process during the diagnostic imaging study or intervention lead to adverse events where the patient comes to the hospital for a diagnosis and goes home with impairment. The key to integrated safety is the identification and mitigation of hazards in these systems and adverse events in their workflows.

The matter of patient safety has come to be a problem of great concern in healthcare, many researchers have identified the importance of risk analysis in healthcare (e.g. Stathiakis *et al*. (2003) and Maglogiannis *et al.* (2006)). In response to these concerns, safety analysis approaches from other industries have started to be adopted in healthcare. For example, classical safety assessment techniques such as Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA) are employed to predict the safety of clinical processes(Ward *et al.*, 2007; Abujudeh and Kaewlai, 2009). However, classical techniques are traditionally applied through a manual process, where the information is produced from a number of informal sources. In the context of clinical workflows, this may become difficult, laborious and error-prone. Moreover, analysis performed in this way can be subjective and dependent on the skills of the safety engineer. For this reason, FTA and FMEA are usually performed to analyse a number of incidents for a certain workflow.

Therefore, the lack of defined models for the clinical workflows and their failure modes drives the efforts of the analyst to gather information about the workflow architecture and the workflow behaviour in order to insert this information in safety artefacts such as fault trees. This situation can be significantly improved by performing safety analysis activities based on formal models for the workflow under development.

Clinical workflows need to be analysed and broken down into simple processes or even into atomic tasks in order to improve the process of service delivery. Although improving the service delivery process is often understood as key to efficient services, to date there have been few process improvement studies (Shukla *et al.*, 2014).

Therefore, clinical workflows must be designed and modelled to include and identify the basic activities involved in the workflow, care flow and information flow (dataflow). During and after the modelling process, if prospective contributors leading to the workflow failure can be identified, potential system and workflow weaknesses may be discovered and effectively improved. Finding the root causes of possible failures allows greater understanding of the factors contributing to undesired events that can potentially lead to a serious clinical risk. This understanding can be used to detect the gaps between the actual guidelines and the actual practice, and accurately specify any **deviations**. In other words, the analysis not only needs to show where the workflow is incorrect, but also where critical errors may arise if the correct workflow is not followed in the operational phase. The analysis must take place at the design stage (the stage at which the workflow is first created, before it is put in operation) in order to guarantee correct operations in the operational phase of the workflow.

Finding methods to undertake safety analysis has the potential to improve understanding of the workflow behaviour and its potential for failure, thus highlighting areas where additional checks or amendments to the workflow need to be introduced. Moreover, automated methods would help to deal with the complexity and time cost issues, and reduce the load on safety analysts.

To date it appears that researchers have given little attention to the safety analysis of clinical workflows in general and to the automated analysis of such workflows in particular. Furthermore, from reviewing the literature it appears that little work has been done on evaluating the use of safety analysis methods in healthcare. This is possibly because of the efforts required for evaluating their outcomes in practice and the resistance from healthcare experts. This resistance may arise from a lack of both clear analysis goals and well-designed methods for performing the analysis process.

Overall, healthcare is not as safe as it should be. An important body of evidence pointed to medical errors as a leading cause of death and injury (Kohn *et al.*, 2000). Healthcare safety calls for developing well-designed techniques for the analysis of patient safety when carrying out clinical processes. Lessons learnt from industry and computer science approaches for safety analysis have the potential to help healthcare organisations to avoid prospective hazards and to deliver safer care; this is the motivation of this thesis.

1.2 Research Context and Scope

The focus of this thesis is on the safety of clinical workflows and patient safety in the face of potential failures arising from human, software, and hardware errors. This safety can be achieved through intensive application of safety engineering to create robust, reliable, and dependable medical applications (Schrenker, 2006).

The study of dependability has long played an important role in the development and deployment of safety critical systems (Knight, 2002). Safety analysis is one of the main factors in the study of dependability (Lahoz *et al.*, 2012). Safety analysis techniques, for example FTA Vesely *et al.* (1981) and FMEA, have been prominently used in many safety critical industries, particularly in the nuclear and aerospace industries.

In this context, dependability of healthcare systems and clinical workflows is considered a major concern as with the dependability of many other safety critical systems. In order to provide reliable, efficient, and individualised care for patients efficient techniques are required for the purpose of safety and dependability analysis of clinical workflows.

This thesis investigates how the experience developed over the past 50-60 years in the field of dependability can be applied outside the usual type of systems, in this case to workflows in the healthcare domain. Therefore, it utilises and builds on an existing safety engineering technique to produce a systematic approach (SAFE-FLOW) for the safety analysis of clinical workflows. Consequently, it is concerned with developing an approach that focuses on the integrated application of safety analysis techniques to safety critical workflows, and in particular the application of model-based safety analysis techniques to this domain. SAFE-FLOW allows searching for root causes that lead to failures and accidents in different workflows within the healthcare domain.

Leveson *et al.* (2009) stated that focusing the study of dependability only on the technical part is insufficient, and they showed the importance of organisational and human factor contributions. SAFE-FLOW overcomes the limitation of many studies of dependability by considering human, organisational, procedural, software and hardware errors.

Therefore, the thesis develops a link between the healthcare domain and the established safety engineering concepts, enabling the utilisation of existing safety analysis software to be applied in the healthcare domain. At the end, the thesis systematically evaluates the approach over three levels in terms of benefits and limitations.

In many situations, hazards can threaten clinical staff and hospitals' reputations as well. However, the scope of this thesis is limited to the analysis of hazards that threaten patient safety.

1.3 Research Questions

Safety analysis tools have been successfully used in mechanical systems to identify weak points in systems (Papadopoulos *et al.*, 2011). In this thesis, it is argued that the gap in the safety analysis of clinical workflows can be overcome by adapting model-based safety analysis techniques.

The following research question develops from the general consideration of the problem of safety analysis in healthcare:

> **How can established dependability analysis techniques be adapted to improve the safety of clinical workflows?**

This main research question leads to the following sub questions:

1. To what extent can existing safety analysis methods and lessons learnt from industry help in improving the safety of clinical workflows?
2. How can workflows be captured in a model, and given that, how can that model be made compatible with model-based safety analysis approaches?
3. How can safety analysis be used as part of a robust methodology for designing dependable clinical workflows and improving patient safety?
4. How can new workflow analysis methods be evaluated in terms of their impact on the safety of clinical workflows?

These questions show the need for investigating the available modelling approaches and safety analysis methods that have been used in industry, and to test the applicability of these methods to clinical workflows. Using such approaches and methods can increase trust and confidence in the healthcare system through helping in the validation of workflows. Moreover, the last question shows the need for evaluating safety analysis methods once they are adapted in healthcare, as well as the need for finding suitable evaluation frameworks to perform such evaluation.

1.4 Aim and Objectives

The aim of the thesis is to demonstrate the potential value of computer-based dependability approaches to healthcare and in particular the appropriateness and benefits of these to overall clinical workflows. A particular focus is to show that model-based safety analysis techniques can be mapped and usefully applied to such areas and then to evaluate this application.

Through the application and the evaluation of such techniques, healthcare experts and administrators will be able to understand the care flows more clearly and will be able to manage risks more effectively.

Answering the research questions and achieving the above aim relies on meeting the following objectives:

1. To examine related safety analysis methods in high-risk industries and investigate their strengths and limitations. The purpose is to establish a conceptual and realistic basis for the review of methods that have been used for the analysis of adverse events in healthcare.
2. To develop appropriate link between traditional components for such dependability approaches and the constituents of a healthcare workflow. In other words, to capture workflows in models that are compatible with safety analysis approaches. This involves investigating how inputs to tools can be constructed, in particular, how to define and model the workflow components.
3. To develop the SAFE-FLOW approach for a systematic safety analysis of clinical workflows.
4. To examine the applicability of SAFE-FLOW to realistic clinical workflows using empirical research.
5. To establish a systematic evaluation plan to evaluate the benefits and limitations of SAFE-FLOW.

1.5 Thesis Structure

The thesis is structured and designed as follows:

1. Introduction

The introduction chapter explains the main problem to be solved: improving the safety of clinical workflows. It also introduces the aim and objectives of the research and demonstrates the structure of the thesis.

2. Background Information

The background chapter contains the essential background information; it presents an overview and explanation of safety analysis techniques that have been used in other industries. Then the chapter describes patient safety and the safety analysis process in healthcare industry. It also presents an introduction to workflows, clinical workflows, workflow management and modelling and defines the challenges in workflow modelling within the healthcare domain. Finally, the chapter presents the background information required to understand the evaluation chapter.

The research gaps found in this background investigation have been used to arrange the development and evaluation of SAFE-FLOW.

3. SAFE-FLOW: An Integrated Approach for Safety Analysis of Clinical Workflows

This chapter introduces SAFE-FLOW as an approach for safety analysis of clinical workflows; explaining the basic concepts and describing various steps involved.

4. Case Study

Having explained the detailed steps of SAFE-FLOW, this chapter illustrates how it can be used in practice by applying it to two scenarios for the workflow within a radiology department. The application and analysis is explained in detail and the analysis results are discussed, showing how SAFE-FLOW can successfully facilitate improvements in workflow design.

5. Evaluation

This chapter evaluates SAFE-FLOW. The evaluation is done over three levels. It first tests the usability of SAFE-FLOW, and then it applies an evaluation framework to systematically evaluate SAFE-FLOW, and finally compares SAFE-FLOW with other approaches available in the literature. Finally, the chapter provides a summary and recommendations.

6. Conclusion and Future Work

This chapter describes what has been achieved.

References

A list of the references used in the thesis is provided here.

Appendix 1: List of Abbreviations

This appendix provides an explanation of some of the abbreviations and terms found in this document.

Appendix 2: Interviews Questions

This appendix provides the questions that were used to evaluate the proposed approach.

Appendix 3: Case study

This appendix describes a case study on the workflow of a home Telemonitoring system, and presents a model which was adopted from Mohktar *et al.* (2010). This case study provides a second example of the feasibility of SAFE-FLOW and demonstrates how safety analysis of the workflow can shape its development.

1.6 Note on Publications

Some of the material in this thesis has already been published in the following conferences and journals:

Al-Qora’n, L., Sharvia, S., Gordon, N. & Papadopoulos, Y. 2013. Safety Analysis of a Remote Patient Monitoring System with a Guideline Based Decision Support. In*: proceedings of Med-e-Tel,* April 10-12 2013 2013 Luxembourg. 322-327.

Al-Qora'n, L., Sharvia, S., Gordon, N. & Walker, M. 2014. Safety analysis of clinical workflows: The case of the workflow within a radiology department, *Science and Information Conference (SAI), 2014* (pp. 72-78). IEEE.

Al-Qora’n, L., Gordon, N., Sharvia, S., Walker, M. & Papadopoulos, Y. 2014. An Approach to Safety Analysis of Clinical Workflows, Athens: ATINER'S Conference Paper Series, No: COM2014-1157. (The same paper is published in *Athens Journal of Health* September 2014, pages 201-216).

Al-Qora’n, L., Gordon, N., Walker, M., Sharvia, S., & Kabir, S. 2014. A Safety Analysis Approach to Clinical Workflows: Application and Evaluation, *International Journal of Advanced Computer Science and Applications* (IJACSA), Special Issue on Extended Papers from Science and Information Conference 2014, 2014, 4(3).

2 Background

This chapter reviews the relevant literature that provides a base for understanding the rest of the thesis. The first part of the chapter explores classical safety analysis methods, and investigates the contemporary methods developed to deal with the more complex designs. The techniques are discussed and evaluated, with emphasis on their benefits and shortcomings. Although studies of probability are used in some forms of analysis, the focus here is on the qualitative aspects of safety analysis and the qualitative process that is primarily concerned with the identification and establishment of relationships between causes and effects of failures. The second part introduces the concept of patient safety and reviews the safety analysis process in healthcare. Then it discusses and explains in detail the concepts of workflow, clinical workflows, workflow management and workflow modelling. In addition, it provides an overview of the techniques that are in use for workflow modelling in healthcare and discusses some issues and challenges related to them to provide a more detailed view of the research problem. Further, it examines the possibility of reusing methods that have been used in other industries in healthcare. Finally, the third part of the chapter introduces a background on possible evaluation methods that have the potential to help in evaluating SAFE-FLOW.

2.1 Introduction to Safety Analysis

Nowadays, people depend on different technologies and systems to perform a wide range of daily tasks. They expect those machines and systems to work without being interrupted by failures; this is called the reliability of the system. System failure occurs when the system delivers a service that deviates from the intended service (Avizienis *et al.*, 2001). In other words, it is a modification of the correct service into an incorrect service. Different systems always have their own failure modes, which are the ways in which the systems can fail. Failure to start, failure to open and failure to shut down are examples of failure modes. System safety is concerned with avoiding the catastrophic consequences of these failures. Safety was defined by Papadopoulos (2013) as the system's ability to operate without causing hazards to people and the environment. Avizienis *et al.* (2001) outlined system safety as an attribute of reliability, and both reliability and safety as attributes of a more comprehensive concept termed dependability, which they defined as the ability of the system to provide a service that can reasonably be trusted. So, if the system is dependable this means the user is confident that the system will function as anticipated and it will not fail in normal use (Lahoz *et al.*, 2012). Dependability is related primarily to assurance that systems resist faults when they occur, e.g. through mitigation of standby components. Other major aspects include fault tolerance, which provides an acceptable level of service even when faults occur (Lutz, 2000) and fault prevention, through which designers try to design the system to be as fault-free as possible in the first place.

So, safety critical systems are those systems whose failure could cause consequences that are determined to be unacceptable: for example loss of life, significant damage to a property, or damage to the environment (Knight, 2002). It is vital to ensure that those systems do not fail catastrophically by making sure that those systems are as reliable and as robust as possible (Walker, 2009).

Because of their nature, safety critical systems should be checked and analysed for their safety before their deployment. The process of system analysis, in general, is a focused process to investigate and acquire specific system information that is relevant to a specified decision at the right time and in the right order (Vesely *et al.*, 1981). Vesely *et al.* (1981) declared that the system can be analysed for different purposes: for example to test out whether the system accomplishes some task successfully; to investigate whether the system will prove more costly than originally anticipated; or to check whether the system fails in some hazardous way. The latter analysis is called safety analysis, through which identifying hazards and making design changes to reduce the risk and the severity of the hazardous states must be considered. Through safety analysis, designers achieve a deeper understanding of the system context, how it works and how they can fail. Safety analysis is considered an essential part of the development process of safety critical systems.

The attributes of interest for system safety can vary for different types of safety analysis methods. Each of these attributes is addressed at some point during the safety analysis process (Ericson, 2005). (Shishko and Aster, 1995) defined functional analysis as the process of classifying, describing, and linking the functions performed by a system in order to fulfil its goal and objectives. This analysis results in a functional model. Here, different system elements (e.g. people, hardware, software and procedures) cooperate to perform a certain function. This thesis focuses on the safety analysis process; it addresses and considers hardware components, software components, human factors**,** functions (such as failure to perform a function or performing an incorrect function) and interfaces (e.g. inaccurate inputs/ outputs).

Different analysis techniques which have been used by safety engineers are explained in the following sections.

2.2 Safety Analysis Methods

Classical safety analysis methods were developed primarily to support the analysis process in the aerospace and nuclear industries. Most classical techniques operate in either an inductive or a deductive approach. Inductive techniques aim at determining the effects of a failure, while deductive techniques attempt to discover the causes of a failure. Some of them, such as FTA and FMEA, are still employed for hazard identification and for linking causes of failures and their effects.

With the increasing complexity in safety critical systems new approaches are being developed to deal with the complications of such systems. An example of these approaches is model-based safety analysis in which certain models are used as input sources for complementary safety analysis and assessment techniques, in addition to being a basis for the documentation of the assessment results (Gran *et al.*, 2007).

The following sub-sections provide an overview of classic and contemporary safety analysis techniques that have been used in areas that might be comparable to the research context.

2.2.1 Fault Tree Analysis (FTA)

FTA is considered one of the most widely used safety analysis techniques. It was developed first by Bell Laboratories in 1961, in connection with a U.S. Air Force contract, to analyse the Minuteman Missile launch control system (Watson, 1961). The fault tree itself is a logic diagram that demonstrates the logical relationship between the undesired event (often termed as 'top event') and the basic events. In other words, it is a structure to define the ways in which the top event may occur and it can be constructed for a system that is being designed as well as for a system that is implemented and operated (Huang *et al.*, 2004). The fault tree uses logical AND and OR gates to show the relationship between different events which are statistically independent.

The following figure shows the basic fault tree structure:

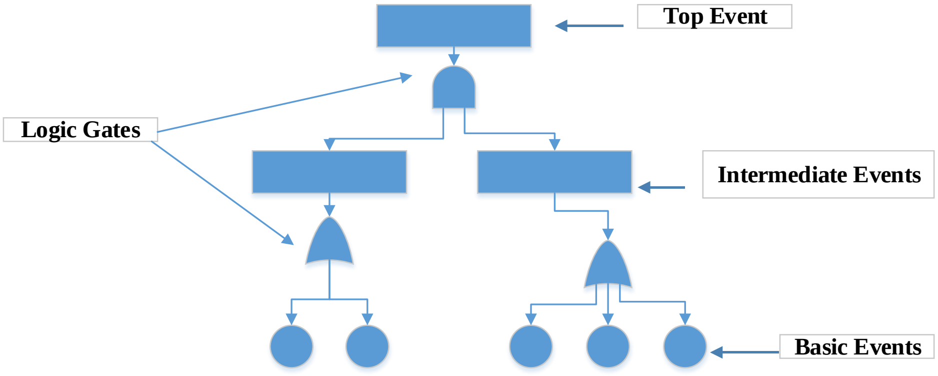


Figure 1 Basic Fault Tree structure

Therefore, FTA is a system analysis technique that is supported by the logical structure to represent basic events (faults) that lead to a certain undesired outcome (system failure). To find all possible ways in which the system failure can take place, the system environment and operations are analysed. This is done by assigning the undesired event at the top of the tree and then working in a deductive approach to detect the root causes (called 'basic events') of the top event and their combinations. The combinations of basic events that cause the top event to happen when they take place are called cut sets, and the cut set is called a Minimal Cut Set (MCS) when all the basic events in the cut set are necessary to cause the occurrence of the top event.

The analysis in FTA is accomplished through a qualitative analysis step, which can be followed by a quantitative analysis phase. In the qualitative analysis, MCSs are identified; this helps the designer to focus on the design's weak points. For example, if the failure of component C1 is identified during FTA as being a direct cause of the failure of the system, the system designer is now informed about this critical component, and can reconsider the design (e.g. by introducing a backup component to prevent this single point failure). Qualitative analysis can be beneficial for early models of system design when probabilistic data are not available.

In the quantitative step, probabilities are assigned to the failure events of the basic components to calculate the overall probabilities of system hazards. When basic components of the system under analysis do not have enough probabilistic failure information available, then qualitative analysis is more useful. In such situations where the probability data of the basic events is not available, experts' opinion can sometimes be used to estimate the basic event data and uncertainties that need to be covered. Manual evaluation can be completed and computerised methods can be used for the evaluation of FTs that are more complex. Fuzzy set theory has been used recently in FT analysis by many authors to reduce error boundaries that might be caused by inaccurate and incomplete data on the primary events (Khakzad *et al.*, 2011)

FTA has the ability to reflect the logical combinations of software, hardware, and human errors that cause the top event to occur and can help in identifying effective upgrades of the system. Overall, it can help in assessing the reliability of the system design. However, the analysis is dependent on the analyst's abilities, particularly the identification of the hazardous top events in the first place. Recent work has introduced improvements to the fault tree method by the use of automated analysis to extract

MCSs. Furthermore, FTA has moved on from its early origins in aerospace to be applied efficiently in many other industries including healthcare.

2.2.2 Failure Mode and Effect Analysis (FMEA)

FMEA is an important tool to evaluate system design from the reliability and safety perspectives. The method was first developed and described in a US Armed Forces Military Procedures document in 1949. In the early 1950s, it was used to evaluate the design of flight control systems (Coutinho, 1964). After that a tool was designed for use by teams; it was early use was by NASA, and it became better known when it was implemented by the Ford car manufacturers in about 1977 (Gilchrist, 1993). Unlike FTA, FMEA is an inductive technique (see the figure below) that tries to determine the consequences of a fault, thus provides a detailed analysis of the possible failure modes for each component and their effects on the system. FMEA is presented in a tabular manner and can contain additional information about the component failure (e.g. criticality and probability of occurrence).

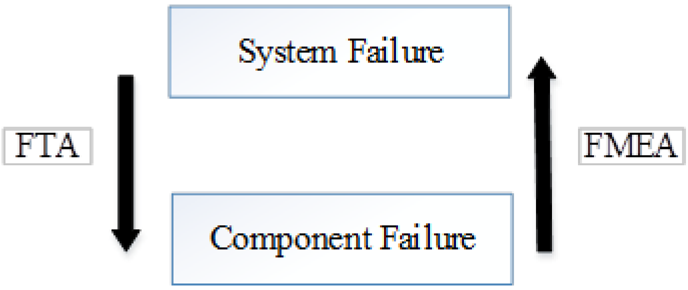


Figure 2 Inductive FMEA and deductive FTA

The process can be done by picking the high-risk processes to be analysed. Then a team of experts is selected to start the analysis process and to identify procedures for improvement. Finally, the efficiency of actions taken is evaluated.

Classical FMEA relies heavily on human perceptions and experience. It is unable to determine complex failure modes and their effects. This procedure always starts by listing all components of the system, then listing all possible failure modes and failure rates. After that, the possible effects for each failure are determined. Therefore, it is traditionally a difficult manual process.

Like FTA, FMEA has moved on from its early origins in aerospace to be applied effectively in many other industries including healthcare. More about the use of FMEA in healthcare will come in the forthcoming sections.

2.2.3 Petri Nets

The theory of Petri nets has developed from the work of Carl Adam Petri (Petri, 1962), and has been proposed for many applications in areas such as manufacturing, production, networks, software design, software specifications, and simulation. It uses basic symbols to define relations between conditions and events. The classical Petri net is a directed bipartite graph that has two node types (places and transitions) connected by directed arcs, where an arc never runs between nodes of the same type. Places are signified by circles and transitions by rectangles: each place may contain one or more tokens. Every place stands for a state in the system. The following figure shows a simple Petri net example:

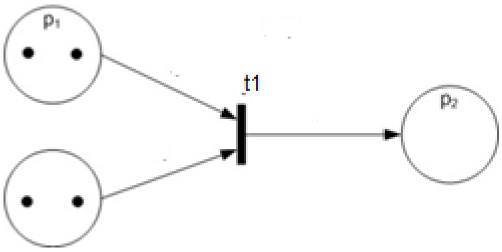


Figure 3 A simple Petri net example

A Petri net is defined mathematically as:

$PN = < P, T, I, O >$

P: is a finite set of places, *{p1, p2,…, pn}*

T: is a finite set of transitions, {*t1, t2, …, tn*}

I: is an input function, and *O*: is an output function

In a Petri net, if an edge is directed from place *p* to transition *t*, then *p* is said to be an input place for transition *t*, and an output place is defined in the same way. Transition *t* is supposed to be enabled only if every input place for it has at least one token. When an enabled transition is fired, a predefined number of tokens from each input place is removed and added into each output place.

Petri nets are a very general model which can capture finite state machines, dataflow networks and in theory any process that can be represented as a graph (Patkar *et al.*, 2008).

Leveson and Stolzy (1987) identified that since Petri nets have been used to analyse different system properties like deadlocks and reachability, and because of their ability to model hardware, software, and human behaviour, they can then be used for designing and analysing other properties like safety and fault tolerance. Therefore, they described the use of Time Petri nets in the design and analysis of safety-critical systems by extending the basic model to allow the modelling of failures and faults. They proposed an algorithm that provided a solution to the long reachability graph problem, which can cause the analysis of Petri nets to be difficult. The reachability set for a Petri net is the set of states that results from executing the Petri net; it facilities the determination of how the system design can reach any high-risk state.

Liu and Chiou (1997) presented a Petri net approach to failure analysis; they used Petri nets to obtain the MCSs efficiently and claimed that Petri nets are more efficient for failure analysis than fault trees. Later, Knezevic and Odoom (2001) developed a methodology which used Petri nets instead of fault tree methodology and used the Fuzzy set theory for representing the failure rate and repair time.

2.2.4 Bayesian Networks (BNs)

BNs are defined by a Directed Acyclic Graph (DAG) in which a set of random variables and their conditional dependencies are represented. The nodes represent the variables, the arcs signify direct dependencies between the linked nodes, and the conditional probability tables assigned to the nodes specify how strongly the linked nodes influence each other.

A simple example of Bayesian Networks is shown in Figure 4:

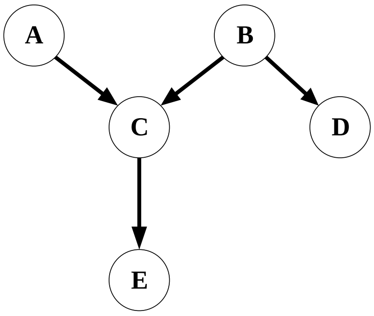


Figure 4 A simple Bayesian Network example

If there is an arrow from one node to another then the first node is called the parent of the other node. Therefore, node B is the parent of both C and D because there is an arrow from B to C and D, and C is called the parent of E. A node without a parent is known as a 'root node' and a node without a child is called a 'leaf node' (e.g. A is a root node and D and E are leaf nodes in Figure 4).

A BN consists of a qualitative part, a directed acyclic graph where the nodes reflect the random variables, and a quantitative part, the set of conditional probability functions (Langseth and Portinale, 2007). However, BNs are primarily used for quantitative rather than qualitative analysis.

Researchers gave BNs great attention in the last decade because of their ability to provide a global safety assessment through combining different sources of information as well as their ability to provide a robust probabilistic method of reasoning under uncertainty (Bobbio *et al.*, 2001; Langseth and Portinale, 2007; Mahadevan *et al.*, 2001).

BNs models require specialised technical knowledge and there are no well-defined rules for creation of BNs models for safety analysis purposes. Therefore, building BNs can be a challenging and laborious task, as it needs a BNs expert to encode the information and assumptions from the studied domain to a BNs model, and the safety analyst requires basic knowledge about BNs.

2.2.5 Simulation Based Verification and Formal Verification

Simulation is the use of a computer model to represent people, components and spaces. It needs a detailed descriptive data of the system to be embedded within the model in order to define the behaviour of each element. Having the model embedded with detailed failure data enables the engineer to simulate different failure scenarios. Here the engineer can visualise the effect of the fault on the workflow. This mechanism can easily detect safety problems in common scenarios.

Simulation-based verification is different from formal verification in the fact that it requires input vectors to derive reference outputs, while in formal verification the user starts out by stating the required output behaviour and then lets the formal checker prove or disprove it (Lam, 2005). Model checking will be explained in the following section.

2.2.6 Model-Based Safety Analysis (MBSA)

Classical methods like FTA are usually performed by safety engineers based on information synthesised from different sources such as informal design models and requirements documentation (Joshi *et al.*, 2006). Model-Based Safety Analysis (MBSA) is a safety analysis approach that is based on introducing semi-formal and formal models in the design and assessment process. Model-based safety development is based on the construction of the formal specification of the system model, which is subsequently used as the foundation for various development activities like visualisation and code generation (Heimdahl, 2007; Joshi *et al.*, 2006).

Tool support and automation of safety processes can be put into practice, through MBSA. This has the potential to reduce the time, effort and the responsibility of developers to deal with tiny computational details. Besides, safety analysis in MBSA can be performed corresponding to system development, which allows the design to be focussed on functionality as well as on safety. The two most common examples of MBSA are compositional safety analysis (e.g. Hierarchically-Performed Hazard Origin and Propagation Studies (HiP-HOPS)) and behavioural safety analysis, which mainly employs model checking to assess the satisfaction of safety requirements (Sharvia, 2011).

In the compositional approaches, the system utilises safety information from the system's components to analyse the system's failure behaviour. While in the behavioural analysis, formal verification techniques are uses to perform the analysis.

2.2.6.1 Behavioural MBSA Methods: Model Checking

Model checking was initially developed to solve Concurrent Program Verification problem (e.g. Clarke, 2008). It is an approach for formal verification where models are checked for meeting certain specifications. Such approaches have the potential to determine if a certain condition can occur during the system's operation or not through the evaluation of all system's states. This helps to ensure that all errors are replicated.

Model checking has many advantages including the automation and has the disadvantage of the extensive use of memory and long runtime to reach the verification decision (Lam, 2005). Moreover, the number of states that need to be evaluated can be very large, which is referred as **state explosion.**

For example, the Spin model checker is an automated tool with a simple specification language (Promela) that is used for analysing Petri nets. Moreover, the Altarica language (Arnold *et al.*, 1999) helps users to formally specify both the nominal and failure behaviour of a system. This specification can then be analysed using a provided tool set in several ways.

2.2.6.2 Compositional MBSA Methods: Hierarchically-Performed Hazard Origin and Propagation Studies (HiP-HOPS)

HiP-HOPS is a compositional MBSA tool that was initially proposed by Papadopoulos and McDermid (1999). It is a state-of-the-art technique that has been prominently used in mechanical systems to effectively identify weak points in the system design. It automatically generates fault trees from functional models and analyses them to produce FMEA. In other words, it is a predictive safety analysis technique that integrates and automates a number of classical techniques.

To begin with, the analyst builds the functional architecture of the system and expresses the local failure information for each function, which explains how each component function can fail. Then HiP-HOPS takes a failure in an output function and moves backward to find all failures from other functions that contribute to this particular output failure. In other words, HiP-HOPS investigates how the component failures propagate through the system architecture or the system topology to produce sets of reliable fault trees that determine how a system failure (top event) can be caused by internal failures or their combinations. This method also captures the hierarchical structure of the system and equips designers with comprehensive information about how the system under analysis can fail, which helps to improve its design.

The analysis can be done in a qualitative step and a quantitative step. The qualitative step is performed to identify the MCSs, while the quantitative analysis calculates the probability of the top event. The qualitative FTA results are summarised in an automatically generated FMEA table. The FMEA table shows the direct effects of potential internal component failures of all functions in the model towards the output function. In addition to the direct effects, so-called further effects (effects of a functional failure when it happens in combination with failures from other functions) are also shown, which gives an advantage over traditional FMEA tables, which show only the direct effects.

HiP-HOPS can work with many system modelling tools or packages (e.g. Matlab Simulink (Dabney and Harman, 2001), Eclipse-based UML tools and Simulation X). Failure editors can be integrated with these modelling tools to allow the system analysts to annotate the components of the model with the failure expressions. There is a fully integrated interface from Matlab Simulink to HiP-HOPS.

Therefore, HiP-HOPS includes three main phases: a modelling phase, a synthesis phase, and the analysis phase where MCSs and FMEA are generated. In the modelling phase, as explained above, analysts build a model of the system and annotate its components with detailed failure information that describes how the component fails and links this failure with other component failures in the system. Internal failure information can be annotated into the components as a set of expressions that are manually added to each component to describe how failures of the component output can be caused by a combination of input failure and/or by internal malfunctions of the component itself. This failure annotation step can be considered as the most critical step as it is a manual step and it is at risk of using inappropriate failure data.

In the synthesis process of the fault tree, HiP-HOPS combines the interior failure data for different components and subsystems to indicate the ways that each component failure propagates from one component to another on its way to affect the system output. This leads to constructing a set of organised fault trees which specify the root causes of the failure of a system output (Papadopoulos *et al.*, 2011).

In the analysis phase, analysis of the synthesised fault trees is completed, the data is combined to result in FMEA and a qualitative analysis is accomplished to find a list of MCSs. As mentioned earlier the FMEA shows both direct and indirect effects of failure modes on the system and presented in tables that can be practically displayed through a web browser.

The following figure provides an overview of HiP-HOPs:

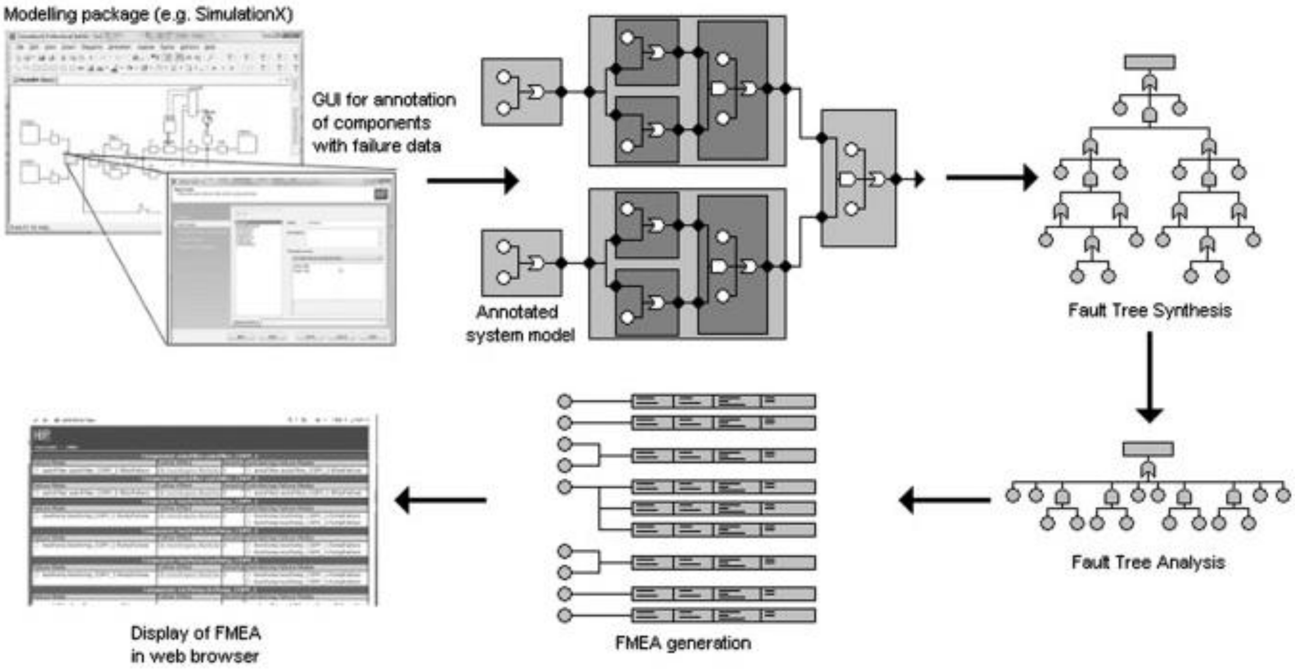

Modelling package (e.g. SimulationX)
GUI for annotation of components with failure data
Annotated system model
Fault Tree Synthesis
Fault Tree Analysis
FMEA generation
Display of FMEA in web browser

Figure 5 Overview of HiP-HOPS (Papadopoulos *et al.*, 2011, pg. 596)

To conclude, HiP-HOPS is a flexible model-based safety analysis technique, which has the potential to provide a dependable, effective and robust model through the design and analysis process. In other words, possible design flows can be detected early before they become serious problems.

2.2.7 Discussion

HiP-HOPS has the advantage of producing safety artefacts (FTA and FMEA) which are meaningful to safety engineers. Moreover, it is easy to understand and has the potential to guide the redesign process. Classical methods like FTA and FMEA have some limitations that are addressed and overcome in HiP-HOPS where FTA and FMEA are automatically generated and analysed from a system model in a hierarchical approach. This enables the analyst to determine the further effects of a component failure when it occurs in conjunction with other failure modes.

HiP-HOPS as a tool is suitable to be applied on functional block diagrams, engineering representations, piping and instrumentation diagrams, hardware descriptions, data flow diagrams, and other models commonly used in engineering and software engineering (Papadopoulos *et al.*, 2006).

HiP-HOS has been developed and tested on several industrial systems (Papadopoulos *et al.*, 2006). Moreover, unlike static methods that are unable to capture the dynamic behaviour of systems, HiP-HOPS has extensions to provide the capabilities to enable the analysis of temporal fault trees and FMEA and support assessment of sequences of failures (Walker, 2009). Furthermore, it has been extended to enable multi-objective optimisation (Parker, 2010).

Petri nets have the advantage of having formal, mathematical representation with a well-defined syntax and semantics (Gehlot and Hayrapetyan, 2001). Petri nets also were extended with colours to address some of the shortcomings; for example, models often become very large because of the absence of data concepts for the modelling and analysis process of basic Petri nets. This extension can as well overcome the inability of simple Petri nets tokens to model the attributes of an object (van der Aalst, 1993).

The following table summarises the main positive and negative points of each technique.

Technique	Fields of normal Application	Positive Points	Negative Points	Clearness of the steps
FTA	One of the most widely used safety analysis techniques in many industries	FTA has the ability to reflect the logical combinations of software, hardware, and human errors Has a qualitative step and a quantitative step The identification of MCSs in a fault tree helps the designer to focus on the design weak points The concept is easy to learn	Can be difficult to construct and complicated for systems that are more complex. Redesigning the system means that the entire FT must be reconstructed and reanalysed.	Depends on the abilities of the analyst No well-defined rules
FMEA	Evaluation of system design from safety perspectives Still employed for hazard identification and relating causes of failure to their effects.	Early identification of potential failure modes and their impact	Relies heavily on human perceptions and experience Requires a team of professionals where personal issues could make the analysis process more complicated There is a danger of not recognizing all failure modes Considers only single failures (e.g. not common mode failures) Not a systematic approach	Depends on the abilities of the analyst No well-defined rules

Petri Nets	manufacturing, production, networks, software design, software specifications, and simulation Extended to allow safety analysis of safety critical systems	Have a formal, mathematical representation with a well-defined syntax and semantics. Petri nets extended to address the negative points like hierarchy concepts.	There are no data concepts and hence the models often became excessively large. There is no hierarchy concept in the basic Petri nets.	Depends on the analyst's ability
Bayesian Networks	Safety analysis Primarily used for quantitative analysis Robust probabilistic method of reasoning under uncertainty	Can be used to capture uncertain failure behaviour. Quantitative analysis in BNs is independent of component's failure rate distribution. Both forward and backward analysis can be performed in a system model.	Building BNs can be a challenging and laborious task	No well-defined rules to create BNs models for safety analysis purposes
HiP-HOPS	Safety analysis of mechanical systems. Tested on different industrial systems.	Allows a degree of automation in the analysis. Producing safety artefacts (FTA and FMEA). Easy to use and understand. Can guide the redesign process.	HiP-HOPS struggles to model systems in which failure behaviour	

	Suitable for analysing many models in engineering and software engineering	Capable of perform analysis at subcomponent level and to provide some reuse. Determines direct and further effects of a component failure. Extended to enable multi-objective optimisation and dynamic behaviour. Makes use of an early architectural design model of a system to perform the analysis, which saves time, effort and cost.	is dependent on the sequence of events and the extension that allows assessing the sequences of failures (dynamic behaviour) is still limited.	

Table 1 Positive and negative points of safety analysis methods

2.3 Patient Safety and Safety Analysis in Healthcare

Risk management of healthcare activities, the issue of patient safety, prevention of medical errors, and reporting of adverse events are now broadly studied due to the growing number of adverse events in healthcare. A report in 1999 entitled "To Err is Human: Building a Safer Health System" which was released by the Institute of Medicine (IOM) stated that errors cause between 44000 and 98000 deaths every year in US hospitals and over one million injuries (Kohn *et al.*, 2000). Moreover, around 425,000 patients (5% of the total) admitted to hospitals in England and Wales each year experience adverse events from medical errors (Ruffolo *et al.*, 2007). In addition, many physicians experience significant emotional distress and job-related stress following serious errors and near misses (Waterman *et al.*, 2007). Hospitals' reputation can be harmed as well because of medical errors and adverse events (Thomas and Petersen, 2003).

Failing to produce the planned clinical service, producing it in the wrong way, not producing it at all or producing it with side effects that are not related to the patient's medical conditions can cause adverse events. Leape *et al.* (1993) categorised adverse events as treatment (for example, carrying out the inappropriate procedure), diagnostic (for example, failure to act on results of radiology or lab tests), preventive, and other (for example, application or equipment failure).

Hazards are circumstances that can cause harm. The probability that a specific adverse event will happen in a particular time or because of a certain condition is defined as the risk (NHS, 2007). Therefore, risk is the combination of probability and result of a hazard being recognised, and a clinical risk or healthcare risk is the chance of an adverse outcome resulting from clinical investigation, treatment or patient care (NHS, 2007). Once a hazard is triggered, it can lead to an adverse event (ACCIRAD, 2013). In other words, a hazard indicates a thing (which could be human, equipment, application, a task or a process) that is likely to cause harm or damage if it is not controlled properly. The probability of this hazard leading to an adverse event is called risk.

Because of its dangerous consequences, patient safety is considered the main domain of quality in healthcare and is defined as the freedom from accidental injury (Kohn *et al.*, 2000a; Hughes and Mitchell, 2008). Identifying threats to patient safety and avoiding their occurrence through implementing barriers will have a positive impact on the quality of healthcare. Moreover, giving this attention to patient safety by hospitals leads to improvements in their ranking and encourages patients to choose them because they support their safety.

All over the world, the issues of patient safety, prevention of medical errors, and reporting of adverse events are challenging and broadly studied research topics that motivates and inspires the computer science research community (Ruffolo *et al.*, 2007). In practice, adverse outcomes and sometimes failures in healthcare are reviewed in injury and death meetings. Many incidents are viewed during a meeting, usually within one department, which makes it difficult to resolve more general issues without having the chance to review a case in detail (Woloshynowych *et al.*, 2005).

Root Cause Analysis (RCA) is one of the widely used approaches in healthcare to analyse and investigate serious adverse events (Taitz *et al*., 2010). It has the potential to help different professionals, experts and patients to work together and to develop a detailed picture of why things went wrong and what should be arranged to address those problems and improve patient safety. Therefore, it is used to address problems after they occur and has become an important tool to prevent adverse events from re-occuring. It is possible to use FMEA through RCA to find out what should be undertaken for improvement.

Taitz *et al*. (2010) concluded that the final output of a RCA process may not in fact achieve the desired patient safety improvements.

CORAS is a model-based risk assessment that combines complementary risk assessment methods for assessing different models for the target evaluation. Moreover, it provides methodology to support the documentation of risk assessment results (CORAS, 2000). It was the output of a research and development project under the European Information Society Technologies Programme, which ran from January 2001 to 2003 and aimed to produce an improved methodology for precise risk analysis of security critical systems. Stathiakis *et al.* (2003) identified the importance of risk analysis in medicine as medical information has a direct effect on patient safety. They used CORAS to assess the cardiology eHealth service and for the implementation of security controls and mechanisms.

Wreathall and Nemeth (2004) stated that illness or death that come from medical errors require a better understanding of healthcare as a system. They used Probabilistic Risk Analysis (PRA) (Bedford and Cooke, 2001) for identifying and evaluating risk in high-hazard applications and found that it has the potential to improve patient safety efforts in healthcare. PRA is a comprehensive method to evaluate risks associated with complex engineered technological systems.

Furthermore, to reduce patient safety risks in healthcare Raheja and Escano (2009) used FTA to analyse a failure where a patient with hypoventilation (on mechanical ventilation) is receiving the wrong frequency of breaths from the ventilator. They considered FTA as a powerful tool for patient safety, and they claimed that it could be expanded to risk prediction and mishap probability analysis. FTA also was effectively used by Ong and Coiera (2010) to study the execution of redundant processes during inpatient transfers to radiology, and how they affect errors during the transfer process. They explored the use of a classical safety analysis method for modelling error detection in the transfer process, and provided guidance for system improvements.

Healthcare FMEA is a qualitative method for detecting and correcting errors in particular healthcare processes before they lead to adverse events (Weinstein *et al.*, 2005). It is a systematic process which stimulates systematic thinking about the safety of patient care processes and activities (Spath, 2003). In other words, it proactively identifies and reduces risk points in healthcare processes that may impede patient safety.

Healthcare FMEA was used by Burgmeier (2002) who describes the use of FMEA to redesign the blood transfusion process. In addition it was applied by Abujudeh and Kaewlai (2009) to analyse a number of common sources of errors in the radiology department. Abujudeh and Kaewlai (2009) stated that the adoption of health care FMEA into the radiology department in the form of a radiology FMEA has facilitated the prospective assessment of a number of radiologic processes, helped in determination of risks related to radiologic care, and aided in development of solutions and preventive actions. However, this methodology is not particularly different from the classical FMEA that is discussed above.

To sum up, classical safety methods like FTA and FMEA have a wide use in exploring and analysing issues related to patient safety (e.g. Ward *et al.* (2007); Ekaette *et al.* (2007); Abujudeh and Kaewlai (2009); Thornton *et al.* (2011); Castiglia and Giardina (2011)). They showed their ability to analyse clinical processes, and can be seen as powerful and helpful techniques for the safety analysis of clinical workflows. However, FTA and FMEA are typically performed for analysing distributed cases without affecting the design of service delivery process. Patient safety should focus on the design of the service delivery process instead of reacting to adverse events and analysing them. Moreover, using FTA and FMEA to analyse clinical processes is dependent on the analyst's ability to determine the top event, and its application is usually tedious. The healthcare environment in general has become ever more complex; many new systems and different parties are involved. Different systems' components interact with different agents. Thus, using classical analysis such as FTA and FMEA becomes increasingly inflexible.

The lack of systematic methods for the development process, the management of the design models and handling of safety analysis separately can cause problems. Moreover, implementing safety analysis in a manual process is time-consuming and can suffer from the absence of consistency and accuracy. Undertaking FTA and FMEA by means of automated analysis would provide more efficiency for analysing healthcare processes.

To conclude, controlling adverse events needs the planning, managing, and control of activities and operations within hospitals. This management requires a thorough understanding of systems in hospitals, detailed information about the internal interactions within these systems and in-depth information about the interactions between these systems and other parties in the hospital. Therefore, the flow of patients' information and the flow of the work to deliver a clinical service need refined models to reflect the complexity, resources and interactions.

2.4 Workflows and Clinical Workflows

A workflow defines the activities planned to accomplish a process, the order of invocation of activities, the conditions under which such activities must be invoked, and the synchronization and information flow (dataflow) between activities (Belhajjame *et al.*, 2001). Business process re-engineering uses the term workflow to refer to the process involved in arriving at a given objective, which can be completed only through certain steps, and handled by more than one person (Ouvry, 2002). Therefore, workflow can be understood as an explanation of a process model, and management of automated and manual tasks of business rules (Fischer, 2001).

Referring to these workflow definitions, the thesis defines the term clinical workflow as the set of tasks that are performed rigorously by more than one participant to accomplish a set of clinical processes (e.g. treatment or diagnosis) and to produce a certain clinical output.

Healthcare processes have both medical and non-medical activities which can be considered within a particular workflow; both types include potentially high-risk activities and failure in any part may lead to catastrophic consequences (Ruffolo *et al.*, 2007, Miller and Hegi-Johnson, 2012). Medical activities can be treatments, drug administration and guidelines, which may have an inflexible method of manual process management. This inflexibility means that particular agents must execute the tasks within processes accurately and in a particular order. In other words, a healthcare workflow includes medical and administrative activities that are executed to produce a clinical service; deviations in these activities have the potential to deliver a faulty service.

The continuous application of information technology in clinical practice has the potential to improve the healthcare system; however, it introduces new types of risks and threats that are critical to patient safety. This is due to the construction of complicated systems and sophisticated human interactions that lead to complex workflows. Therefore, healthcare delivery requires improvements, continuous traceability of all care activities, reduction of variations in practices besides the detection, and measurement and prevention of adverse events occurring during healthcare delivery (Hannan, 1999).

Thus, clinical workflows are critical to patient safety; accordingly, the thesis terms them as safety critical workflows because they are in many aspects similar to safety critical systems, especially in that both have various conditions that must be controlled carefully and both require the consideration of their safety from the early stages of their development. Moreover, their operational deviations have the potential to lead to catastrophic consequences or loss of human lives.

Clinical workflows incorporate numerous components and employ complex human interactions. Therefore, the development process of such workflows should not be random; a systematic and organised set of steps to be followed is required. The workflow must be designed and analysed for its safety in order to produce a safe and dependable theoretical workflow that has the potential to operate as safely as possible. Such safety in the operational phase of the workflow means that it should not cause adverse events when it runs. Before discussing the issues related to safety of clinical workflows, workflow management and modelling and their importance in the development and analysis of clinical workflows are discussed in the following sections.

2.5 Workflow Management and Workflow Modelling

The field of workflow management provides logistical management of business processes to ensure that organisations carry out the right activities by the right people at the right time. The software implementations that are used to support the management of such workflows are called Workflow Management Systems (WFMSs) (van der Aalst, 1998). A WFMS is a system that defines, creates and manages the execution of workflows through the execution of software (Workflow Management Coalition, 1996). Van der Aalst (1998) pointed to the fact that most people associate workflow management with workflow management systems even though it is possible to do workflow management without using a workflow management system. This thesis is concerned with workflow management rather than WFMSs; however, the analysis and modelling have the potential to help in the design of WFMSs.

Workflow modelling is the basis of workflow management technology; the correctness of the workflow model is the key to determining the success or failure of workflow management systems (Cai, 2012). This is because supporting the definition, execution, registration and control of processes is the main purpose of a workflow management system (van der Aalst, 1998). When it comes to the process modelling, there is always a dilemma between simplicity and appropriateness; while a model should be rich enough for designers to say what they need to say, it should be simple enough to be understood (Ward, 1986). The simplicity is related to how easy it is to generate and read models and the appropriateness is about how well the characteristics of the process are represented (Jun et al., 2005).

Workflow modelling can be helpful in defining the workflow specifications that can set the functional representation of a workflow. Kwan and Balasubramanian (1998) pointed out that workflow models can address different perspectives like functional, organisational, informational, behavioural, or metric perspectives. These different perspectives can produce different models; for example, a data flow model explains how the data is used and processed within the workflow, an architectural model shows different components and their interrelationships and behavioural models explain workflows' behaviour, like the sequence of activities and the constraints on them.

The workflow model must specify the systems involved within the workflow, humans interacting with these systems, and the way they are interacting in order to produce a service. Moreover, the flow of data and the sequence of events must be identified. Consequently, designing, analysing and generating the workflow at the conceptual level is required. Workflow models should have all the processes required to produce the service, the tasks included within these processes, and the resources required to accomplish each process.

2.6 Workflow Modelling in Healthcare

Workflow modelling in general is widely recognised as an indicator for quality improvement because the efficient modelling of business processes has the potential to improve the quality of services and products provided by organisations (Smart Cities Project, 2011; Jun *et al*., 2009). As mentioned previously, clinical workflows are safety critical, and therefore, the ability to analyse their safety is important to produce high quality models. The following sections describe popular techniques of business workflow modelling which have been used within the healthcare context.

2.6.1 Flow Chart Technique

A flowchart (flowchart and flow chart are used interchangeably) is a diagram through which operations, data flow and equipment are symbolised to illustrate, define and analyse a problem (Lakin, R., *et al.*, 1996). Flowcharts appear in the literature under different names, including process flowchart, functional flowchart, process map, process chart, functional process chart, business process model, process model, flowchart diagram, and business flow diagram.

Using flowcharts to model business processes is a common technique because of their simplicity and flexibility. Moreover, a flowchart can be beneficial for process modelling as it has the potential to help in clarifying and understanding complex processes and identifying the detailed steps that are included. The flexibility of flowchart modelling allows a process to be described in different ways and the simplicity makes them easy to be developed and understood. However, this may produce unclear process margins because its rules give the designer the choice of putting different building blocks together (Aguilar-Saven, 2004). In addition, it is difficult to connect processes with their actors, as there is no regular or standard way to do this, which creates a deficiency for using the flowchart method for process modelling.

Flowcharts can be helpful for modelling simple workflows that do not have many details, but once the model has lots of processes and tasks, and once it needs in-depth presentation of processes, tasks flow charts usually begin to show their deficiencies. They have been used to model healthcare processes as an initial step to apply healthcare FMEA (e.g. Weinstein *et al.* (2005)).

It is well known that clinical processes have many details and data flows as well, which may create huge flowcharts when using them to model clinical workflows. The following diagram shows an example of a simple clinical process model using a flowchart:

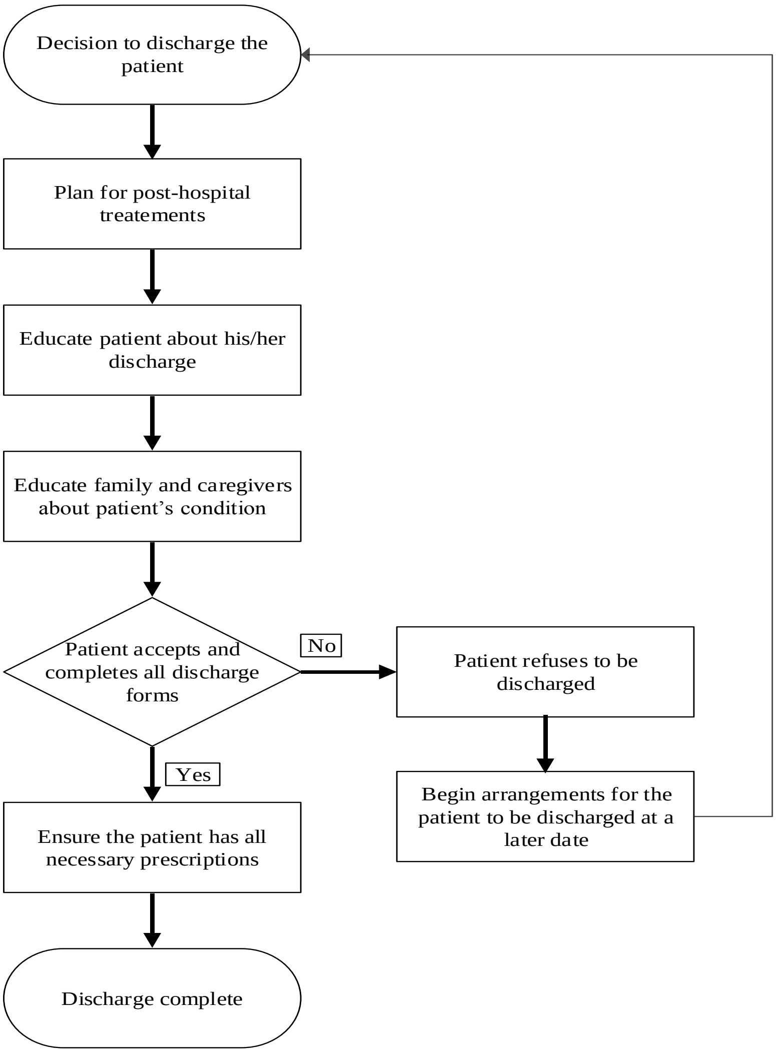

Decision to discharge the patient
Plan for post-hospital treatements
Educate patient about his/her discharge
Educate family and caregivers about patient’s condition
Patient accepts and completes all discharge forms
No
Patient refuses to be discharged
Begin arrangements for the patient to be discharged at a later date
Yes
Ensure the patient has all necessary prescriptions
Discharge complete

Figure 6 Flowchart for modelling of clinical process modelling

The process starts when a clinician makes a decision to discharge the patient, then he/she sets the plan for the post-hospital treatment and the patient is educated about his/her discharge. After that, the patient’s family are educated as well and the patient has the option to accept the discharge or not. If the patient accepts the discharge, then the healthcare team must make sure that the patient has all the necessary prescriptions and the discharge is completed. Otherwise, if the patient refuses to be discharged, the healthcare team must begin arrangements for the patient to be discharged at a later stage.

The example shows a simple clinical process, and it can be concluded that flowcharts are able to represent simple processes. However, it is possible to encounter complex workflows containing many clinical processes that cannot be easily represented by a compact flow chart. Moreover, it can be seen that it is not possible to show the dataflow or the tasks and actors; although actors can be shown informally next to the process, interactions between the actors themselves and actors and other components cannot be shown. Therefore, flowcharts are able to describe some aspects of workflows, but they have to be complemented by further diagrams to describe the other aspects. Nonetheless, flowcharts are easy to understand by healthcare practitioners and can be used as an initial step by the workflow analyst to understand the initial workflow and to start building other types of workflow models.

2.6.2 Role Activity Diagrams (RADs)

Role Activity Diagrams (RADs) are graphical interpretations of the process from the individual roles perspective, concentrating on the responsibility of roles and the interactions between them (Holt *et al.*, 1983). Roles in RADs are used to describe organisational functions, software systems, customers and suppliers. Each role enacts an individual who performs a set of activities to achieve an objective or many objectives, and roles interact with each other where an interaction is essentially some coordination between roles (Patel, 2000). The following diagram shows an example of using RAD to model healthcare processes:

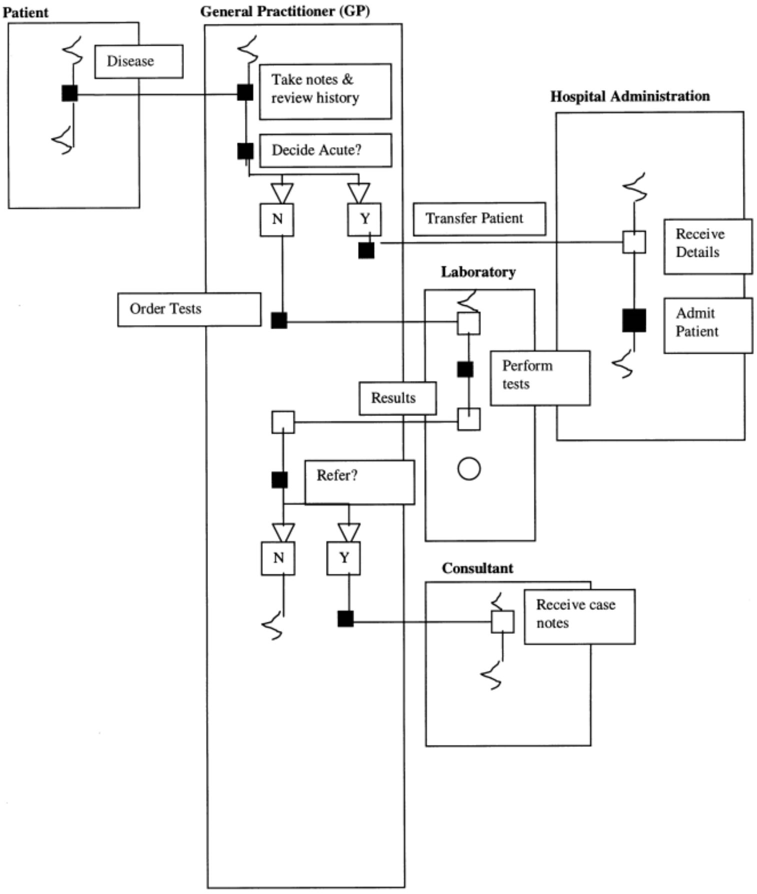


Figure 7 RAD for modelling of clinical process (Patel, 2000)

As can be seen from the example, RADs are easy to construct, read and understand and they have the potential to show a detailed view of the workflow and how processes within the workflow interact with each other. However, the technique excludes business objects (such as machines or products) and instead shows the workflow as a sequence of activities (Aguilar-Saven, 2004).

The main deficiency of RADs is that they exclude business objects, and in the case of clinical workflows, excluding such objects means excluding core objects manipulated by clinical processes, for example, excluding machines involved in the workflow. In effect, the supporting architecture of the workflow is not represented. Moreover, for the analysis of workflow safety, excluding such objects means ignoring their internal errors, which may propagate causing failures for the produced clinical service. Finally, manual analysis processes like RAD require a great deal of time and effort to perform.

2.6.3 Data Flow Diagrams (DFDs)

Data Flow Diagrams (DFDs) are those diagrams concerned with showing the flow of data and information. They describe how different processes are linked to each other through data stores as well as how these processes are connected to different users and to the system environment. DFDs are used to specify what processes are expected to do and to define processes at the analytical level.

Thus, they are concerned with what the process will do rather than how it will be done. DFDs are easy to develop and to understand, and to show how more detail processes can be broken down to describe sub-processes at a lower level (Aguilar-Saven, 2004). However, DFDs are found to be the least used modelling type in healthcare and they are considered not very helpful in understanding general care delivery processes which are not usually data-driven (Jun *et al.*, 2009). The following example shows the use of DFD in modelling a simple clinical workflow:

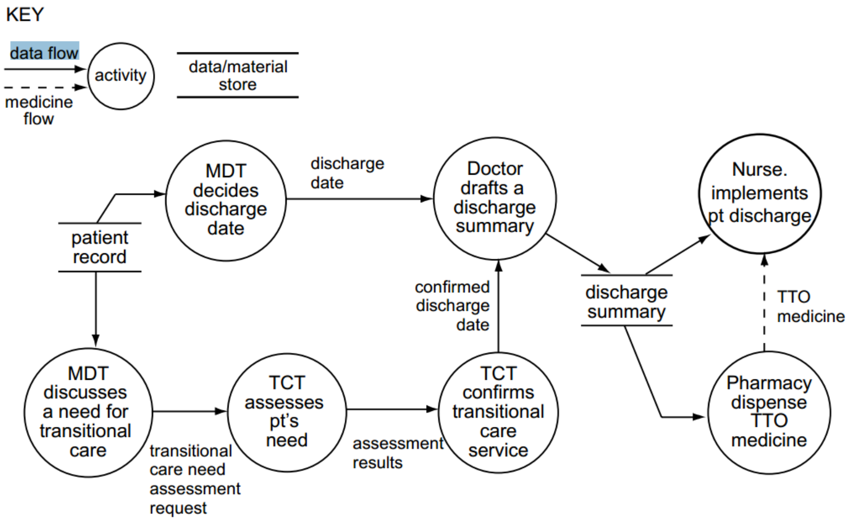

KEY
data flow
activity
medicine flow
data/material store
patient record
MDT decides discharge date
discharge date
Doctor drafts a discharge summary
Nurse. implements pt discharge
confirmed discharge date
discharge summary
TTO medicine
MDT discusses a need for transitional care
TCT assesses pt's need
TCT confirms transitional care service
Pharmacy dispense TTO medicine
transitional care need assessment request
assessment results

Figure 8 DFD for modelling of clinical workflow (Jun *et al.*, 2009)

2.6.4 IDEF

The Integrated Definition (IDEF) is a collection of methods that support a standard which has the ability to meet the modelling needs of an enterprise and its business processes (IDEF, 2003). IDEF was initially developed by the US Air Force (USAF) at the end of 1970 within an Integrated Computer Aided Manufacturing (ICAM) project in order to improve manufacturing operations by using information technology. The requirement to model activities, data, and dynamic (behavioural) elements of the manufacturing operations resulted in the initial selection of the Structured Analysis and Design Technique (SADT), which is a complete methodology that can be used as a regular approach to analysing an enterprise. The IDEF family is used according to different applications. The most important parts are IDEF0, IDEF1, IDEF2, IDEF3, IDEF4 and IDEF5. For business process modelling the most useful versions are IDEF0 and IDEF3 (Aguilar-Saven, 2004).

IDEF3 is the IDEF for the process description capture method that is used to capture information about how systems work and can be considered complementary to IDEF0 (Mayer *et al.*, 1995). Mutic *et al.* (2010) used IDEF0 to model several functional areas of a teaching radiation oncology department, and they demonstrated that IDEF0 can be used by healthcare professionals to model their clinical operations. IDEF0 is found to be similar to DFDs (Jun *et al.*, 2009) and it can be considered a well-structured method to represent healthcare processes. However, it needs a lot of time and concentration, which healthcare experts would not have.

2.6.5 Petri Nets

Petri nets - as explained in section 2.2.3 - are a graphical method that uses some basic symbols for describing relations between conditions and events and can represent and analyse the dynamic behaviour of the system (Liu and Chiou, 1997). They are well-established and rigorous mathematical models, which are prominently used for workflow modelling (e.g. van der Aalst (1998); Eshuis and

Dehnert (2003); Liu *et al.* (2002)). Petri nets benefit from the availability of many tools to support their modelling, analysis and simulation.

Liu *et al.* (2002) used coloured Petri nets as a formal language for workflow process definition, and proposed a workflow coloured Petri net to extend the workflow net. Pettit and Gomaa (2000) presented an approach for using coloured Petri net segments to model the dynamic behaviour of concurrent object architectures expressed in UML by using a synchronised architecture and coloured Petri net segments. An engineer can continue with behavioural analysis by first mapping the UML architectural elements into a coloured Petri net representation. The resulting coloured Petri net is then used to validate such dynamic properties as the absence of deadlock and starvation conditions. It also helps in providing a timing analysis of the architecture through simulation. This analysis through coloured Petri nets reduces the overall risk of software implementation by allowing behavioural characteristics to be validated from an architectural model rather than waiting for the system to be coded.

Bertolini *et al.* (2012) argued that even though Petri nets can be used for describing workflow processes, since they can be visualised in a graph notation and they can provide the mechanism of sequencing and choice which distinguish the routing of tasks of workflows, Petri nets have a number of disadvantages and limitations. These are summarised below:

1. Petri nets lose track of the relations between resources and their functionalities.

2. At the same time, where tokens are used as enabling conditions of transitions, cases are modelled as tokens. Cases in the workflow are the subject of an operation, for example, patient admission. Modelling cases as tokens do not allow tokens to distinguish the copies of processes of cases of the same and different kinds. In addition, this modelling makes it difficult to relate the dynamic behaviour to the statics relation between cases.

3. Petri nets do not have the capability to express the data flow, which is needed for sharing health information and care resources. For this purpose, Petri Nets are extended with colours, which complicate the understanding of the models.

4. Petri nets are not able to provide an architecture description representation. Therefore, they do not support compositional reasoning and verification. Moreover, they do not support algebraic reasoning and derivation of workflow, which are frequently important for understanding and judgment of the accuracy of workflow with the need of semantic-based verification.

To sum up, this section and section 2.2.3 show that although Petri nets can support behavioural analysis and reasoning they are not able to support the necessary compositional reasoning and verification, although this problem can be overcome by generating Petri nets from UML architecture models as in (Liu *et al.*, 2002). Therefore, analysis using coloured Petri nets has the potential to allow validating behavioural characteristics from architectural models. The hierarchy and colour are two modelling concepts that have the ability to improve the model.

Coloured Petri nets have a formal, mathematical representation with well-defined syntax and semantics and their behaviour can be analysed, either by simulation or by formal analysis methods (Aguilar-Saven, 2004). Moreover, coloured Petri nets incorporate hierarchical decomposition. However, coloured Petri nets can produce large and complicated nets, which are too complex if they are used for workflow representation.

Consequently, workflow models that are created using basic Petri nets may not reflect all the characteristics of the actual workflow, especially the architectural characteristics. Petri nets are often said to lack compositionality and scalability; these problems have been addressed by ‘higher-level nets’, such as Object-Oriented Petri Nets by Patkar *et al.* (2008) who think that Petri nets could be an important candidate for designing and implementing clinical services in the future.

2.6.6 Unified Modelling Language (UML) Based Workflow Modelling

Unified Modelling Language (UML) (Bastos and Ruiz, 2002) is a standard object oriented modelling language that can be used to identify, document and construct objects of software systems and for modelling of business processes. Using UML for workflow modelling can be user-friendly with the extension mechanism; however, the concept used to describe it is still incomplete and is not sufficiently clear (Cai, 2012).

UML has the potential to offer many symbols to specify complex concepts because it is rich with syntax and semantics. However, it is useful to remember the importance of using simple annotations since it is easier to be understood by the others (Schedlbauer, 2007).

UML contains different diagrams. Each of these diagrams may show the static or the dynamic features of the system. Static diagrams that show the static structure of the system include Class Diagrams (which define the structure of the system) and Object Diagrams (which state possible combinations of specific class diagrams) (Bouchet, 2007) . Those that demonstrate the dynamic behaviour of the objects in the system include State Chart diagrams (that express potential states of system classes and can be considered as extensions of classic state machines), activity diagrams (that represent events and activities which happen in a system) and sequence diagrams (that show how processes work and what is their order).

Inverardi *et al.* (2005) provided an extensible UML-based notation for software architecture modelling and analysis. Although UML diagrams have the advantages of not being specific to any software or technology and have the advantage of being a visual language, it can be a complex modelling technique, due to having many diagrams and extensions for analysis purposes.

2.7 Challenges of Workflow Modelling in Healthcare in Comparison to Industry

For a modelling technique to be accepted by the healthcare industry, it must be easy to learn, logical in its formulation and supported by available commercial computer programs (Mutic *et al.*, 2010). Moreover, valid models should show the structure that correctly represents the connection between the inputs, outputs and internal variables.

The above sections describe some of the deficiencies in currently used modelling techniques. Another major deficiency in them is the separation between the process-modelling tool and the analysis tool that allow the analysis of interactions and analysis of the data flow within the model. To overcome these issues, the next chapter outline an integrated approach to workflow modelling and analysis — SAFE-FLOW — that has been developed to support the modelling and analysis process of such workflows.

Modelling and analysis of workflows within healthcare institutions have the potential to provide clinicians with the ability to define and understand their internal and external healthcare procedures (both clinical and administrative) through a workflow diagram, which gives the institution the ability to interconnect and symbolise these procedures in a formal manner. This would also help in visualising the workflow in a manner that makes the detailed tasks available for practitioners. Clinical workflows must be able to deliver clinical services as safely, proficiently and effectively as possible (Bertolini *et al*., 2012). However, workflow modelling in healthcare can be a subjective task due to the absence of precise structure for healthcare workflows and the lack of the information necessary to create the models.

In general, healthcare processes are complex, as they need decision making, communication and information sharing that take place asynchronously across multiple providers (Rossi and Turrini, 2006). In other high-risk industries (e.g. nuclear and chemical) it is generally easy to define a state of routine operations, unlike healthcare in which this sounds difficult, because the processes of such industries are more accurate, structured and established (Woloshynowych *et al.*, 2005). The delivery of healthcare depends on a complex sequence of interactions between medical practitioner and patients (Marx and Slonim, 2003), which are difficult to model and to be symbolised. Model developers should have intensive knowledge about these workflows in order to model them appropriately. Therefore, they cannot accomplish their job without getting help from medical practitioners who are involved in the workflow, as processes in hospitals usually have the problem of being unstructured. In other words, although healthcare is similar to other high-risk industries in many aspects, the clear routine processes in other high-risk industries make the process of workflow modelling much easier than the workflow modelling in healthcare. Furthermore, in healthcare the outputs can often only be measured in a subjective way, in contrast to other industries where the outputs can be measured objectively, which again makes the modelling process in healthcare more difficult than in other industries.

To conclude, to model a clinical workflow, the model should specify:

1. the systems involved in producing the clinical service;
2. who is interacting with these systems;
3. the way they interact with each other;
4. the interactions between medical practitioners and patients;
5. what is expected from the workflow;
6. the flow of data and the sequence of events.

2.8 Evaluation Background

In Chapter 5 of this thesis, an evaluation design is established and used for evaluating SAFE-FLOW. The following sub-sections provide the background required for understanding the evaluation design.

2.8.1 Usability Testing

Usability as defined by the International Standards Organisation ACCIRAD (2013) is the level to which a product can be used by specified users to complete specified goals within a specified context with effectiveness, efficiency and satisfaction. Rosenbaum (1989) stated that there are two tools available for making judgments about product usability: usability testing and the expert evaluation. A usability test assists in quantifying to what extent the intended users are satisfied and their needs are met, and in expert evaluation, experts in usability issues assess the product's usability.

Usability testing for a product can be done in the laboratory or within its actual context or field (Kallio and Kaikkonen, 2005). Testing usability within the relevant context has the advantage of identifying problems with the product and enabling collection of qualitative data about the target audience (Dumas and Redish, 1999).

Usability testing with the participants can be considered a fundamental evaluation method (Nielsen, 1994). A typical usability test includes 6 to 12 participants (Dumas and Redish, 1999). Many researchers focused on less formal usability testing, because it is widely accepted that the value of usability testing is in diagnosing problems rather than validating results (Dumas and Redish, 1999).

Usability testing is relevant to all types of products (Dumas and Redish, 1999). Therefore, the usability of safety analysis technologies needs to be tested within the healthcare context. This thesis assumes that the application of usability principles instead of applying safety analysis technologies by itself in healthcare has the potential to provide great benefits. Moreover, it can help in finding the problems related to this application, and help in providing solutions for such problems.

2.8.2 Evaluation Frameworks

Evaluation is a process of collecting and analysing information about the activities, characteristics, and outcomes of a programme to make judgments about it, to improve its effectiveness, and/or to inform programming decisions (Patton, 1990).

There is an increasing interest in evaluation studies and in the use of appropriate methods for evaluation in health informatics (Ammenwerth and de Keizer, 2003). Ammenwerth and de Keizer (2003) identified that such evaluations are focused on two trends: moving from technical issues to human and organisational issues, and moving from an objectivist to subjectivist approach.

Yusof *et al.* (2008) investigated evaluation frameworks that have been used for evaluating Health Information Systems (HIS). They found that evaluation is a complex process; however, it is possible to consider a HIS evaluation framework with more comprehensive and precise measures that would integrate technological, human and organisational issues to enable HIS evaluation.

The US Center for Disease Control and Prevention published a framework for Program Evaluation in Public Health in 1999. The term ‘program’ here is used to describe any public health action (e.g. research initiatives or education and training services). The framework summarises and organises the steps and standards for effective program evaluation. Therefore, it provides a systematic way to approach and answer key evaluation questions which are usually derived from the purpose of the evaluation. Therefore, the framework is chosen to evaluate the use of SAFE-FLOW.

A technique or a method also can be evaluated by comparing the method with other methods used by other researchers for the same purpose. Following this can lead to help in determining the advantages of a method and specify its deficiencies.

3 SAFE-FLOW: A Systematic Approach for Safety Analysis of Clinical Workflows

This chapter proposes SAFE-FLOW: a technical approach that supports the safety analysis of clinical workflows. Before presenting SAFE-FLOW, the following section presents some of the challenges that SAFE-FLOW is intended to resolve.

3.1 Challenges in Safety Analysis of Clinical Workflows

As explained in Chapter 2, the increasing dependence on technology in healthcare combined with potential risks of failures from human interactions mean that safety becomes gradually an important factor in workflow design. Safety analysis of the workflow can help analysts to understand how workflows can fail. Faults within the workflow can lead to deviation of the service provided by the workflow. In this thesis, a failure occurs when the workflow of the system or a workflow process is unable to deliver its intended function without side effects (because even if the intended function is delivered, if it affects the patient's health then this is a failure as well). Malfunction is the failure to function normally that occurs when an element does what it is supposed to, but at the wrong time or in the wrong context (Banach and Bozzano, 2013).

Failure of a clinical service may occur when an error is propagated at the service boundary and causes the service delivered by the workflow to deviate from correct service. Service failure of a workflow may cause an external fault for the other workflows that receive service from the given workflow and thus cause another service to fail. Therefore, the safety of clinical workflows must be analysed carefully to try to minimise their potential to cause harm to patients. Furthermore, identification of adverse events (both those that cause serious injury or death and those that do not result in harm) and their causes should be targeted and evaluated in terms of the ability to introduce improvements into the delivery system. This is possible through designing the healthcare system at all levels to make it safer, and through building safety into processes of care instead of blaming individuals (Kohn *et al.*, 2000).

The chapter has also reviewed the concepts related to patient safety and the work done in analysing adverse events in healthcare. There are many approaches are in use for analysing patient safety. Some of these approaches aim at analysing past adverse events and others aim at predicting and expecting potential harmful events in order to find the current and future safety state for a healthcare organisation. These approaches contribute in improving patient safety and in representing the overall picture of it; however, the application of more advanced safety engineering methods to clinical workflows is still challenging. This is due to the characteristics of the target workflows and the efforts required for evaluating safety analysis outcomes in practice.

The need for enhancing patient safety and improving the safety of care processes has quickly developed in healthcare. However, a knowledge gap may still exist, especially in understanding the capability of various safety analysis methods and their requirements to be applied within the healthcare context.

An integrated safety analysis that considers hardware components, software components, human factors and different clinical processes is required. However, various difficulties often arise when safety analysis is applied in the healthcare domain and this can cause many problem areas. Such complications lead to obstacles that obstruct meaningful and useful safety analysis in healthcare. The major difficulties that were found in the safety analysis cases available in the literature are:

1. *Unclear safety analysis aim and purpose when safety analysis is applied to clinical workflows or clinical processes.*

   The required analysis explained previously stipulates that the integrated analysis should take into consideration the hardware, software, clinical processes and human interactions with information technology and with other humans involved in the workflow. The problem with the available work on safety analysis in healthcare is that most of the work was done to analyse different adverse events without a clear goal for the analysis. Safety analysis in healthcare needs to be a structured process in which safety analysis tools are used to reduce risk over the workflow. Woloshynowych *et al.* (2005) criticised the literature on the analysis of critical incidents and adverse events in healthcare, since most studies focused on the analysis of single or multiple incidents in many hospital specialities instead of focusing on the development of a method for safety analysis either conceptually or practically. In other words, instead of focusing on the analysis of several adverse events, the analysis should aim at finding methods to increase the safety of the workflow.

2. *Complexity of the safety analysis environment.*

   As explained previously, the lack of detailed models of the clinical workflow architecture and its failure modes often forces safety analysts to allocate much of their effort to collecting information about the workflow architecture and its behaviour, and embedding this information in the safety artefacts such as the fault trees. This is usually applied in a manual process, which in the healthcare context becomes challenging, laborious and error-prone.
3. *Lack of available information that is required for the safety analysis process.*
4. *The safety analysis process is usually done in the operational phase, when the workflow is already in operation.*

As mentioned in the first point, typically this process is done to analyse separate cases instead of analysing the workflow design model to be safe when it is in operation. The analysis results therefore do not influence the workflow design, so that potentially similar problems will be experienced in the future according to the lack of systematic methods to capture and manage the workflow design models.

All of the above stated difficulties in the safety analysis process in healthcare show the gap left for further development of systematic methods for safety analysis in healthcare. Human interactions and the involved systems within the workflow must be addressed and should be given more attention. Human failures are expected in any large organisation, which leaves the system vulnerable to this hazard for which there is no technological remedy (Reason, 1990). In this thesis, human errors are considered as an important part of the workflow safety analysis process as the analysis should focus on the operational errors and failures of workflows.

It is important to develop well-established approaches that have the potential to help in accomplishing a comprehensive safety analysis and in evaluating the conditions that lead to adverse events and patient harm in healthcare organisations. The safety analysis of theoretical workflow has the potential to help in redesigning workflows to achieve the best results that can lead to a safer and better-designed operational workflow.

Constructing a formal model for the workflow can lead to deeper understanding and accuracy of thought about the workflow and its components. It also supports the healthcare team in understanding how different tasks can affect the output of the workflow. Furthermore, considering the safety analysis all over through the workflow design process has the potential to have a positive impact on the design of the workflow.

A better job of modelling healthcare delivery is required before IT can be designed to support it (Benyoucef *et al.*, 2011). Thus, before thinking of any automation to support workflows within a hospital, the workflow should be understood, modelled and analysed. In order to produce dependable workflows, safety analysis should be an essential part of their analysis. Finding formal methods for workflow modelling and analysis that have the potential to produce official workflows to be followed by medical staff and patients is required.

For producing safe operational workflows, this thesis proposes SAFE-FLOW, a safety analysis approach that can help to improve the safety of clinical workflows. The focus of SAFE-FLOW is on the safety analysis of clinical workflows through the analysis of their components; components here are hardware, software, humans, processes and tasks. The use of MBSA in which early models for the workflow are built and analysed has the potential to help in the development of safer workflow processes in healthcare. In the standard model-based development, the focus is on building a formal description of the system model. This description produces a model that is then used as the basis for different development activities like visualization, code generation, testing or prototyping (Heimdahl, 2007). In MBSA these models are extended with the failure behaviour to analyse their safety. While the standard model-based development was originally designed for the development of software systems, it was also used for the development of hardware systems. This thesis proposes the use of MBSA for analysing clinical workflows and claims that it can be beneficial for them.

3.2 SAFE-FLOW: A Systematic Approach for Safety Analysis of Clinical Workflow

The SAFE-FLOW is developed to assist with the design and production of safe clinical workflows. It provides a systematic method for capturing clinical workflows into models and then automatically predicts how workflows can fail. Therefore, the goal of SAFE-FLOW is to capture clinical workflows in conceptual workflow models that explain and describe different components, their functions and their interactions. These models can then be used for safety analysis as early as possible in the design of the workflow. This means that before a certain department in a hospital can define an official workflow, the ideas for the workflow should be modelled and analysed. The safety analysis results can then be used to iteratively redesign the workflow in order to achieve the safety requirements. Safety analysis results can also be used to refine the models and to derive more detailed functional models and specifications of workflows. The analyst does not have to capture all the scenarios and possibilities because he/she will never finish documenting the possibilities. However, what he/she needs to do is to document the main scenario and the alternative scenario.

The focus of the workflow safety analysis must be on determining whether the workflow meets the safety requirements in the presence of component failures. Components here are hardware, software, humans, processes and tasks. Repeated analysis and redevelopment of the workflow model are performed until a qualified workflow design is achieved. A healthcare team in cooperation with a safety engineer can develop the model. After the model is developed, it must be annotated with the fault behaviour. A graphical language such as Simulink can be used for modelling.

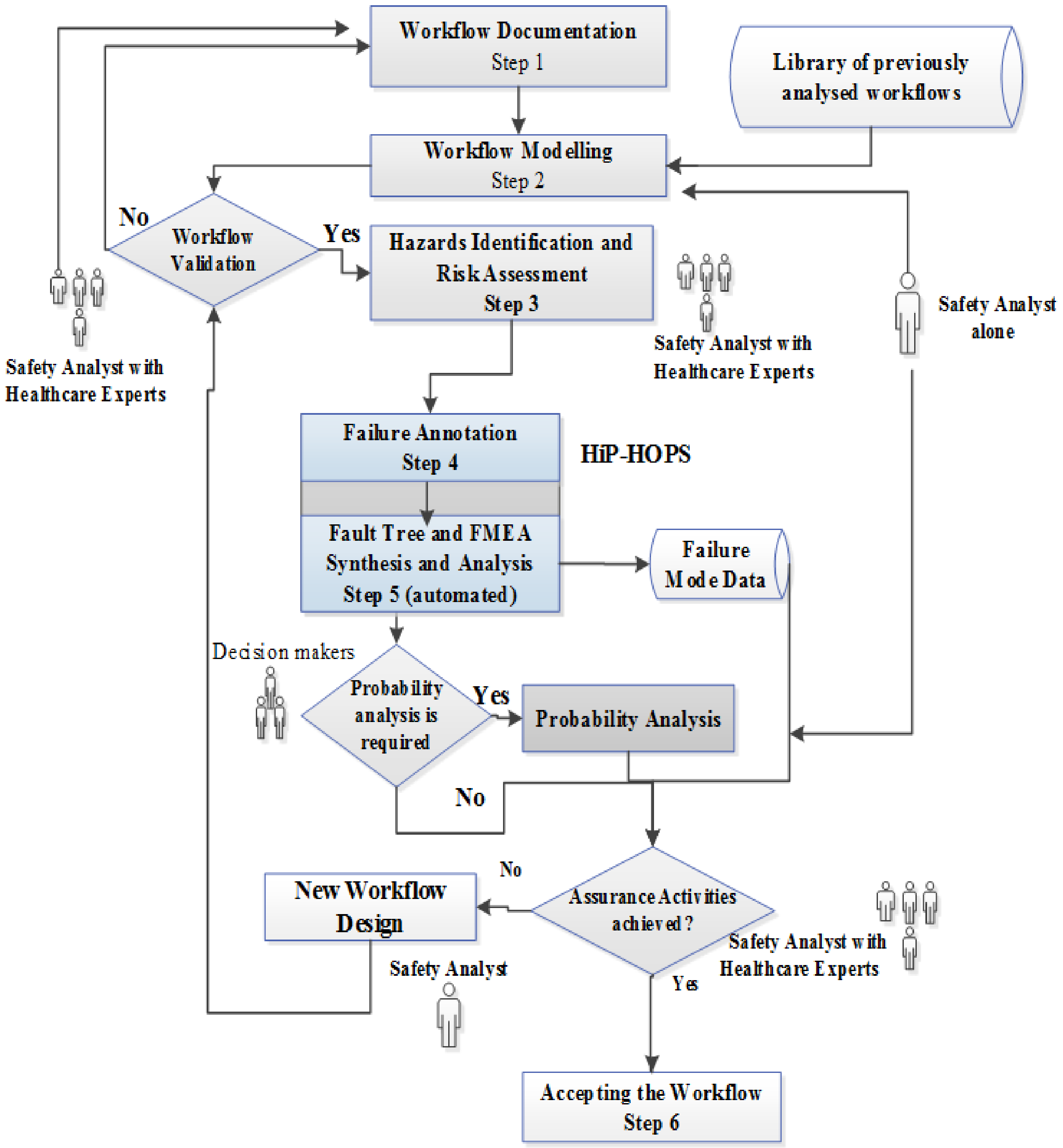
SAFE-FLOW takes into consideration the integration between the architectural design of the workflow, the applications involved within the workflow, the dataflow within the involved systems and the system environment. In other words, the interactions between the involved parties in the clinical workflow (e.g. physicians, radiologists, nurses, patients, and system environment) must be modelled and analysed in combination with other hardware and software components. Modelling these interactions and focusing on the relations and the communication between all agents for the purpose of the safety analysis helps in the holistic analysis, and can be efficient in finding preventable procedures and solutions for prospective failures.

HiP-HOPS is one of the more prevalent model-based safety analysis methods and has therefore been chosen to facilitate SAFE-FLOW because of the many advantages it offers (see section 2.2.6). HiP-HOPS can in general be applied to systems that involve data, information or material flow. However, here the “components” can represent clinical processes or components of clinical workflow architecture. Therefore, this thesis uses the capability of HiP-HOPS to analyse such components and builds SAFE-FLOW, which uses the tool to analyse clinical workflows. However, SAFE-FLOW is not limited to a specific tool and it is important to note that model-based safety analysis in general can help in analysing such clinical workflows.

The thesis explains SAFE-FLOW in detail, and demonstrates how it can be used to analyse clinical workflows. Two case studies are provided: the workflow within a Guideline Based Decision Support System (GBDSS), which is used to give recommendations for patients with Chronic Obstructive Pulmonary Disease (COPD) (Appendix A), and the workflow within a radiology department (see

Chapter 4). However, the SAFE-FLOW approach is intended to be generic and can be used to analyse the impact of software, hardware, as well as human failures in the healthcare environment.

The diagram below illustrates the outline of the SAFE-FLOW process:



Workflow Documentation
Step 1
Library of previously analysed workflows
Workflow Modelling
Step 2
No
Workflow Validation
Yes
Hazards Identification and Risk Assessment
Step 3
Safety Analyst with Healthcare Experts
Safety Analyst with Healthcare Experts
Safety Analyst alone
Failure Annotation
Step 4
HiP-HOPS
Fault Tree and FMEA Synthesis and Analysis
Step 5 (automated)
Failure Mode Data
Decision makers
Probability analysis is required
Yes
Probability Analysis
No
No
New Workflow Design
Assurance Activities achieved?
Safety Analyst with Healthcare Experts
Safety Analyst
Yes
Accepting the Workflow
Step 6

Figure 9 SAFE-FLOW: An approach for safety analysis of clinical workflows

The following sections explain the steps involved in SAFE-FLOW in detail.

3.2.1 Workflow Documentation (Step 1)

The first step in the safety analysis process is performed by a safety engineer in the healthcare organisation in cooperation with a team of healthcare experts. The safety engineer is responsible for collecting sufficient and in-depth information about the workflow components and interactions between those components that can help in modelling the workflow and its critical parts. Such components include the involved individuals, hardware and software components, processes and tasks involved in the workflow.

SAFE-FLOW recommends that the safety analyst must collect the data about a new workflow from scratch instead of using any existing models for the purpose of the analysis. However, SAFE-FLOW does permit the use of previously analysed components in this phase and in the modelling phase; this could happen if the workflow might be connected with another workflow or parts of another workflow in the hospital. An individual workflow component can be a task, a process, a software agent, human agent, hardware, or a workflow that encapsulates a set of related tasks or processes.

For human components; the processes, the tasks accomplished by them, their interactions and the information they receive or produce must be specified. For process components, each process should describe its atomic tasks, inputs, outputs and its interactions. The same is for other components, inputs, outputs, interactions and any other properties that are specified by the healthcare team, they need to be identified during the workflow documentation phase.

A proper method to document the workflow could be to ask the people who are involved in the workflow to describe the overall practice from the beginning until producing the clinical service. This will yield documentation that consists of the workflow detailed information and specifications in a natural language. Producing the right workflow documentation has the potential to create the correct models, can help in analysing atomic task related hazards, and can help to analyse human related errors.

Although this phase produces the documentation in a natural language, it can be represented using many other methods like flowcharts, UML diagrams or any other method that the healthcare team feels comfortable with. It also can be organised using a table that identifies the components, their inputs, outputs, sub-components and their interactions (other components that they are connected to). For example, the following table shows a sample of how to organise the documentation of a workflow for collecting and analysing blood sample by a nurse:

Table 2 Organising a human component example

Human Component	**Interactions**		**Information received**	**Information produced**	**Processes performed by the human component**
Nurse	**Receive from**	• **Patient (human component)**	• **Patient information** • **Test information**	• **Blood sample labelled with patient information and test information**	**Collect sample (process component)**
	Send to	• **Analyse sample (process component)**			

The table shows details about the nurse component that interacts with a patient component and send information to another process component (Analyse sample). The nurse receives patient information and test information, and then performs a process (Collect sample) to produce a blood sample and label it with both patient and test information.

3.2.2 Workflow Modelling (Step 2)

Once comprehensive data about the workflow has been amassed, the available documented data needs to be organised and structured into a model. The workflow model should show the basic topology of the workflow and the interactions between various components and subcomponents.

The modelling phase produces in-depth models that are specially designed to be appropriate for the purpose of safety analysis and explicitly describe different workflow components as well as the communications between participating agents and information systems. The modelling framework for this approach consists of the following components:

1. Human agents involved in the workflow.
2. The involved healthcare systems.
3. The processes carried out.
4. The tasks that are involved within each process.
5. The dependencies between human agents and the tasks required to complete these processes. Processes are characterised by the communication actions required to undertake them.

Now, for modelling, as discussed earlier, starting from scratch is preferred. However, the analyst can benefit from any available information and diagrams. After getting detailed data about the workflow, the analyst can start the modelling process. Although the analyst can use the proposed constructs to develop the workflow model, brainstorming might sometimes be required to model some aspects.

Dependencies between human actors and dependencies between human actors and information systems or machines that are involved in the workflow are represented as shown in the following figure:

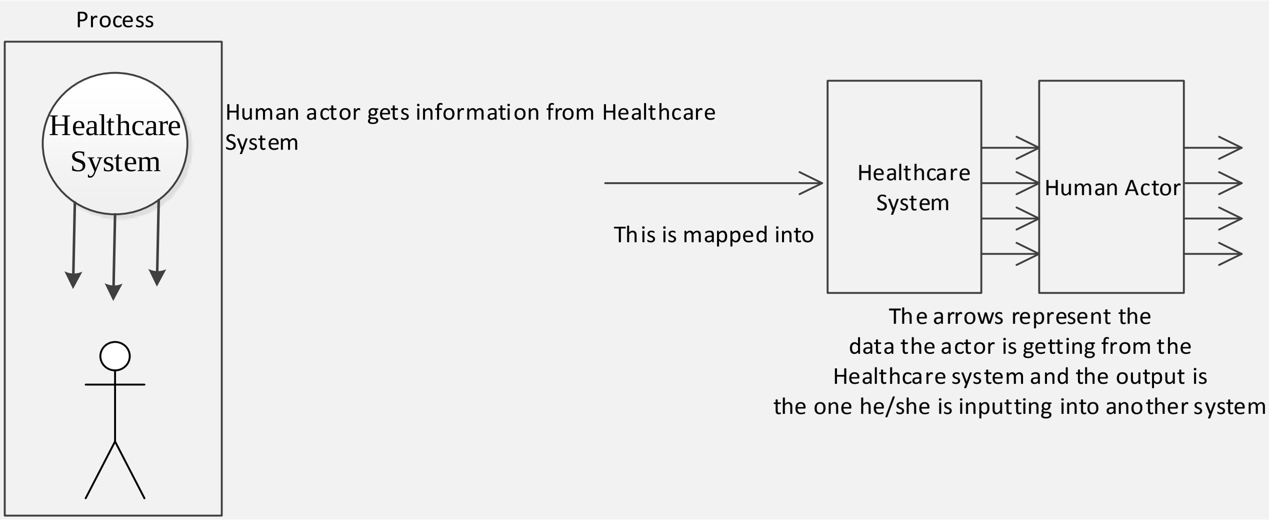

Process
Healthcare System
Human actor gets information from Healthcare System
This is mapped into
Healthcare System
Human Actor
The arrows represent the data the actor is getting from the Healthcare system and the output is the one he/she is inputting into another system

Figure 10 Modelling the interaction between an information system and an actor

The following figure shows the interaction between an actor and a system:

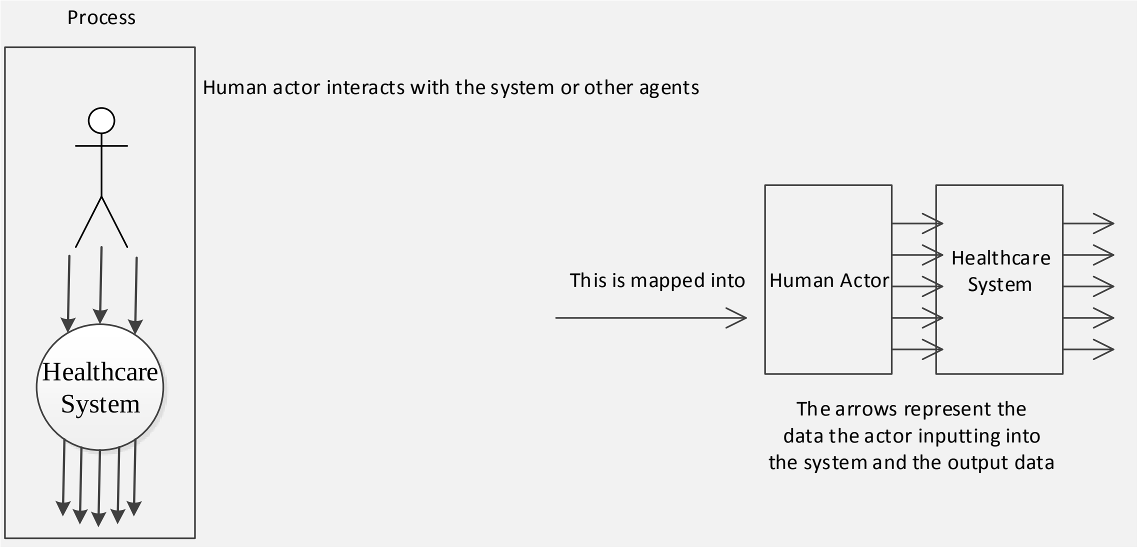

Process
Human actor interacts with the system or other agents
Healthcare System
This is mapped into
Human Actor
Healthcare System
The arrows represent the data the actor inputting into the system and the output data

Figure 11 Modelling the interaction between an actor and a system

Processes can be modelled as separate components if they do not belong to any other processes or if they are not semantically related to a human component. Parallel processes can be modelled as shown in figure 12. Processes are usually described as parallel processes if they are expected to be performed simultaneously. For example, if process A in the figure represents the first visit to the doctor, process B represents lab test, process C represents X-ray imaging and process D represents consultant visit, then D is waiting for an input from both processes B and C which can be represented as shown in the figure, while the results from B and C must be seen by the consultant to make the right diagnosis. Here, both B and C should be performed before D, but do not necessarily take place simultaneously.

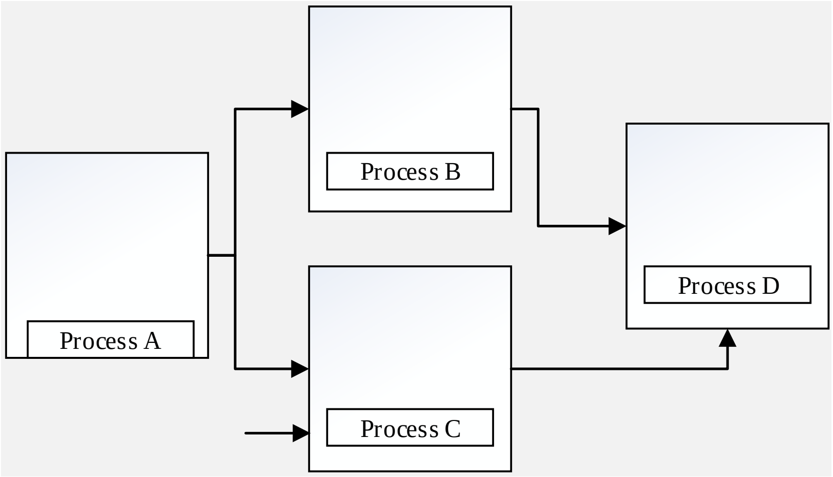


Figure 12 Modelling Parallel Processes

There are some occasions when the execution of a certain process can be conditional; for example, when the process that follows a lab test depends on the test result. The conditions can be represented by adding a sub-component to the process where the logic of the condition can be modelled. Another sub-component may be required to represent a decision module. The logic of a certain condition can represent an established algorithm or a new algorithm can be established to continue with the modelling (see Figure 13).

An example of modelling conditions using SAFE-FLOW can be found in the case study in appendix A.

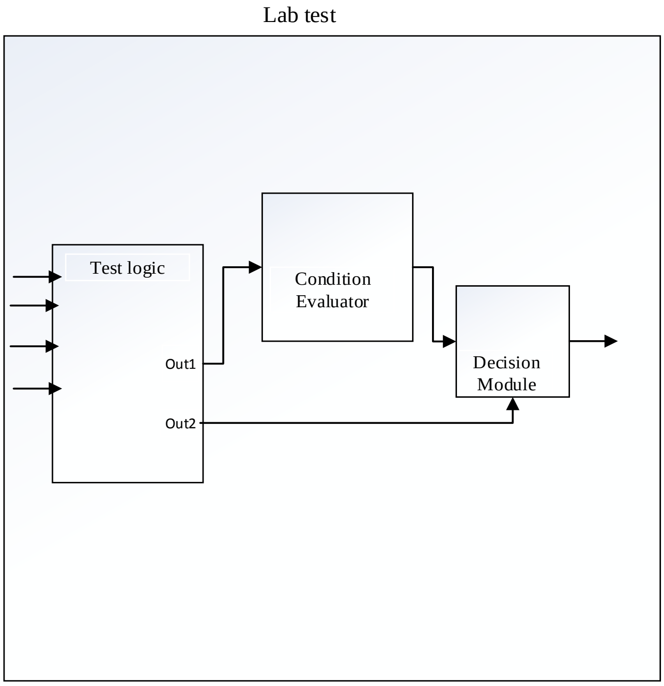


Figure 13 Modelling of conditional processes

Human actors are important components of the workflow. Therefore, modelling humans as separate components allows the analyst to annotate the failures into these components so that the analysis results can explain the consequences of human errors.

The modelling framework allows hierarchical representation of the components. Many safety analysis tools allow compositional modelling, including HiP-HOPS. This allows for hierarchical analysis as the following figure illustrates, where component1 is decomposed into sub-component1, sub-component2 and sub-component3. Component1 produces output for component2.

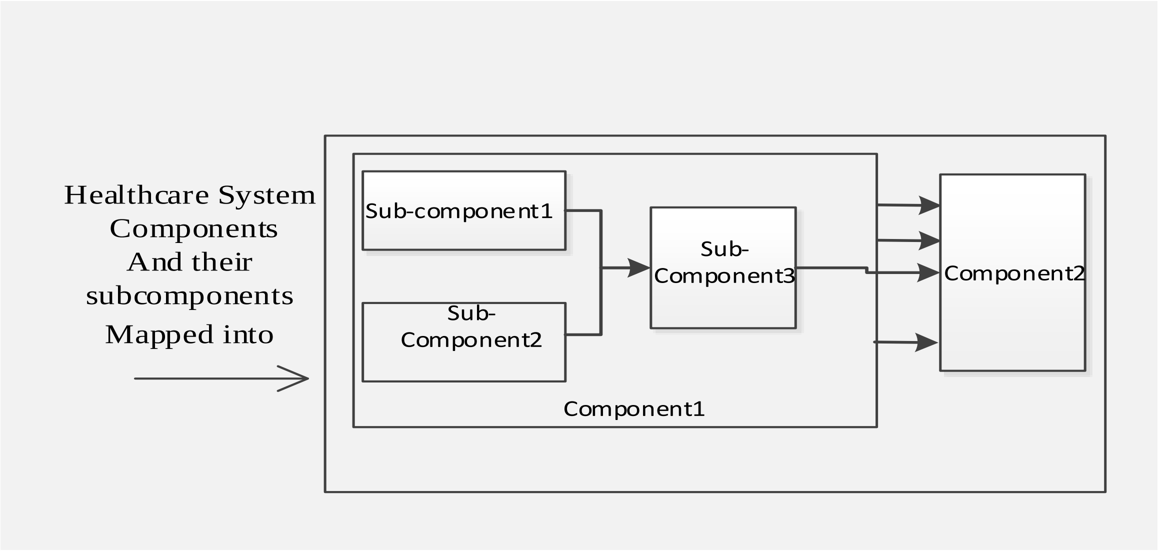

Healthcare System Components And their subcomponents Mapped into
Sub-component1
Sub-Component2
Sub-Component3
Component1
Component2

Figure 14 The hierarchical representation of components

Modelling clinical workflows can benefit from the hierarchical representation, as workflow processes are placed into separate components so that all of the tasks and different agents inside each component are semantically related; that is why it can be said that the components are interconnected. Therefore, for processes that must be performed by a human actor, such processes should be encapsulated within the human component. For example, figure 15 shows the modelling of a nurse collecting blood sample and sending the sample for analysis:

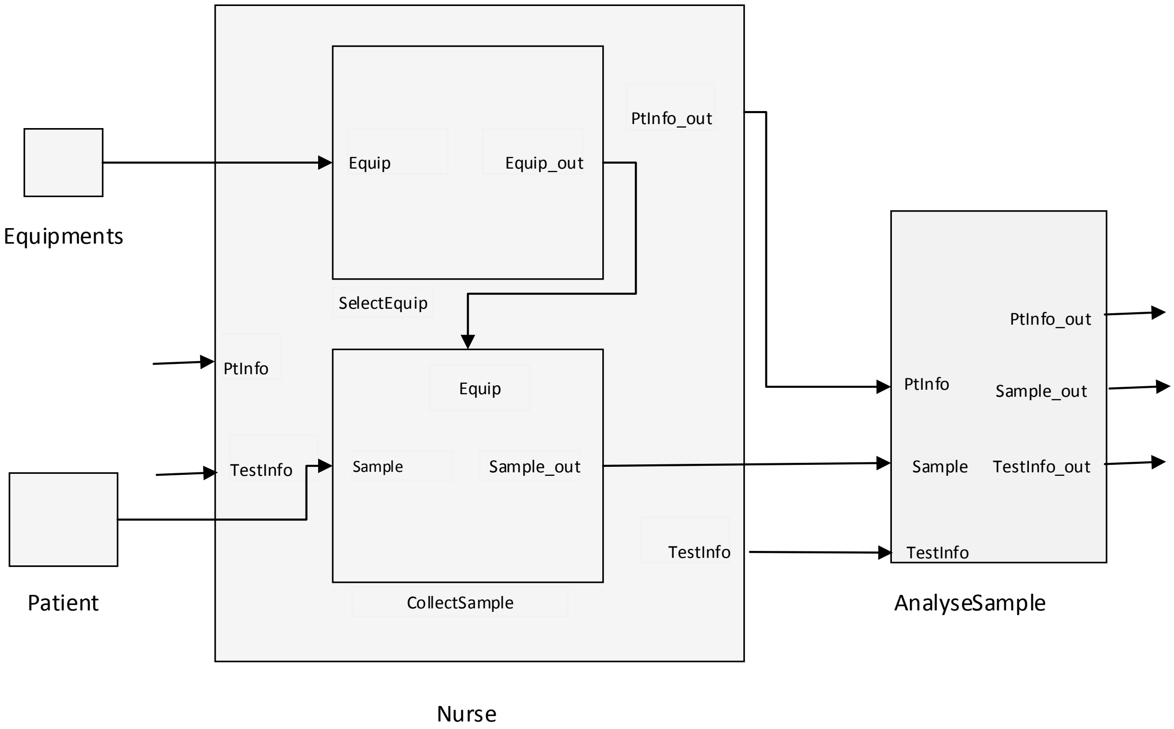


Figure 15 Modelling of a nurse collecting blood sample

The sub-processes: SelectEquip and CollectSample are encapsulated within the nurse component. SelectEquip represents the process of equipment selection and CollectSample represents the process of sample collection. The two processes: SelectEquip and CollectSample are represented as sub-processes of the component nurse, because the nurse should perform them.

If the process is a shared process that should be accomplished by more than a human actor, it should not be encapsulated within any of them. It should be represented as a main component by itself and the relationship with actors should be represented as well. This is demonstrated in the following example:

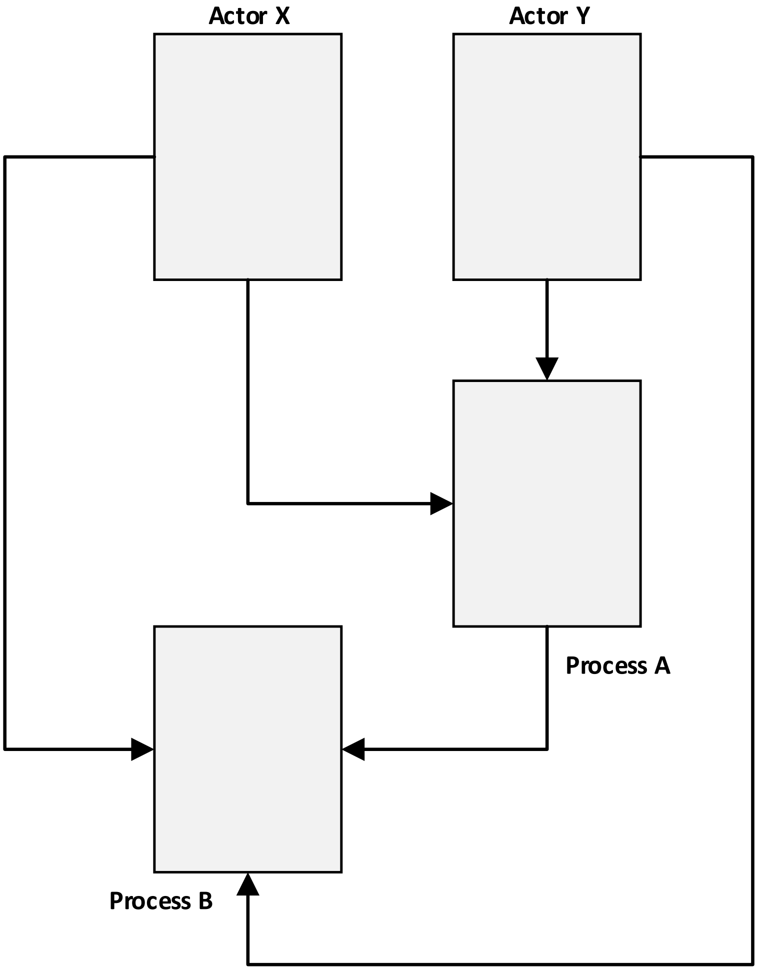


Figure 16 Modelling of shared processes

Process A is accomplished by actor X and actor Y, so it is represented as X and Y interact with A. In other words, A receives inputs from X and Y. Process B is accomplished by X and Y as well, and receives information from Process A. Therefore, processes A and B were not encapsulated within any of the human actors because they interact with other human actors. Process B in the figure also receives information from process A.

When the workflow model is ready, the healthcare team and the analyst must validate it . The model can be validated by checking whether the model captures the healthcare team needs and specifications. This can be done first through checking the model to ensure that it correctly reflects the specifications in the workflow documentation. Then it should be checked with the healthcare team to ensure that it reflects the real-world workflow. If the healthcare team confirms and validate the model then the whole team can start the process of hazards identification; otherwise, the analyst has to go back to step one to confirm reflecting the workflow requirements or any other requirements specified at the time of validation.

From the previous explanations of possible ways to model some of the workflow features, it can be seen that the modelling used is flexible and can be used to model structures that are more complex.

3.2.3 Hazards Identification and Risk Assessment (Step 3)

After building the model, the possible ways the overall workflow can fail are to be determined. This is the responsibility of the safety engineer and the healthcare experts. This step requires a careful and a systematic examination of the workflows in order to specify and determine problems that may cause harm. Qualitative techniques such as Hazard and Operability Study (HAZOP) can be used here to determine what hazards may arise from the workflow and how the overall clinical service (which is the output of the workflow) can fail. These hazards can then serve as the basis for further analyses, which will determine their possible causes. HAZOP was developed by Imperial Chemical Industries (ICI) in 1960 to systematically identify potential hazards and operability problems in newly designed chemical and petrochemical plants (Johnson, 2010). Such specified hazards can be used to identify the top event of a fault tree in FTA-based techniques such as HiP-HOPS.

After specifying hazards, risk assessment is enabled by specifying the severity of each hazard. **Safety Integrity Levels (SIL)** are classification levels that can be used to identify safety requirements in safety critical systems; they were originally described in UK Health & Safety Executive guidelines and then widely adopted by IEC 61508 and other safety standards (Papadopoulos *et al.*, 2010). The functional safety standard ISO 26262 uses ASILs to represent the stringency of safety requirements. ASILs can range from A to D where A is the least severe and D is the most severe (Parker *et al.*, 2013). After ASILs are mapped to hazards, safety goals to prevent their occurrence need to be identified to specify the initial requirements of the system (Parker *et al.*, 2013).

A similar concept, called **Development Assurance Level (DAL)** specifies the level of consistency of the development of a software or hardware function of an aircraft and guides the assurance activities that should be applied at each stage of development (Bieber *et al.*, 2011). DAL has five Development Assurance Levels (A-E), which are assigned to elements of the system's architecture over the course of development. Each level encapsulates the safety assurance activities required to be conducted for the corresponding element assigned to it. The higher the DAL requirement, the more assurance objectives are required to ensure the safety of the development of a particular component.

Thus, in the case of workflow models a number of assurance levels can be set in a similar way to SIL and DALs concepts. In SAFE-FLOW, four assurance levels are available. Each hazard should be mapped to a level. This can help in the validation and verification (V&V) process, where the assurance activities are specified for each level. The resultant workflows are checked against these assurance activities in order to build confidence with the workflow and highlight areas for redesign and improvement.

Thus, the safety levels can help to specify the requirements for an acceptable level of risk. In SAFE-FLOW, following the example of the SIL approach, those levels are identified and described qualitatively. Four safety levels are specified: level A (no safety impact), level B (low safety issue), level C (medium safety concern) and level D (high requirement for safety). Those levels are assigned to hazards based on the severity of each hazard. The high severity hazards require more safeguards and assurance activities. Medium to low-level hazards may require less assurance activities.

Although a general description of these assurance activities is provided, the healthcare team and the safety engineer should specify any context-dependent activities for each level to make sure that the workflow should never enter this hazardous state. Here, for example, if the hazard is of level D, then any single point of failure in the causes of that hazard must be avoided. In other words, tasks or components whose failure can directly lead to hazardous failure may need to be replicated or implemented to the highest safety standards. This can be verified by checking that the resultant fault tree for that hazard to ensure it has no single order cut sets.

If the hazard is of level C, then this requires less assurance, although it may still require additional monitoring and critical tasks could be highlighted as important tasks. This can be verified by allowing the resultant failure data from the fault tree with order one cut sets to be accepted, but highlighting those cut sets as critical tasks that should be carefully verified.

In a similar way, for a process with a low-level hazard, the goal could be to require less assurance that resultant fault trees with order 2 and order 3 cut sets are brought to the healthcare workers' attention and for tasks associated with order 1 cut sets to be highlighted. For those hazards that have no effect on patient safety, the resultant workflow is accepted even if it has order 1 cut sets. The following table shows the workflow safety levels with a brief description of their assurance activities:

Table 3 Workflow Safety Levels

Workflow Safety Levels	**Level A**	**Level B**	**Level C**	**Level D**
Hazard Severity	**No effect**	**Low**	**Medium**	**High**
Assurance Activities	• The workflow is accepted anyway.	• Single points of failure in the causes of hazard (order 1 cut sets) are accepted with highlighting the them as critical. • Order 2 and order 3 cut sets are accepted and brought to healthcare workers attention. • No need for workflow redesign.	• Single points of failure in the causes of a hazard (order 1 cut sets) are allowed with extra monitoring and assurance. • Order 2 cut sets are allowed with assurance and monitoring. • Redesign is not mandatory but recommended.	• Single points of failure in the causes of a hazard (order 1 cut sets) must be avoided and implemented to the highest safety standards. • Order 2 cut sets are allowed with assurance and monitoring. • Workflow must be redesigned where single points of failure are removed.

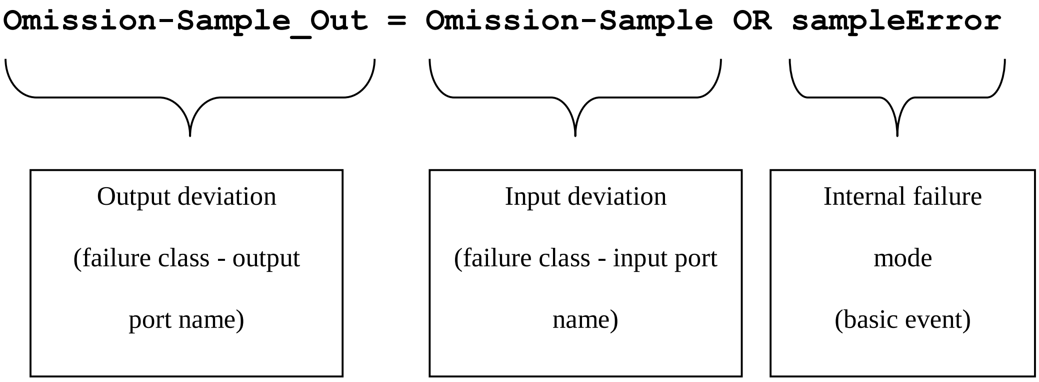
3.2.4 Failure Annotation (Step 4)

After preparation of the model and specification of the failure behaviour for each component in the model, the process of annotating the model with the failure behaviour starts. The HiP-HOPS tool needs to know how various components of the system are interconnected and how each component can fail. In this phase, components are annotated with a set of the failure expressions showing how deviations in each component output can be caused by either internal failure of this component or corresponding deviations in its input. In other words, the failure information defines how failure in the component output can be caused by the propagation of failure to the component input or the internal malfunction of the component itself.

Therefore, each component (which could be a process, task, user, application, or hardware) needs to be annotated with its own failure data that describes what could go wrong with the component and how it responds to failures elsewhere in the system. The basic failure events for each component (e.g. faults in the component itself or environmental factors), as well as the output deviations for the same component (specifying relationships between the basic events and the inputs and the outputs of the component) must be specified. The output deviation is given a name that consists of two parts, separated by a dash.

The first part is the failure class, which describes the type of failure. Although these can be defined as required by the analyst, the general categories include: **Commission,** where an action is happened when it should not have happened; **Omission,** where an event or action does not happen at all when it should happen, or **Value failure** where the wrong action happens at the right time. These are often abbreviated to C, O, and V respectively. To ensure the failure propagation works properly, whatever failure classes are used must have consistent spelling throughout the model.

The second part of the name is the port at which the deviation occurs, which should refer to the inputs of the current component (because this is the description of local failures). A hyphen can be used to separate the two parts. For example, using the nurse component in Figure 15:


Omission-Sample_Out = Omission-Sample OR sampleError
Output deviation (failure class - output port name)
Input deviation (failure class - input port name)
Internal failure mode (basic event)

Omission-sample_out would describe an output deviation in which no sample is provided for analysis either because the nurse made an error (an internal failure mode) or because the nurse did not receive the sample in the first place (propagation of external failure mode).

Logical operators **AND** and **OR** can be used to combine multiple input deviations or failure modes together, and brackets can be used if necessary to link the operators to the correct operands.

Human actors' components can fail like any other components. However, failure of a human component (e.g. a clinician or a nurse) does not mean that this component has a physical failure. In this thesis, human errors are categorised into commissions where a human performs an action when they should not have done, omissions where a human does not perform the correct action when they should have done, and value failures where a human performs the wrong action at the right time. As a simple example of this, a computer program may require the user to press a key at a certain time. If the user presses it without the need to, it is a commission. If he/she does not press it at all, it is an omission. If he/she presses the wrong key, it is a value failure.

Human actions are necessary for proper functioning. Thus, they need to be considered whenever there is an interaction between a human and: a process, an application, or a patient within the workflow. Unintentional human error can result in other faults occurring later in the workflow and cause a failure of the clinical service. In other words, procedural errors must be annotated within the model because they may propagate within the workflow to cause adverse events. In addition, any errors that might lead to inappropriate actions must be annotated into the model as well. This annotation allows better analysis results, which helps lead to the detection and recovery of these errors. Human errors could include but are not limited to decision error, inadequate verification, action of the wrong type, action at the wrong time, missed action, or wrong identification.

An important issue identified here is that although leaving a level of compliance and flexibility to human work can result in more effectiveness, it may also be a cause of failures. For example, healthcare experts are sometimes required to adjust their procedures and activities to cope with the current condition of the patient and to solve a particular problem. This alteration can lead to new kinds of failures that were not identified before. Therefore, analysing diverse workflows that include alternatives for the steps to be taken by humans to produce the same service can lead to the identification of the specific activities that may cause adverse events. Accordingly, analysing human activities can improve service delivery by specifying the safest path that leads to delivery of the desired clinical service. Moreover, this form of analysis can transform the unpredictable failures that may occur because of unanalysed workflow in to predictable failures, where the consequences of each human error are clear.

To clarify the failure annotation step, the example shown in figure 15 is a model for collecting blood sample by a nurse. The SelectEquip sub-process can have a basic event EquipError that can cause an output deviation V-Equip_out, which indicates that the nurse has chosen the wrong equipment. In addition, the nurse component may have the following basic events: adding the wrong information to the label by the nurse (labellingError), receiving the wrong patient information (PtInfoError), receiving the wrong test information (TestInfoError), forgetting to label the sample (missingLabel), forgetting to add patient information (missingPtInfo) and forgetting to add the test information (missingTestInfo). Those can cause the following output deviations: generating incorrect patient information (V-PtInfo_out), collecting an incorrect sample (V-Sample_out), giving incorrect test information (V-TestInfo_out), omission of patient information (O-PtInfo_out) and omission of test information (O-TestInfo_out). An example of the failure expression for these deviations is:

V-PtInfo_out = labellingError or PtInfoError

which means that the nurse either wrote the wrong information on the blood sample or received the wrong information originally. This can be mitigated for example by adding an extra task where the nurse verifies the patient information before collecting the sample.

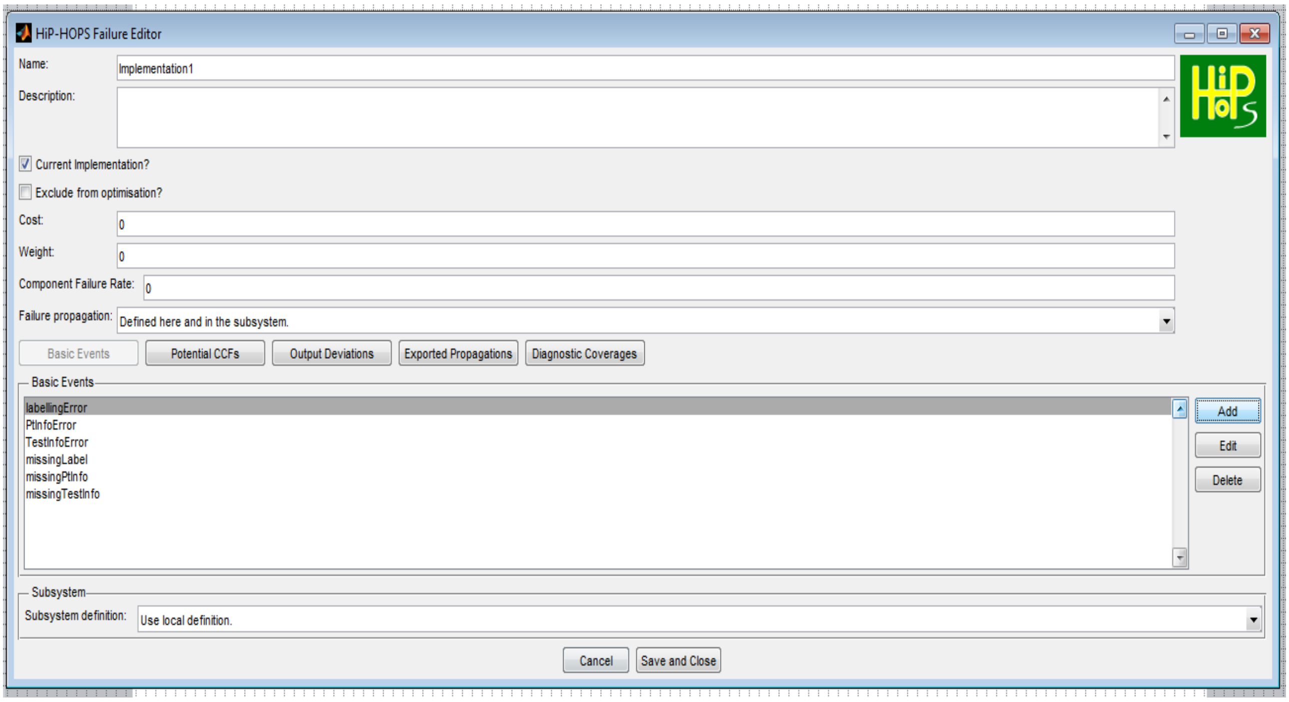
Another example for a failure expression of another deviation is:

O-PtInfo_out = missingPtInfo or missinglabelling

which indicates that the nurse may send the sample for analysis with a missing patient information, and this can be caused by either having the test information without the patient information or by collecting the sample and forgets to label it.

Each output deviation is represented by a logical expression. In HiP-HOPS this is symbolised in a box, where a failure expression links causes (causes could be basic events, input deviations or even common cause failures) to the faults propagated from the outputs. These can be linked using AND and OR operators.

The following figure shows the HiP-HOPS failure editor annotated with basic events for the nurse component:



Name: Implementation1

Description:

☑ Current Implementation?

□ Exclude from optimisation?

Cost: 0

Weight: 0

Component Failure Rate: 0

Failure propagation: Defined here and in the subsystem.

Basic Events

labellingError
PtInfoError
TestInfoError
missingLabel
missingPtInfo
missingTestInfo

Subsystem

Subsystem definition: Use local definition.

Figure 17 HiP-HOPS failure editor

Chapter 4 of this thesis has a full example of the application of SAFE-FLOW to the workflow within a radiology department.

3.2.5 Fault Tree and FMEA Synthesis and Analysis (Step 5)

After the model is annotated, HiP-HOPS is applied and automatically navigates through the failure information. It proceeds backwards, starting from the overall workflow failure(s) and connecting each failure to its causes, linking them with logical operators. This results in the automated production of the main fault tree(s), which can then be analysed. HiP-HOPS synthesises and analyses the workflow fault tree and produces the FTA and FMEA results, which show how the failures in components can lead to workflow failure. During this phase, the minimal cut sets (MCSs) that are required to cause the top event are obtained as well.

The analyst and the healthcare experts then use this qualitative analysis data to check whether the safety requirements are achieved or not, depending on the Workflow Safety Levels assigned to each hazard. If the safety requirements are achieved then the workflow is approved; otherwise, if the safety requirements are not achieved, then the analyst attempts to remove the sources of failures or redesigns the workflow to mitigate such failures and goes back to start from step 2.

In some cases, this qualitative data is enough to refine and reengineer the processes and tasks within the workflow. Therefore, the analyst can start to redesign the workflow immediately after the qualitative analysis. However, in other cases, the new design may require replacement of the existing components with components, which are costly for the healthcare organisation, and thus decision makers in the hospital may ask for quantitative information about the likelihood of the component to fail. In these cases, quantitative analysis is recommended; otherwise, the analyst can move immediately to check if the safety requirements have been achieved or not with the new workflow. If they are achieved then the workflow is accepted; otherwise, the analyst has to perform another iteration to create a new workflow design in which he/she replaces some components with safer components and/or removes the causes of failures. The designer may also add new components, which could be hardware components, software components or extra processes or tasks. Then the analyst should go back and start again from step 3 (workflow validation).

3.2.6 Probability Analysis (Optional Step)

Probability analysis is an optional step, which can be carried out after the previous phases. This could be performed by obtaining failure information on different components and adding numerical information into the components in the modelling phase, allowing HiP-HOPS to provide information about the probability of each top event.

Workflow components could be processes, tasks, or people. Therefore, they are different from other components that have manufacturer failure rates. Human error failure rates can be obtained using quantitative analysis methods of real data to get statistical information from previous experiences. However, this method has the problem that the analysis results may be incorrect results due to the vagueness of the data provided. The reason behind this inaccuracy is that human failures are dynamic as they may be affected by many environmental factors. This was the motivation behind searching for another mechanism for probability analysis, which addresses the uncertainty issue. Therefore, since the probability of human error usually cannot be given an exact value, instead it would be estimated.

The proposed probability analysis in SAFE-FLOW is separated from the analysis phase. After finishing the analysis phase and getting the FTA and FMEA results, the analyst can start the quantitative analysis, if it is required by getting an estimated probability for each of the fault tree components. In this case, analysts can seek experts' opinions and can develop their own tools to get such failure numeric information. After that, fuzzy set theory can be used to quantify the fault trees.

This failure probability analysis approach has the potential to affect the results and the accuracy of the analysis. In other words, it specifies the failure rates that are used for the analysis and consequently has a direct effect on the analysis results.

As explained previously, if the workflow redesign process is costly for the hospital or the healthcare institution, decision makers in the hospital may ask again for probability analysis of the workflow, as they want to see some statistics about the probability of those causes to make an informed decision about the cost of redesign. In other words, this is a part of the cost benefit analysis, where the cost of replacement is compared to its benefits and the severity of the failure.

If probability analysis is required, it must be accomplished before the workflow redesign; if it is not required, workflow redesign is accomplished immediately after the qualitative analysis. After that, it needs to be tested as to whether it meets the safety requirements or not; if yes, the safety engineer can go ahead and the workflow is accepted and approved as the formal workflow in the department. Conversely, if it does not meet the requirements, then the process needs to be repeated until the workflow is satisfactory.

3.2.7 New Workflow Design (Optional Step)

As explained previously, after analysing the workflow, the analysis results can be used by the safety analyst and the healthcare experts to review whether the safety requirements are achieved or not. If the safety engineer and the healthcare team do not accept the workflow design due to not achieving the safety requirements, then the workflow should be redesigned to avoid the causes of possible failures. In the redesign, some kind of replication or monitoring may be required. For instance, if the Workflow Safety Level for a given hazard is level D, then in the new design the safety engineer should ensure that it requires two or more failures to occur rather than just one. As an example, if the analysis results show that a serious failure can be caused if the data provided by the patient is not verified before use, where the patient provides incorrect information, then another task could be added where the clinician verifies the data before beginning a particular critical procedure. This will ensure the hazard occurs only if both failures happen, i.e. incorrect data provided by the patient and the clinician forget to verify the data.

Once the workflow is redesigned, the analyst makes a thorough check to make sure that the causes of significant hazards are addressed. This in-depth check can be done by repeating the analysis (return to step 2), which can be done mostly automatically. If the workflow is slightly redesigned, it might be necessary to add or edit some components in the model, but most of it remains intact. The subsequent analysis can then be performed almost instantly, making it very easy to see (and check) the impacts of any changes on the workflow safety, allowing rapid iterations of design changes. This is not only convenient but allows for multiple phases of modification to take place, using safety to drive the evolution of the workflow design.

3.2.8 Accepting the Workflow (Step 6)

As mentioned in the previous step, once the workflow is analysed and before the workflow can be accepted as an official workflow within a department or a hospital, the safety analyst with the healthcare team must check whether the safety requirements are achieved or not. Failure analysis results can be used as an indicator for achieving the safety requirements in addition to the feedback from the healthcare team. Moreover, the analyst should make sure that the remaining risk is acceptable and he/she should draw experts' attention to this risk. Solutions for the remaining failures must be within the healthcare team's capabilities; for example, tasks that are specified as root causes for failures could be marked as strict tasks that should be done exactly as described.

3.3 Conclusion

To summarise, SAFE-FLOW enables the modelling and analysis of clinical workflows. Utilising SAFE-FLOW has the potential to reveal patterns of diagnostic and procedural failures and to suggest areas for improvement. Systematic analysis of such potential failures can pinpoint their root causes and enable identification of potential preventive strategies to assist in promoting safety in healthcare. This highlights a particularly important issue to consider when planning to adopt new systems or to make changes on the organisational procedures level, which is that these changes must be reflected in the workflow itself. The risks of performing a modification to the workflow (through software or else) must be evaluated against the risks of not performing the modification, or performing alternative modifications. The potential hazards relevant to this consideration may be quite different, and specific to different kinds of clients.

Performing safety analysis in this way helps to understand the implications of different failures that lead to a hazard occurring. In other words, these cumulative failures (amongst other factors) are the trigger events that may lead a workflow to enter that hazardous state. Thus, this analysis helps in preventing hazardous events from occurring.

This chapter described SAFE-FLOW and showed how to apply the involved steps in detail. To evaluate the applicability of SAFE-FLOW the next chapter presents its use to analyse the workflow within a radiology department as an example of a clinical workflow.

4 Safety Analysis of the Workflow within a Radiology Department- Case Study

Radiology Information Systems (RIS) and Picture Archiving and Communication Systems (PACS) are widely used to help in the workflow management in radiology departments. Different architectures have been developed and several workflows are in use in different hospitals. Effective safety analysis is required to ensure reliability of these high-risk workflows, because errors that may happen through routine workflow can propagate within the workflow to result in harmful failures of the workflow output.

With the popularity of RIS/PACS in healthcare institutions, there is a growing need to analyse their safety. This chapter shows how to apply SAFE-FLOW to analyse the safety of RIS/PACS workflows.

Earlier research on safety analysis within the radiology workflow has been concerned with reporting adverse events (Fitzgerald, 2001) and using FMEA to analyse adverse events (e.g. Abujudeh and Kaewlai (2009); Thornton *et al.* (2011)). Other research was focused on the unintended additional phases in patients undergoing pelvic CT scanning which add substantial excess radiation dose with no associated clinical benefits (e.g. Guite *et al.* (2011)). Moreover, adverse reactions to Contrast Media (CM) (which allow the radiologist to distinguish normal from abnormal conditions) were studied by many researchers (e.g. Morcos and Thomsen (2001)).

The following sections explain the case study in detail and show how SAFE-FLOW can be applied to the radiology workflow. Later the chapter explains how the analysis results can be beneficial to the radiology department.

4.1 Why Use Radiology Workflow for a Case Study?

RIS/PACS technology has advanced dramatically in recent years, including the technology of acquiring, storing, retrieving, displaying, and distributing clinical images (Boochever, 2004). It has become a mature technology and has been commonly implemented in a number of developed countries (Paré *et al.*, 2005). Different systems have been designed and developed to assist different workflows in radiology departments in several hospitals. In Jordan for example, RIS/PACS are implemented in a number of private, government, and military hospitals.

A RIS as defined by The Royal College of Radiologists (2008) is a computer system designed to support the operational workflow and business analysis within radiology departments; it is a repository of patient data and reports that contributes to the Electronic Patient Record (EPR) or Electronic Health Record (EHR). The Royal College of Radiologists (2008) described the RIS as an imaging information system since it supports many additional specialists in areas including nuclear medicine, radiotherapy, and endoscopy.

As a RIS contributes to EHRs, then any errors in these systems affect the EHRs, which may put clinicians in a situation where they make wrong diagnose and consequently put patients' lives at risk.

Adverse drug reactions are now the fourth primary cause of death in the United States after heart disease, cancer, and stroke (Starfield, 2000). Adverse events may happen because of undetected errors in any process during the diagnostic imaging study or intervention. These always happen when patients have side effects of unexpected harm during or after a treatment process.

Safety of RIS/PACS workflow is concerned with the process by which patient care is made safer, where safety analysis is done to identify the weak points in the theoretical workflow that may lead to errors during the operational workflow. A weak point is an error that could cause the workflow to produce a hazardous output when it is in operation. The intention is to redesign the workflow in such a way that such unintended events are less likely to happen.

A failure in a radiological diagnostic process can take the form of a misdiagnosis, a diagnosis that is treated wrongly, or a late diagnosis. This could include any failure in different types of radiology images procedures and includes having unexpected side effects that happen as a result of a radiological process.

Fitzgerald (2001) identified the need to develop a safety culture within radiology departments where, every time an error is made, it should be brought to other technologists' attention in a sensitive fashion to develop a learning experience. Radiology departments should pay much attention to workflow failures and human errors related to those failures. They should aim at designing the utmost faultless workflows; and focus on critical human interactions that have the potential to cause adverse events.

With this frequent use of RIS/PACS in healthcare institutions, there is a growing need to analyse the safety of their workflows, and in particular, the theoretical safety that sets the ground for a safe operation. The safe design can be useful later for teaching users how to complete their tasks accurately, instead of blaming systems for their errors.

Analysing and modelling the workflow plays an important role in medical information technology projects, as the implementation of these systems requires an understanding of the processes involved in them (Ouvry, 2002). Moreover, technology (e.g. RIS/PACS) needs workflow description such as identification of tasks, input and output information, people and departments involved, and the management of the information flow according to this description (Lenz and Reichert, 2007).

Moreover, the root cause of radiological error is multi-factorial and requires investigation (Fitzgerald, 2001). There is a need for systematic approaches through which the possible failures can be investigated.

As mentioned earlier there are insufficient studies that focus on the RIS/PACS safety, especially from the workflow perspective. Even if designers make sure of technical safety, operational safety plays an important role in getting the right results. It is essential to address this challenge by using efficient methods to perform the analysis process. Little information is available regarding operational errors in RIS/PACS workflows. For example, Abujudeh and Kaewlai (2009) studied the safety screening of patients with diabetes before interventional procedures to reduce the number of patient emergencies. Research to date has not identified the best approaches for operational error risk reduction. Many aspects of RIS/PACS design can be changed through safety analysis of the theoretical workflow to prepare for a safe operational workflow. This is simply because the flawed design of the theoretical workflow has the potential to decrease efficiency and increase operational errors.

In the face of these limitations and after investigating existing architectures of RIS/PACS systems and their workflow, this thesis applies SAFE-FLOW to one of the existing architectures of RIS/PACS workflows. The unit of analysis is the RIS/PACS workflow in a Jordanian hospital, although the main features, characteristics, roles and processes appear similar to other institutions, countries and clinical workflows.

A healthcare team was selected carefully to represent all levels of operational staff; it consists of a radiologist, technologist, clinician, a nurse and the project manager. The team indicated that they had some concerns regarding the workflow within the department, and the flow of information from the department to the other workflows in the hospital.

The discussions showed that the main concern about adopting the RIS/PACS systems was the potential lack of safety of the workflows within these systems. This was because of faulty operational workflows that may have many problems with clearness and safety, as where the safety issue was not addressed specifically during the workflow design. This led to output failures of different parts of the workflow and eventually harmful failures in the final output of the workflow, e.g. producing a report that had an incorrect description of the patient’s situation, or leading to undesired reactions by the patient. Having the wrong report potentially results in an incorrect diagnosis and treatment, placing the patient’s life at risk, while the effect of having unwanted side effects by the patient varies depending on how serious these effects are.

The discussions ended with recognition of the importance of the safety analysis process for the workflow within the radiology department. However, conducting comprehensive safety for the workflow was found to be a challenging target because there are many analysis topics in the radiology department; the healthcare team, while performing the case study, identified many topics; these topics can be termed as **scenarios**.

Investigating the causes of failures in different scenarios was found as an essential step, which can improve the workflow design through redesigning the workflows to avoid these failures. The applicability of SAFE-FLOW is tested through its application to two scenarios within the radiology workflow. However, SAFE-FLOW could be applied to other scenarios and to a wider range of workflows.

4.2 Applying SAFE-FLOW to the Radiology Workflow

4.2.1 Workflow Documentation (for the Main Workflow within the Department)

Initially, the workflow within the department was documented in cooperation with the healthcare team in order to understand it and specify its topology and components. Furthermore, critical components and prospective failures for this workflow were identified in order to perform the analysis. Critical components are those that potentially experience faults and errors as well as failures that are likely to happen if the component is compromised by the error. Data is collected regarding occurrence of the workflow errors and their prevention in the same scenario environment. This resulted in documentation that consists of detailed information about the components and the relationships between them. Moreover, it identifies full description of failure information for each of the components.

The resultant documentation ends with the following details:

The ideal architecture for a RIS has a hospital information system (HIS) which works as a master patient index, where data goes immediately to the RIS without the need for a technologist to enter any data.

In the studied workflow, the hospital combined the RIS and PACS and has them as a stand-alone departmental radiology system. They have a non-complete HIS that does not have full functionality and is not connected to the RIS. All the data needs to be entered in the RIS by the clinicians manually. The information to be entered includes the following: Patient name, Patient National Number, Date of Birth (DoB), Age, Address, Patient medical Information, and Order Information.

After the above information is entered into the RIS either by the clinician (as in this case) or immediately from the HIS (in other cases), then this information (which includes the patient’s medical, administrative, demographics, and billing information) is kept in the RIS, in addition to the information which is added at the RIS to identify the examination order. These may include the following:

Order ID, Order Description, Scheduling, Patient Arrival Information, and Examination Room Scheduling.

This discussion considers the case where the clinician enters part of the information into the RIS, and there is some information that is entered into the RIS by another party who might be a radiologist. After that, the output of the RIS goes to the modality worklist (MWL) which acts as a database through which orders are scheduled to be sent to the image acquisition modality. Here in the image acquisition modality, there is no chance for human error as the data comes immediately from the RIS. However, this database, which has all the scheduling information and orders information, is open to hardware and software errors. In the image acquisition modality the patient is supposed to have the examination that is specified in the order. The output of the image acquisition modality is patient id, patient name and the image itself.

After that, these outputs are sent automatically to the PACS which archives them and then sends them to the diagnostic workstation to be seen by the radiologist. The radiologist is now able to interpret examinations from several clinical sites and/or hospitals (in the case of Teleradiology), and produce a report as an output. This report is to be passed to the clinician to make the diagnosis and give a medicine or recommendation for another procedure such as an operation.

Documentation of the CT Scan Scenario

In the first workflow scenarios; a Computed Tomography (CT) scanner creates cross-sectional images of the body using X-rays; the result is a very detailed 3D view of the body interior. CT scans are used to make a cancer diagnosis or assess the effects of cancer treatment.

The workflow documentation phase for this scenario resulted in the following information about the scenario:

When the patient sees the clinician, the clinician decides if there is a need for a CT scan. Once a CT scan is recommended, the risk of exposure to radiation is considered before deciding to send the patient to the exam. This is because the accumulative amount of radiation the patient is exposed to has a potential risk for the patient, so clinicians recommend it when they think that the benefits will exceed possible risks. In order to consider the amount of radiation, in most cases the date of the last CT scan must be considered by the clinician before such a decision can be confirmed. Moreover, if required, a pregnancy check must be done to make sure that the woman is not pregnant.

Commonly, patients who will receive a CT scan must follow certain preparation guidelines. These include no eating for two hours before the appointment, and drinking 500 ml of water over this time. The water is useful to hydrate the patient before having the CM for the CT scan. Another preparation guideline is to ask the patient to drink another 500ml of water after arriving in the waiting area. It also helps to show the bladder on the scan.

Verbal verification by the radiologist is needed to check these preparations with the patient together with other preparations such as ensuring there is no metal present (e.g. wearing of a metal belt, or jewellery or having an internal device inside their bodies). Moreover, verbal verification of the patient’s DoB at this point plays an important role in correcting any previous errors in the DoB, as the DoB is important in determining the amount of CM and the amount of radiation. Some patients may require a blood test before CM can be given.

CM is usually used to aid in distinction of anatomic structures, improve lesion localisation, and support injury characterisation (Antoch *et al.*, 2004). The rate of adverse reactions to iodinated CM on the market is very low, but such reactions do occur (Morcos, 2014). The adverse reactions associated with CM can be divided into two groups: those reactions that are clearly dependent on the dose and concentration of the CM administered and those that are almost independent of dose and concentration.

Dose-dependent adverse reactions are mostly due to the physiochemical effects of the CM, such as its osmolality, or electrical charge. Possible adverse reactions include heat, pain, vasodilation, cardiac depression and hypotension. The adverse reactions, which are almost independent of dose and concentration, are nausea and vomiting as well as allergy-like or hypersensitive reactions such an urticaria (hives), certain cardiovascular reactions, bronchospasm and laryngospasm. These reactions cannot be predicted and their underlying cause remains unknown.

An injection of the CM is often given before or during the scan. CM contains iodine and appears as white areas on the scan, which help the radiologist to differentiate between certain organs or tissues and other structures. The CM may be ingested as a drink, injected around the required area, or given via a cannula, which is placed in the patient’s arm prior to the scan. Again, verbal verification is required here to confirm any allergies and medications that the patient takes in order to judge the suitability of the injection and to minimise interactions with other medications.

Typically, people who feel claustrophobic do not have problems with CT scan as they might have with other scans, like Magnetic Resonance Imaging (MRI). However, the radiographer should check this with the patient before the scan, as if the patient thinks that he/she is expecting to feel this way then an injection may be given before the scan to calm the patient.

After the scan is finished, the patient should be asked to wait for at least an hour after the injection to make sure the patient is in good health, and he/she did not have allergic reaction to the CM injection, because people sometimes have different reactions; in these circumstances, medical staff should be able to manage different reactions appropriately. The radiologist then should give some instructions to the patient to follow once he/she goes home, for example, again asking the patient to drink 500ml of water to rehydrate the body after the CM injection.

Component	Interactions		Information received	Information produced	Sub-components
HIS	**Receive from**	None	• Patient ID • Patient Name • Patient DOB • Information	• Patient ID • Patient Name • Patient DOB • Information	• EHR
	Send to	Clinician (human component)			
Clinician	**Receive from**	HIS (System component)	• Patient ID • Patient Name • Patient DOB • Information	• Patient ID • Patient Name • Patient DOB • Information • Order information	
	Send to	RIS (System component)			
RIS	**Receive from**	Clinician (Human component)	• Patient ID • Patient Name	• Patient ID • Patient Name	

	Send to	Modality Worklist	• Patient DOB • Information • Order information • Order ID • Schedule Information • Patient preparation information	• Patient DOB • Information • Order information • Order ID • Schedule Information • Patient preparation information	
Modality Worklist	**Receive from**	RIS	• Patient ID • Patient Name • Patient DOB • Information • Order information • Order ID • Schedule Information • Patient preparation information	• Patient ID • Patient Name • Patient DOB • Information • Order information • Order ID • Schedule Information • Patient preparation information	
	Send to	Image Acquisition Modality			

Image Acquisition Modality	**Receive from**	Modality Worklist Accession number input Verbal verification	• Patient ID • Patient Name • Patient DOB • Information • Order information • Order ID • Schedule Information • Patient preparation information • Accession Number • Preparation verification	• Patient ID • Patient Name • Image • Reactions	• CM dose • Other reactions • Reactions
	Send to	PACS Patient (Human component)			
PACS	**Receive from**	Image Acquisition Modality	• Patient ID • Patient Name • Image	• Patient ID • Patient Name • Image	
	Send to	Diagnostic Workstaion			

Diagnostic Workstaion	**Receive from**	PACS	• Patient ID • Patient Name • Image	• Report	
	Send to	EHR			

Table 4 organising the components of the radiology workflow

4.2.2 Workflow Modelling

The following figure shows the model that represents the workflow within the department. The information from the EHR is relayed back to the HIS component.

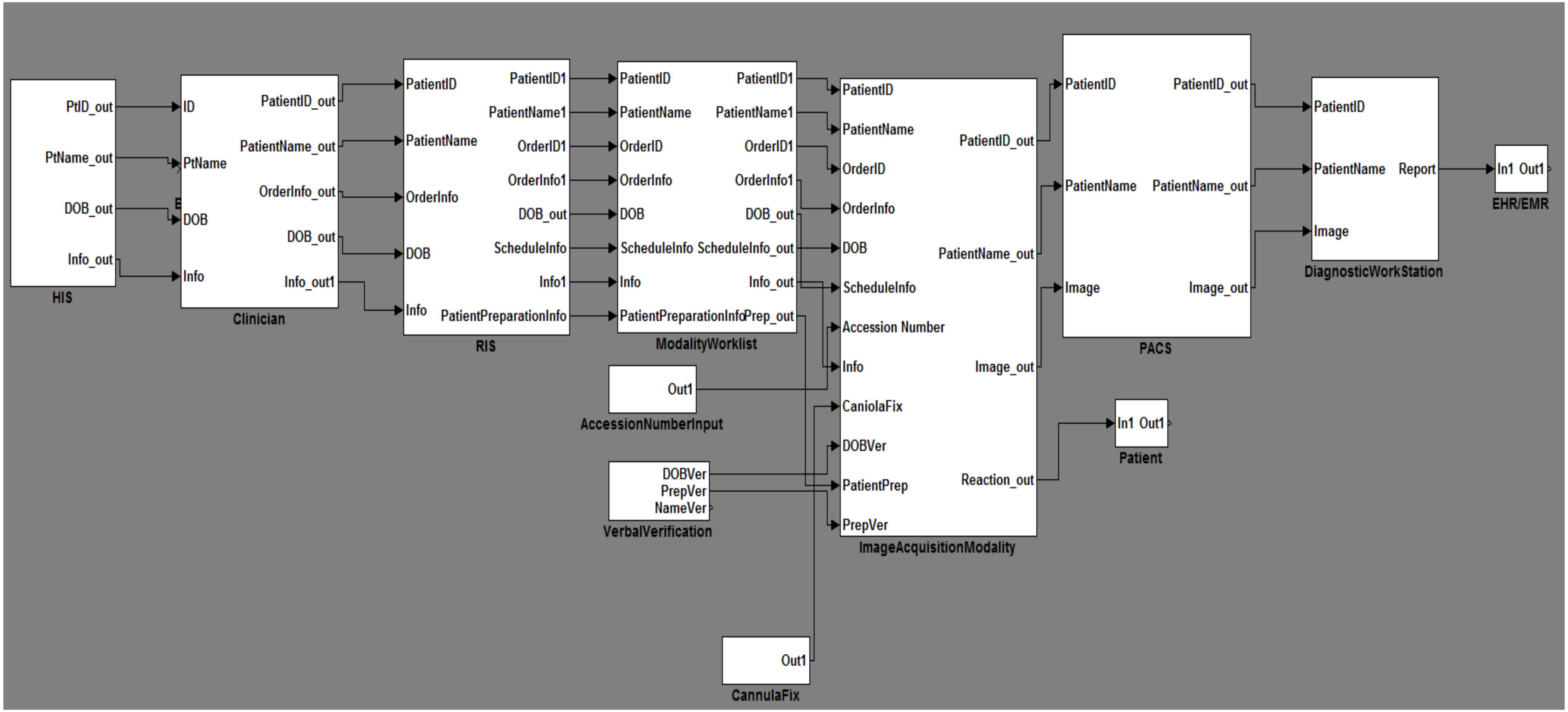


Figure 18 The Radiology workflow (HiP-HOPS snapshot)

The EHR has the following information:

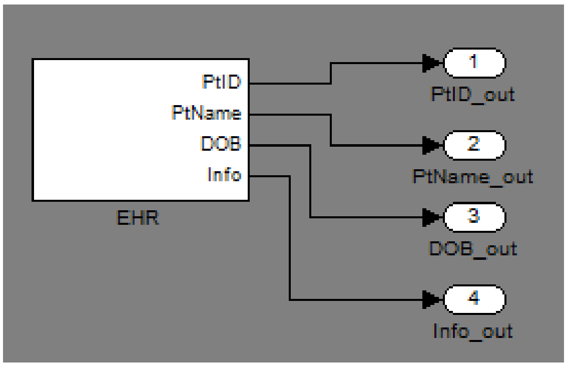


Figure EHR component (HiP-HOPS snapshot)

The CM is modelled as a separate component:

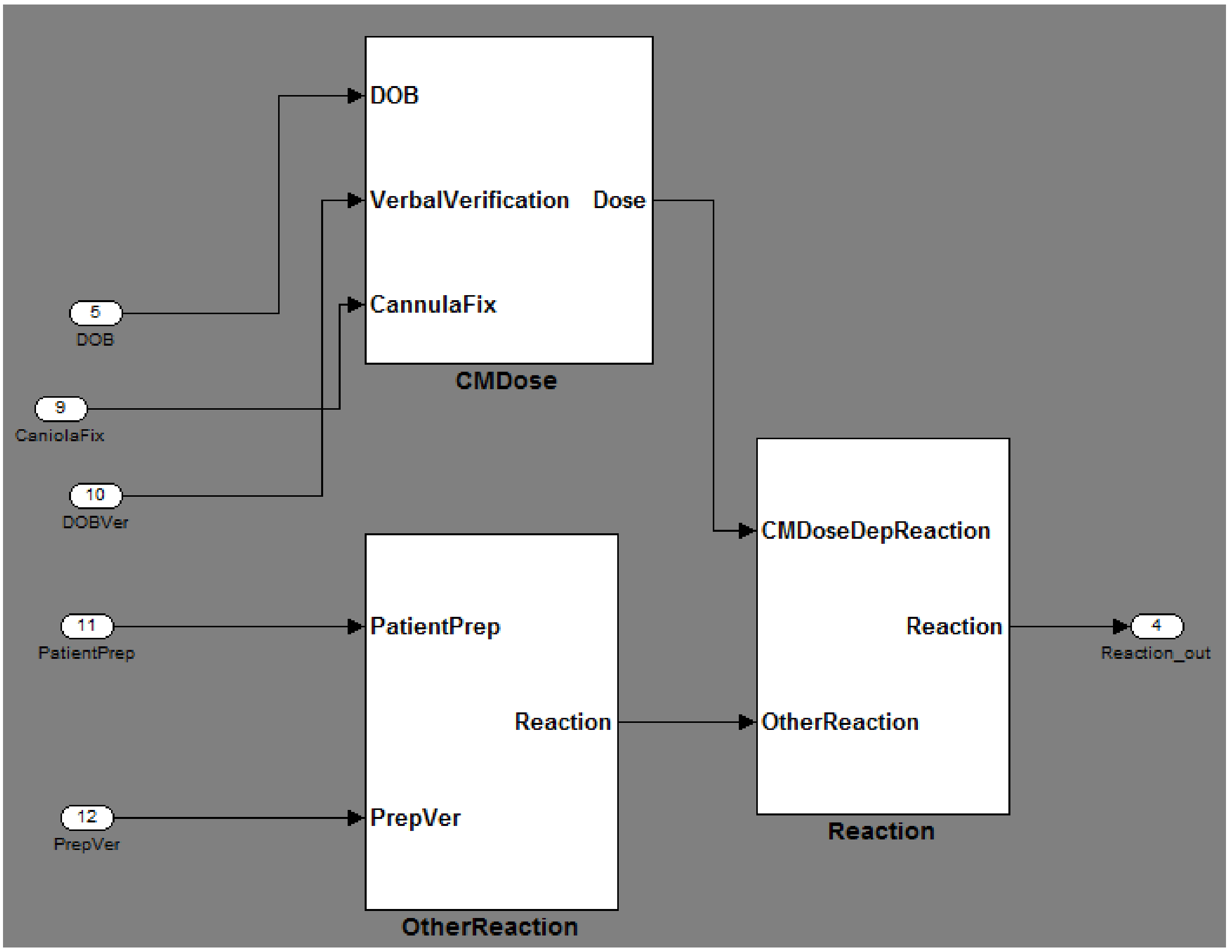


Figure 19 The CM component (HiP-HOPS snapshot)

The ability of HiP-HOPS to arrange the components hierarchically helped to model the CM in such a way as to be a sub-component of the image acquisition modality. The CMDose Calculations is modelled as a subcomponent of the CMDose.

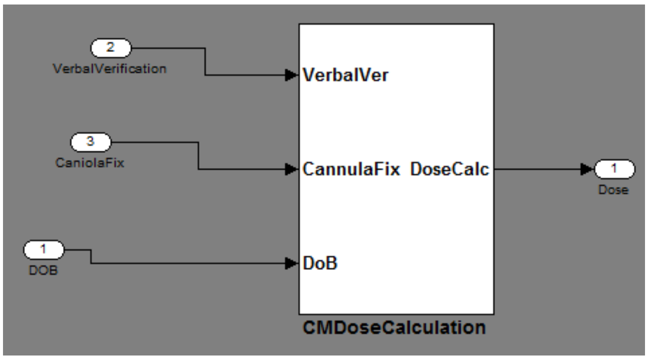


Figure 20 CMDoseCalculation Component (HiP-HOPS snapshot)

4.2.3 Hazards Identification and Risk Assessment

The team of experts (a radiologist, technologist, clinician, a nurse and the project manager) identified the following hazard for the first simplified workflow scenario:

- ErrorIn-PatientOut (where the patient has unanticipated reactions)

A wrong value in the patient output happens when the patient has unexpected reactions. The severity of this hazard is identified as medium (level C); it occurs if the patient receives the wrong dose of CM (value deviation from CMDose-out) or receives other reactions like wrong preparation of the patient (value deviation of OtherReaction-out). This results in the following:

Hazard	Causes	Hazard Severity
H1 (ErrorIn-PatientOut)	**Value deviation of CMDose.out OR Value deviation of OtherReaction.out**	**Level C: Medium**

4.2.4 Failure Annotation

The RIS/PACS system's workflow is modelled to enable the automated analysis. The team identified several failure modes associated with each component. Then, the model is extended with failure information for each component. This failure information describes how a failure in the component output is caused by a propagation of failure from the component input or the internal malfunction of the component itself. Failure is represented in the format of "FailureType-ComponentName.ComponentPort" in HiP-HOPS.

The CT scan scenario analysis focuses on the patient having side effects or bad reactions by the patient. As described by the workflow architecture, the effect on the patient is considered as an 'output' component. This failure is represented by the value failure of the patient component, and so is referred to as ErrorIn-Patient.Out1. For the purpose of simplicity, the failure is presented in the results shown in this chapter as **Reaction**s.

The patient's DoB is entered into the HIS together with other information. Value failure of DoB which could be caused by wrong data entry is represented as ErrorIn-DoB_out. An omission of the DoB causes problems and it is classified here as an output deviation of the HIS. Omission of DoB is represented here as OmissionOf-DoB_out. Moreover, HIS internal malfunctions can cause output failures of the HIS; these are represented as HWError, SWError, and DataEntryError.

Similarly, the clinician — who is included in the workflow as a separate component — can have output deviations. The clinician might make data entry errors which are represented here as

IDDataEntryError (error in entering patient ID) or DoBDataEntryError (error in entering patient DOB). The output deviations are represented as ErrorIn-PatientID_out and ErrorIn-DoB_out.

RIS internal malfunctions may include software or hardware malfunction, represented as HWError, SWError. RIS as well as potentially receiving the wrong DoB from the Clinician, represented as DoBDataEntryError. In addition to these malfunctions, the RIS may suffer from failure of the preparation data, which is PrpDataEntryError. Therefore, output deviations at the RIS could be the omission of DoB or having the wrong DoB or having the wrong preparation information or omission of preparation information; these are represented respectively as: OmissionOf-DoB_out, ErrorIn-DoB_out, ErrorIn-PatientPreparationInfo, and OmissionOf-PatientPreparationInfo.

ModalityWorkList is a database that keeps orders' scheduling information and patients' information. It can have two basic events, which are software error or hardware error. These are represented as SWError and HWError respectively. Each of the ModalityWorklist inputs has its own failure but in the CT scan scenario, some failures have been considered and the others are ignored as they are assumed to be free from failures. The failures that are to be analysed are the failure of the value of the DoB and the failure of the preparation information output as either a value failure or omission of this value. These are represented as ErrorIn-DoB_out, ErrorIn-Prep_out, and OmissionOf-Prep_out.

When it comes to the image acquisition modality itself, at the time of the test the radiologist should verify some information with the patient, e.g. DoB, name, and preparations for the test. The process of verbal verification is represented as a separate component that may have two basic events, both human errors; they are represented as: DoBHumanError and PrepHumanError. Failures of the output of this component are represented as: OmissionOf-DOBVer and OmissionOf-PrepVer.

Fixing the cannula for the CM is also considered as a separate component, and annotated with the failures that might be a human error (represented as HumanError); the output failure of this component is represented as ErrorIn-Out1.

The CM dose is considered as a subcomponent of the image acquisition modality and failure of this is giving the wrong dose to the patient. This is represented as ErrorIn-Dose. Other reactions are considered as well as subcomponents of the image acquisition modality component, which may have a failure that is represented as V-Reaction, where the patient has some reactions or side effects when he/she is not supposed to have them. These kinds of reactions that happen according to not following the preparation guidelines by the patient are separated from the CM dose-dependent reactions.

The output of the CMDose component and OtherReactions component goes to the Reaction component. This separate component is also annotated with possible failures. The output deviation of this component is any type of reaction by the patient. This is represented as ErrorIn-Reaction.

The reactions component is connected to the patient who is having these reactions. The image output is connected to the PACS component that receives the images and archives them into a database.

PACS and the diagnostic workstations component were not annotated with failure information for the purpose of this scenario. It is assumed that they are free of errors and they only propagate failures. A comprehensive analysis must consider failures of these components and annotate them with all possible errors to get the root causes for other possible failures of the workflow.

Table 5 Failure information for the CT scan scenario

Component Name	**Basic Events**	**Output Deviations**	**Failure Expressions**
HIS	HWError SWError DataEntryError	OmissionOf-DOB_out ErrorIn-DOB_out	SWError OR DataEntryError DataEntryError
Clinician	IDDataEntryError DoBDataEntryError	ErrorIn-PatientID_out ErrorIn-DOB_out	IDDataEntryError DOBDataEntryError OR ErrorIn-DOB

RIS	HWError SWError DoBDataEntryError PrepDataEntryError	OmissionOf-DOB_out ErrorIn-DOB_out ErrorIn-PatientPreparationInfo OmissionOf-PatientPreparationInfo	SWError OR DOBDataEntryError DOBDataEntryError OR ErrorIn-DOB PrepDataEntryError SWError OR PrepDataEntryError
Modality Worklist	HWError SWError	ErrorIn-DOB_out ErrorIn-Prep_out OmissionOf-Prep_out	ErrorIn-DOB ErrorIn-PatientPreparationInfo SWError OR OmissionOf-PatientPreparationInfo
Verbal Verification	DoBHumanError PrepHumanError	OmissionOf-DOBVer OmissionOf- PrpVer	DOBHumanError PrepHumanError
Cannula Fixation	HumanError	ErrorIn-Out	HumanError
CMDoseCalculation	HumanError	ErrorIn-DoseCalc	(ErrorIn-DOB AND OmissionOf-VerbalVerification) OR CalcHumanError
CMDose		ErrorIn-Dose	ErrorIn-DoseCalc OR MeasurementError
OtherReaction		ErrorIn-Reaction	ErrorIn-PatientPrep AND OmissionOf-PrepVer
Reaction		ErrorIn-Reaction	ErrorIn-CMDoseDepReaction OR ErrorIn-OtherReaction

4.2.5 Fault Tree and FMEA Synthesis and Analysis

The components of the model were annotated with the corresponding failure information and then performed with the root cause analysis. HiP-HOPS synthesises and analyses the system fault trees and produces the FTA and FMEA results, which show how the value failure in an input and the component failures (or their combinations) can lead to failure, causing unintended reactions or side effects for the patient.

The following figure shows the FTA:

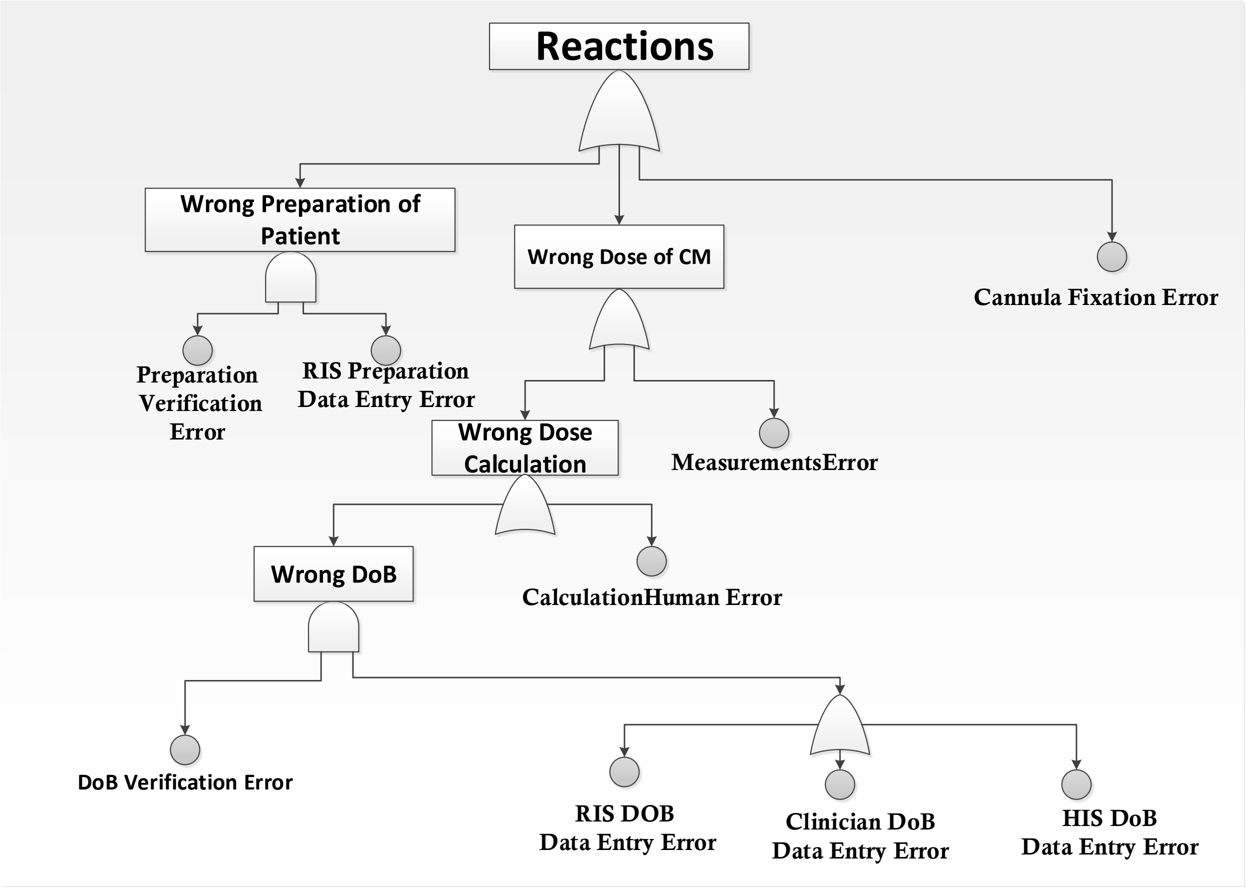
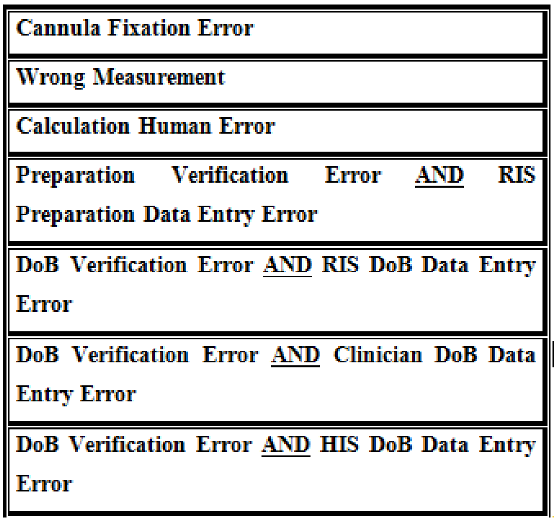


Figure 21 FTA result for the CT scan scenario

The following list shows the MCSs from the FTA:



Cannula Fixation Error

Wrong Measurement

Calculation Human Error

Preparation Verification Error AND RIS Preparation Data Entry Error

DoB Verification Error AND RIS DoB Data Entry Error

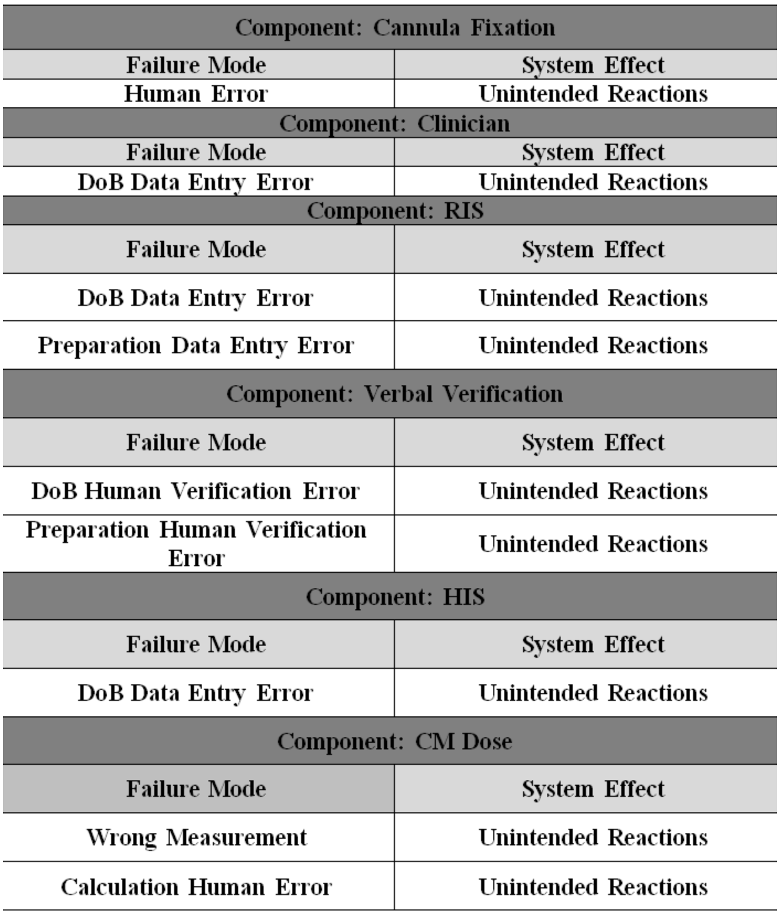
DoB Verification Error AND Clinician DoB Data Entry Error

DoB Verification Error AND HIS DoB Data Entry Error

Figure 22 MCS result for the CT scan scenario

The following table shows the resulting FMEA table of the direct and further effects:

Table 6 FMEA of direct and further effects



Component: Cannula Fixation	
Failure Mode	System Effect
Human Error	Unintended Reactions
Component: Clinician	
Failure Mode	System Effect
DoB Data Entry Error	Unintended Reactions
Component: RIS	
Failure Mode	System Effect
DoB Data Entry Error	Unintended Reactions
Preparation Data Entry Error	Unintended Reactions
Component: Verbal Verification	
Failure Mode	System Effect
DoB Human Verification Error	Unintended Reactions
Preparation Human Verification Error	Unintended Reactions
Component: HIS	
Failure Mode	System Effect
DoB Data Entry Error	Unintended Reactions
Component: CM Dose	
Failure Mode	System Effect
Wrong Measurement	Unintended Reactions
Calculation Human Error	Unintended Reactions

To summarise, the FTA and FMEA results show that the following faults may lead to the failure in the CT scan scenario (which is in this case getting unwanted reactions or what can be called adverse events by the patient):

- Human error in fixing the cannula for the CM, where the radiologist or the nurse makes an error in placing the cannula prior to the scan. This mistake cause problems for the patient as the CM is injected through the scan, which might lead to both side effects of the CM or an extra dose of radiation because the radiologist might need to repeat the scan.

- Data entry error for the DoB by the clinician combined with an error in the verbal verification of the DoB by the radiologist at the time of the scanning. This combination of errors might lead to an extra dose of radiation and/or extra dose of CM, which may put the patient's life at risk.

- Data entry error for the DoB by the radiologist combined with an error in the verbal verification of the DoB by the radiologist at the time of the scanning. Again, this focuses our attention on the importance of the verification of the DoB by the radiologist at the time of the scanning.

- Data entry error for the DoB in the HIS combined with an error in the verbal verification of the DoB by the radiologist at the time of the scanning.

- Data entry error for the preparation guidelines by the radiologist combined with an error in the verbal verification of the preparation guidelines by the radiologist at the time of the scanning. This means, if the patient received the wrong preparation guidelines or did not receive them at all, then at the time of the scanning, if the radiologist does not make sure about their accuracy (and whether they were followed by the patient or not), the patient will experience reactions.

- Wrong measurements to calculate the dose of CM can directly cause the unwanted reactions. This might happen because of not understanding the units of measurement, or using incorrect equipment to measure the dosages.

- Human error in calculating the dose can directly cause the reactions. This may happen through making slips in calculations that result in an incorrect dose.

This means that if there is any error in the data entry in HIS, clinician, and the RIS, combined with a situation where the radiologist does not verify (or verifies incorrectly) the data for DoB or preparation information, unintended reactions towards the patient will occur.

4.2.6 Probability Analysis

Here, in this case study, the results from qualitative analysis were enough to refine and reengineer the processes and tasks within the workflow. The healthcare team did not ask for quantitative results about the failure information. The team accepted the replacements and the suggestions and the final workflow was verified and accepted as an official workflow.

4.2.7 New Workflow Design and Accepting the Workflow

The hazard severity is medium, and the resultant MCSs were of order 1 and 2. The healthcare team accepted the workflow as an official workflow with maintaining some conditions related to emphasising the critical tasks. For example, human error in fixing the cannula, wrong measurement or calculations for the dose can contribute directly to causing unintended reactions. Thus, each radiologists or nurses who performs any of these tasks should be informed about potential failures that the task may cause and about their direct and indirect effects on the patient. The calculations and measurements tasks can probably be performed by more than one person, which will require both of them to accomplish the task incorrectly to cause the hazard to happen.

Moreover, if possible (depending on the financial situation in the hospital) adding extra functionality to the HIS or RIS or both can help in avoiding the hazard; for example, a barcode scanning system can help to avoid data entry errors by radiologists and clinicians. If this is not possible, marking the verification of DoB and verification of preparation as critical tasks which should be confirmed before actions can be done has the potential to help in avoiding such consequences.

4.3 Safety Analysis of RIS/PACS Workflow- Wrong Treatment Scenario

This section describes another scenario for the application of SAFE-FLOW to the previous workflow within the same radiology department.

The following subsections describe the steps:

4.3.1 Workflow Scenario Documentation

As mentioned previously, the established team specified many other scenarios to be analysed for the same workflow architecture, where additional components may be required. However, for simplicity, the thesis analyses only two scenarios.

Here, in this scenario, the same workflow is used. Again, the workflow starts with the data stored in the EHR; the clinician is responsible for sending the data to the RIS, the information to be entered includes again the following: Patient name, Patient National Number (ID), DoB, Age, Address, Patient medical Information, and Order Information. Later scheduling information can be added into the RIS by a radiologist or a nurse.

Next, the RIS output goes directly to the MWL, which is exposed to hardware and software errors. In the image acquisition modality the patient is supposed to have an examination that is specified in the order. The output of the image acquisition modality is the patient id, patient name and the image itself. This output is transferred automatically to the PACS.

When PACS receives this output information it archives it and sends it to the diagnostic workstation to be seen by the radiologist. The radiologist interprets the examination and produces a report as an output. This report is then passed to the clinician to make the diagnosis and to deliver the treatment.

4.3.2 Workflow Modelling

The following figure shows the model that represents the radiology workflow with additional components added for the wrong treatment scenario:

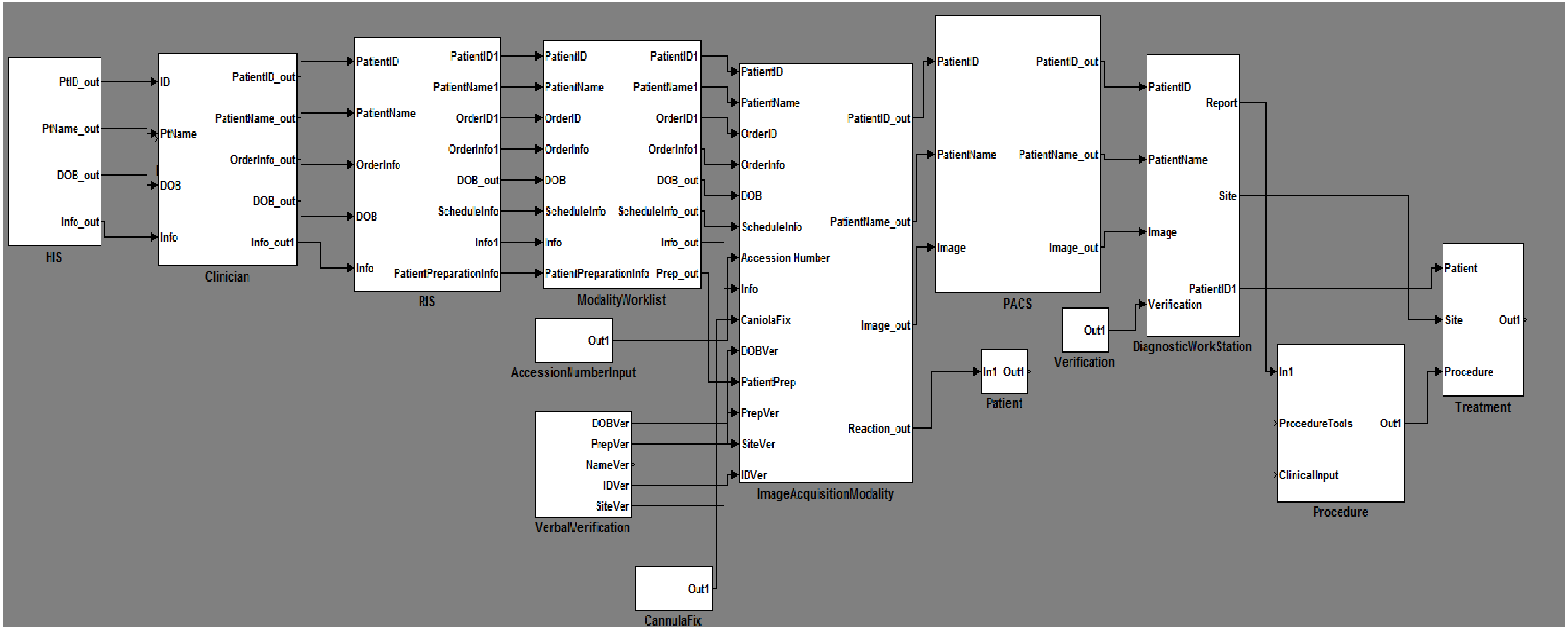


Figure 23 The Radiology workflow- treatment scenario

4.3.3 Hazards Identification and Risk Assessment

As mentioned in the previous scenario, potential errors at component level were discussed with the healthcare team and possible hazards were identified. The hazard analysed here is delivering the wrong treatment to the patient, which was described as level D severity (high).

4.3.4 Failure Annotation

Here, the model was extended with failure information. This information describes how a failure in the component output is caused by a propagation of failure from the component input or the internal malfunction of the component itself. Failure is represented as mentioned previously in the format of "FailureType-ComponentName.ComponentPort".

The scenario on providing the wrong treatment to the patient was analysed. As described by the workflow architecture, the treatment is considered as a separate component; the value failure of the output is represented as ErrorIn-Out1. For simplicity, in presenting the results the value failure of the output was referred to as "wrong treatment".

The patient's ID and DOB are entered into the HIS together with other information. Incorrect data entry may cause a value failure of ID and DoB which was denoted as ErrorIn-ID_out, and ErrorIn-DoB_out. Also omission of the DoB which is denoted as OmissionOf-DoB causes problems and it is classified here as an output deviation of the HIS. Moreover, HIS internal malfunctions can cause output failures of the HIS; these are represented as HWError, SWError, and DataEntryError.

Similarly, the clinician — who is included in the workflow as a separate component — can have output deviations. The clinician might make data entry errors which are represented here as IDDataEntryError or DoBDataEntryError. The output deviations are represented as ErrorIn-PatientID_out and ErrorIn-DoB_out.

RIS internal malfunctions may include software or hardware malfunction, represented as HWError, SWError. RIS may also receive wrong ID and wrong DoB from the Clinician, represented as IDDataEntryError and DoBDataEntryError. Therefore, output deviations at RIS could be having the wrong ID, omission of DoB, or having the wrong DoB; these are represented respectively as ErrorIn-ID_out, OmissionOf-DoB_out, ErrorIn-DoB_out.

MWL can have two basic events, which are a software error or a hardware error. These are represented as SWError and HWError respectively. Each of the ModalityWorklist inputs has its own failure but in the CT scan scenario, some failures have been considered and the others are ignored as they are assumed to be free from failures. The failures which are to be analysed are: the failure of the value of the ID, and the value failure of the DoB either as a value failure or omission of this value. These are represented as ErrorIn-ID_out, ErrorIn-DoB_out.

When it comes to the image acquisition modality, at the time of the test, the radiologist should verify certain information with the patient, e.g. ID, DoB, name, and the site of the image (e.g. right/left). The process of verbal verification is represented as a separate component that may have three basic events, which are human errors, represented as IDHumanError, DoBHumanError and SiteHumanError. Failures of the output of this component are represented as: OmissionOf-IDVer, OmissionOf-DOBVer and OmissionOf-SiteVer. Basic events for the image acquisition modality are represented as ImageUnmarked, and ImageMislabled. These basic events happen when the image is mislabelled with the wrong patient or the wrong data, such as having the image for the right lung instead of the left. The other case may happen when the image has the right information but is unmarked for specifying the site, and therefore the radiologist produces the wrong report.

The output deviations of the PACS component are represented as ErrorIn-Patient_out and ErrorIn-Image_out. The diagnostic workstations component has the HumanError as a basic event, and has a number of output deviations: ErrorIn-Report, ErrorIn-Site, and ErrorIn-PatientID.

The treatment procedure may have an output deviation as well, and this is represented as ErrorIn-Out1, which might be caused by ErrorIn-In1 OR ProcedureTool OR ClinicalInput.

Table 7 Failure information- treatment scenario

Component Name	Basic Events	Output Deviations	Failure Expressions
HIS	HWError SWError DataEntryError	OmissionOf-DOB_out ErrorIn-DOB_out ErrorIn-PtID_out	SWError OR DataEntryError DataEntryError DataEntryError
Clinician	IDDataEntryError DoBDataEntryError OrderInfoError	ErrorIn-PatientID_out ErrorIn-DOB_out ErrorIn-OrderInfo_out	IDDataEntryError OR ErrorIn-ID DOBDataEntryError OR ErrorIn-DOB OrderInfoError
RIS	HWError SWError DoBEataEntryError PrepEataEntryError IDDataEntryError	OmissionOf-DOB_out ErrorIn-DOB_out ErrorIn-PatientPreparationInfo OmissionOf-PatientPreparationInfo ErrorIn-PatientID1 ErrorIn-OrderInfo1	SWError OR DOBDataEntryError DOBDataEntryError OR ErrorIn-DOB PrepDataEntryError SWError OR PrepDataEntryError ErrorIn-PatientID OR IDDataEntryError ErrorIn-OrderInfo

Modality Worklist	HWError SWError	ErrorIn-DOB_out ErrorIn-Prep_out OmissionOf-Prep_out ErrorIn-PatientID1 ErrorIn-OrderInfo1	ErrorIn-DOB ErrorIn-PatientPreparationInfo SWError OR OmissionOf-PatientPreparationInfo ErrorIn-PatientID ErrorIn-OrderInfo
Verbal Verification	DoBHumanError PrepHumanError IDHumanError SiteHumanError	OmissionOf-DOBVer OmissionOf- PrpVer OmissionOf-SiteVer OmissionOf-IDVer	DOBHumanError PrepHumanError SiteHumanError IDHumanError
Diagnostic Workstation	HumanError	ErrorIn-Report ErrorIn-Site ErrorIn-PatientID	HumanError ErrorIn-Image ErrorIn-PatientID
Procedure	ProcedureTool ClinicalInput	ErrorIn-Out1	ErrorIn1 OR ProcedureTool OR ClinicalInput
Treatment		ErrorIn-Out1	ErrorIn-Patient OR ErrorIn-Site OR ErrorIn-Procedure

4.3.5 Fault Tree and FMEA Synthesis and Analysis

The components of the model were annotated with the corresponding failure information and then the root cause analysis was performed. HiP-HOPS synthesises and analyses the system fault trees and produces the FTA and FMEA results, which show how the value failure in an input and the component failures (or their combinations) can lead to failure, causing the wrong treatment of the patient.

The following figure shows the FTA:

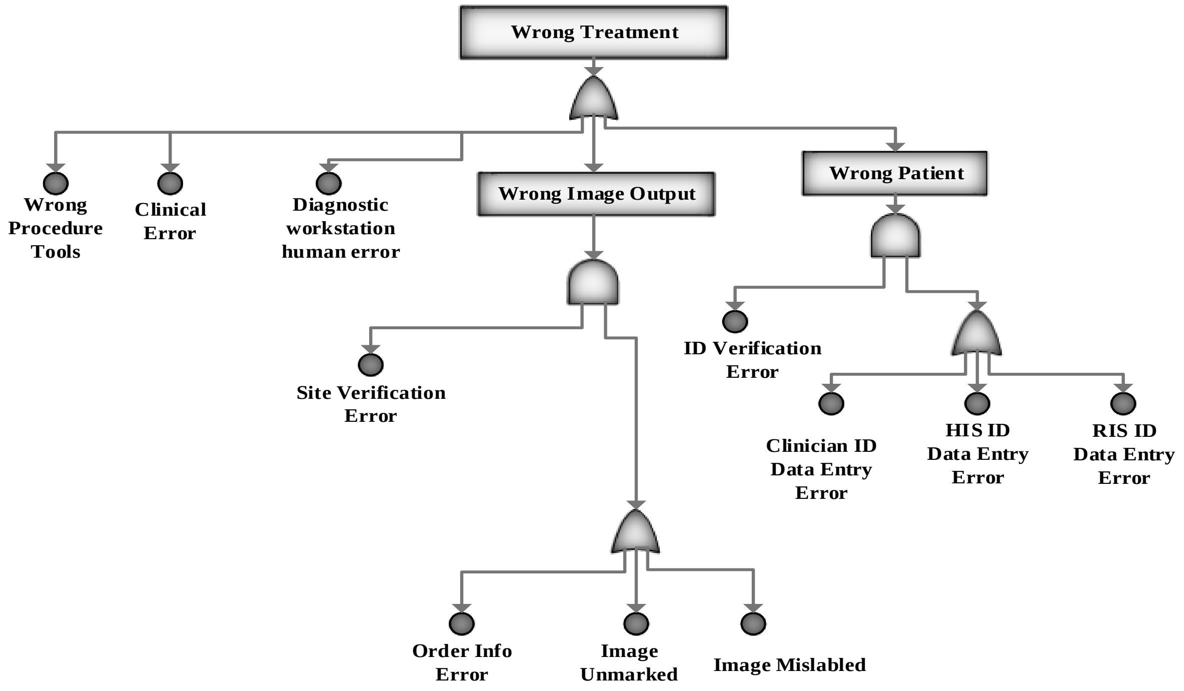
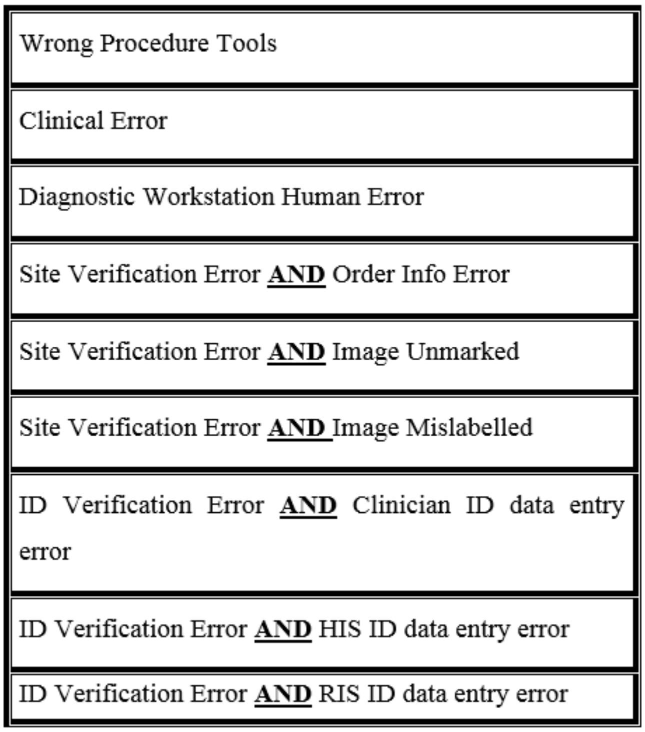


Figure 24 FTA- treatment scenario

The following list shows the MCS from the FTA:

Table 8 MCS- treatment scenario

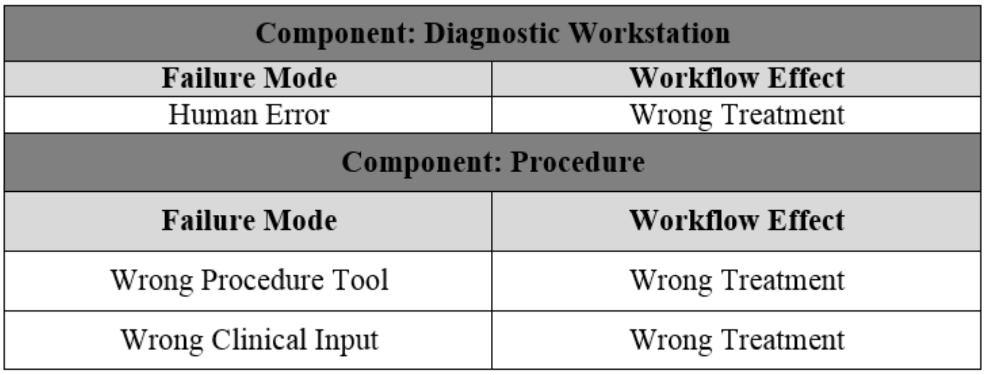


Wrong Procedure Tools
Clinical Error
Diagnostic Workstation Human Error
Site Verification Error **AND** Order Info Error
Site Verification Error **AND** Image Unmarked
Site Verification Error **AND** Image Mislabelled
ID Verification Error **AND** Clinician ID data entry error
ID Verification Error **AND** HIS ID data entry error
ID Verification Error **AND** RIS ID data entry error

The MCS is the smallest — i.e., necessary and sufficient — combination of primary events causing the top event. All of the basic events in the set need to occur to cause the top event. It directly links the top event to the primary events, and the complete set of the MCS provides the complete set of causes of the top event.

The following table shows the resulting FMEA table of the direct effects:

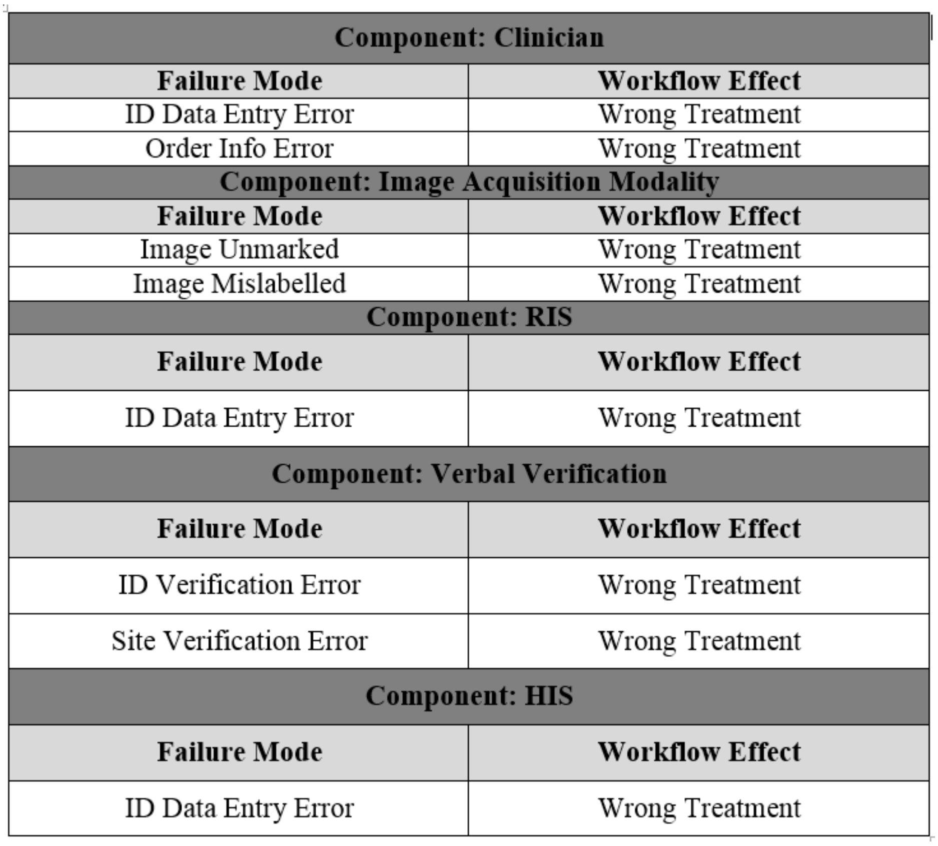
Table 9 FMEA direct effects- treatment scenario



Component: Diagnostic Workstation	
Failure Mode	**Workflow Effect**
Human Error	Wrong Treatment
Component: Procedure	
Failure Mode	**Workflow Effect**
Wrong Procedure Tool	Wrong Treatment
Wrong Clinical Input	Wrong Treatment

The following table shows the resulting FMEA table of the further effects:

Table 10 FMEA of further effects- treatment scenario



Component: Clinician	
Failure Mode	**Workflow Effect**
ID Data Entry Error	Wrong Treatment
Order Info Error	Wrong Treatment
Component: Image Acquisition Modality	
Failure Mode	**Workflow Effect**
Image Unmarked	Wrong Treatment
Image Mislabelled	Wrong Treatment
Component: RIS	
Failure Mode	**Workflow Effect**
ID Data Entry Error	Wrong Treatment
Component: Verbal Verification	
Failure Mode	**Workflow Effect**
ID Verification Error	Wrong Treatment
Site Verification Error	Wrong Treatment
Component: HIS	
Failure Mode	**Workflow Effect**
ID Data Entry Error	Wrong Treatment

To summarise, the FTA and FMEA results show that the following faults may lead to the failure of the CT scan scenario (which is in this case giving the wrong treatment to the patient):

- Human error at the diagnostic workstation, either by making an error in reading the image or the wrong specification of the site. The wrong specification of the site is usually a human error at the scheduling, at the order information level or a human error in the diagnostic workstation itself;
- The use of the inappropriate procedure tools;
- Incorrect clinical input of the procedure;

- Data entry error for the ID by a clinician, combined with an error in the verbal verification of the ID by the radiologist at the time of the imaging. This combination of errors may lead to the wrong treatment because of producing a report for the wrong patient;
- Data entry error for the ID in the RIS combined with an error in the verbal verification of the ID by the radiologist at the time of the imaging. Data entry error for the ID in the HIS combined with an error in the verbal verification of the ID by the radiologist at the time of imaging;
- Clinician order information error combined with the site verbal verification;
- Image unmarked at the image acquisition modality combined with site verification error;
- Image mislabelled with the wrong study combined with site verification error.

This means if there is any error in the data entry in HIS, clinician, and the RIS, combined with a situation where the radiologist does not verify (or verifies incorrectly) the data for ID or site information, the wrong treatment for the patient will occur.

4.3.6 Probability Analysis

Again, in this scenario, the qualitative analysis results did not show a need for a costly replacement of the existing components, probabilistic analysis was not necessary.

4.3.7 New Workflow Design and Accepting of the Workflow

The healthcare team accepted the constructed workflow with maintaining some conditions to avoid the analysed hazard. The results showed three direct causes for the hazard that are explained earlier:

- Human error at the diagnostic workstation;
- The use of the inappropriate procedure tools;
- Incorrect clinical input of the procedure.

A human error at the diagnostic workstation is very critical, so this task can be avoided for example by reading the image by more than one specialist and verifying the site. Moreover, the diagnostic workstation itself should be checked and maintained regularly to ensure that it will not cause wrong specification of the site due to hardware or software errors. The use of inappropriate procedure tools and incorrect input of the procedure by clinician can be avoided by driving the attention of humans who accomplished such tasks to how critical they are and to what they can cause if not verified and accomplished correctly.

For the order 2 cut sets, site verification is very important because even with having the wrong order information, image unmarked or image mislabelled the failure will not occur if the site is verified. The same thing is applied to the verification of patient ID, where even if the wrong ID is provided at the imaging time it will not cause the top event if verified.

Therefore, because the workflow will be available to the people involved in it, and as part of building awareness, they should be made aware of the critical tasks and the potential failures they can cause so that they are able to accomplish them properly and safely.

4.4 Discussion of the Achieved Benefits

The application of SAFE-FLOW has led to the automated identification of the root causes of potential failures, which allows greater understanding of the factors contributing to the undesired event that can potentially lead to a serious clinical risk. This enables the identification of weak points in the workflow, which could then be effectively addressed and improved.

For example, through the simple structure in this example, the application of SAFE-FLOW shows the ability to systematically assist in the identification of failures in the workflow (i.e. failure in the verbal verification or failure in the data entry of the DoB) and the identification of the failures in the system (i.e. hardware or software error in the MWL). This information can be used to guide the improvement in the redesign of both the system and the workflow. The system can be improved by targeting the areas where highly-reliable components and fault tolerant mechanisms can be prioritised and introduced to make the architecture more robust and fault tolerant (e.g. the development of new protocol that emphasise the verbal verification as a vital task).

Moreover, the workflow can be improved by designing the workflow with taking the safety analysis into considerations and to use the results of the analysis to target areas where reliable components (in this case, the components are processes) can be introduced. The workflow should have exact determination of the processes, tasks, procedures, and tasks that must be done by each party.

Having detailed workflows with a detailed analysis of the failure behaviour has the potential to give healthcare organisations good material to be given for the medical staff in safety workshops. Moreover, detecting the potential design flaws early before serious problems happen can help as well in giving the medical staff the awareness they require and help in redesigning the workflow to produce an effective and fault-free workflow.

Therefore, the inclusive safety analysis has the potential to develop a safety philosophy in the radiology department. This comprehensive analysis may have a positive effect on safety performance and patient safety improvement in radiology which should include and emphasize overall patient safety within the workflow in addition to radiology-specific safety issues such as MRI safety, radiation dose exposure, and contrast reactions (Donnelly *et al.*, 2009). Actors like clinicians and radiologists should have better awareness of the high-risk environment in which they work and that they actively lead and participate in activities to reduce risk.

For example, caution is recommended when surgical treatments are suggested depending on radiographic results, which may be disposed to workflow errors; the clinician needs to understand the details of the case rather than relying exclusively on static radiographic results (Clohisy *et al.*, 2009).

The simple act of undertaking a safety analysis in this way helps to improve understanding of the behaviour of the workflow and its potential for failure, thus highlighting areas where additional checks or amendments to the workflow need to be introduced. The automation then additionally helps deal with the complexity and time cost issues, offering benefits over a simple manual analysis. While in this case there were only order 2 MCS, analyses that are more comprehensive might introduce even higher order MCS that are even more difficult to spot manually, potentially highlighting issues that are not even apparent from a manual analysis.

In general, workflow models can be used to train people by providing a clear picture of their role and tasks in the overall organisation.

4.5 Conclusion

It is concluded that SAFE-FLOW is applicable to this area of healthcare and provides benefits through a combination of detailed information on possible risks and descriptive safety analysis based on experts' opinion. This provides a mechanism for the systematic identification of both adverse events and possible safeguards in clinical workflows, which is important in terms of identifying the causes of possible adverse events before they happen and therefore helping to prevent harm to the patient. Moreover, SAFE-FLOW helps in the clear definition of the workflow including its processes and tasks, which provides a valuable opportunity for formulation of safety improvement strategies.

5 Evaluation

The main purpose of this chapter is to evaluate SAFE-FLOW and to examine its characteristics, activities and effects. In other words, the purpose is to review SAFE-FLOW to improve its productivity. The chapter offers a novel evaluation design over three levels through which SAFE-FLOW is systematically evaluated.

5.1 Evaluation Design

The evaluation of SAFE-FLOW is designed to be prepared over three levels. The first level is testing the usability of SAFE-FLOW through the case study. Then the second level evaluates SAFE-FLOW through applying an evaluation framework that is adopted from the literature. Finally, the third level compares SAFE-FLOW with other methods that can be used for the same purpose.

The following figure demonstrates the levels of evaluation:

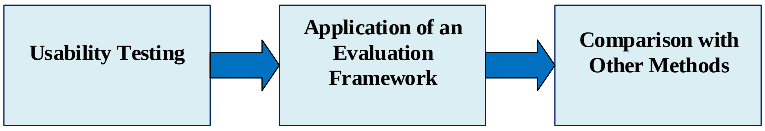

Usability Testing
Application of an Evaluation Framework
Comparison with Other Methods

Figure 25 Evaluation design: Evaluation over three levels

This evaluation design is generic and has the potential to help in evaluating the application of computer science and safety engineering approaches in healthcare. In particular, it can help to evaluate the use of safety analysis approaches in healthcare.

Those three levels are explained in details in the following sections.

5.1.1 Usability Testing

Usability testing (see Chapter 2) could be the best way to understand how the real users (the healthcare team and the safety analyst) experience SAFE-FLOW. However, setting SAFE-FLOW in practice (with engaging a safety analyst) is time-consuming and the additional cost required for doing so make it difficult. Therefore, usability testing is accomplished through the application of SAFE-FLOW to the case study. The researcher represents the safety analyst and the healthcare team represents other users.

The purpose here is to get insights about problems and challenges of SAFE-FLOW application instead of quantifying the usability testing results. In other words, the idea is to get a better understanding of problems that may face such application. For example, for the safety analyst, the safety analysis technique is applied to an atypical domain, which is probably out of the area of expertise for a typical safety analysis. Furthermore, healthcare workers may find the safety analysis process challengeable because it is again out of their area of knowledge. The usability issues noted while accomplishing the case study include the following:

1. Some of the healthcare staff members were found to be annoyed with being involved in the analysis process. Their facial expressions showed that they were not happy with this extra work. This may delay the application of SAFE-FLOW unless hospitals deal with this issue carefully.
2. When asked to provide a full description of a certain process, the healthcare team sometimes give a general picture where they do not give necessary information because they think it is default information that everybody should know. However, an inexperienced member of healthcare staff may not know such details and how important they are to produce the right service to the patient.

Ignoring the previous issues would affect the usability of SAFE-FLOW negatively; the following recommendations and extra steps in SAFE-FLOW can help to overcome the previous issues and can help in achieving the usability requirements:

1. Specify the involvement of healthcare staff within the safety analysis process in the hospital as one of their job responsibilities. This would help in building a sustainable safety analysis culture.
2. The validation step in SAFE-FLOW that follows the workflow modelling can help to overcome the second issue, where the analyst checks the model and validates it with the healthcare team

before continuing the process. The analyst's responsibility lies in checking the detailed processes and making sure that there are no missing tasks.

In terms of usability from the analyst's perspective, SAFE-FLOW is tool-based and the used tool (HiP-HOPS) has a graphical interface, which is relatively easy to use once the analyst is trained. An analyst requires training to use the tool and his/her ability to create the models has a non-trivial impact on the accuracy of the models. However, SAFE-FLOW suggests that models should be checked and approved by healthcare experts before proceeding with any other steps. Moreover, the used tool is uncomplicated in comparison with other methods like manual approaches and more formal techniques like model checking.

Thus, SAFE-FLOW can identify and represent the causal relationships between different components in a systematic manner. Moreover, it can help in providing a logical foundation to investigate the barriers that can improve the safety of clinical workflows.

5.1.2 The Application of the Evaluation Framework

The advantages of using systematic and technical approaches for safety analysis in healthcare over the use of classical safety analysis methods are readily discernible. However, without evaluation information, hospitals interested in considering the adoption of such approaches may not be able to determine the benefits they would achieve from the use of SAFE-FLOW. Therefore, this section considers the application of a systematic evaluation framework to evaluate SAFE-FLOW.

The US Department of Health and Human Services, Centers for Disease Control and Prevention (CDC) published a framework for Program Evaluation in Public Health in 1999. The following figure illustrates the steps involved in the framework and the set of standards for conducting an evaluation:

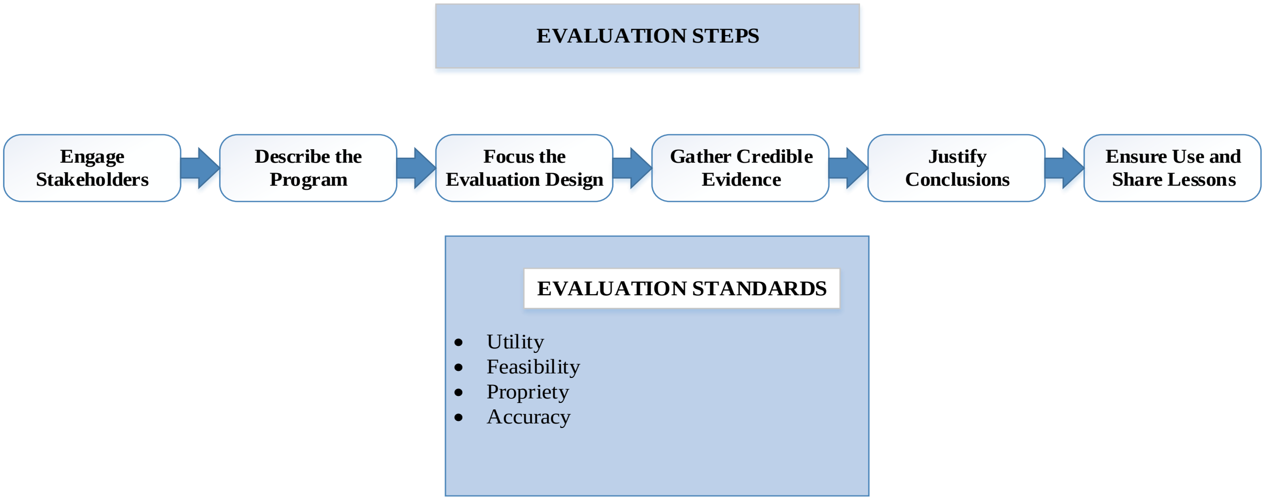


Figure 26 CDC's Framework for Program Evaluation in Public Health (U.S. Department of Health and Human Services, 1999)

The framework is applied to evaluate the use of SAFE-FLOW within hospitals; the purpose is to provide a practical evaluation that can be used by decision makers and healthcare organisations. In other words, the evaluation findings can determine if SAFE-FLOW has the potential to contribute to enhancing patient safety. Accordingly, if any hospital considers the adoption of SAFE-FLOW, this evaluation can help in the decision to adopt or not depending on the available evaluation findings. Moreover, the evaluation can help hospitals to take actions depending on the evaluation results to increase the utility and the impact of SAFE-FLOW.

Firstly, the evaluation steps were translated into a number of stages to perform the evaluation, and then the evaluation process is assessed depending on the standards proposed by the framework.

The following sections explain the application of the evaluation steps in detail:

1. **Engaging key participants**

This step indicates the need to specify the key participants who are expected to have an investment in what will be learned from the evaluation and who must be involved in the evaluation process. In this study, those participants are organised into three groups:

- The first group consists of the healthcare team who were originally involved in the application process within the Jordanian hospital;
- the second group consists of four clinicians from other domains who are working in the National Health Service (NHS);
- the third group involves an academic expert in clinical workflows who also has knowledge about the used tool. This expert has several decades of research experience in safety analysis in computer science.

The reason behind the selection of the first group was that they can represent SAFE-FLOW users and can reflect their experiences in the application process. The second group was chosen to represent potential users who were not involved and so were separate to the original application process and who represent healthcare experts from the United Kingdom. The academic expert in the third group can validate the approach in terms of his knowledge in both clinical workflows and the used tool.

Therefore, there are three sources of information to evaluate the approach:

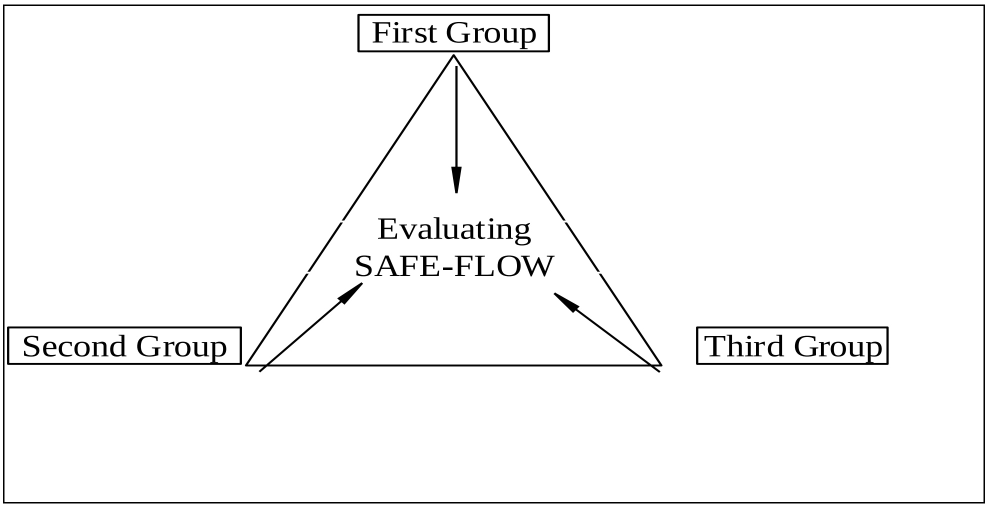


Figure 27 Sources of information for evaluating SAFE-FLOW

The three groups altogether can help in making the decision to adopt SAFE-FLOW or not. The format of their involvement was determined to be semi-structured interviews.

2. Detailed description of SAFE-FLOW

SAFE-FLOW was carefully described to the participants who were involved in the evaluation process. It was relatively straightforward to evaluate SAFE-FLOW with the members who were originally involved in the safety analysis process (the case study), because they had developed an understanding of the models used and the steps of SAFE-FLOW during its application.

SAFE-FLOW was also explained in detail to the other participants. Although some difficulties were found while explaining the process (especially while explaining the used models) which slowed the process, these were addressed and the evaluation was possible.

3. Specification of the evaluation aim and questions

The evaluation design and the actions required to carry it out were specified. In addition, the evaluation questions and aim were identified. The evaluation process aims at answering the following questions:

- How easy were the used models to be understood by healthcare staff?
- How practical was the involvement of staff in the safety analysis process?
- Can the models be used effectively to represent clinical workflows? Do they reflect the communications and interactions within these workflows?
- How helpful is SAFE-FLOW in identifying failure modes and their effects and accordingly in improving workflows safety?

Answering the previous questions can effectively contribute to answering the main research question.

4. Gathering information through interviews

Information that is required to answer the evaluation questions and to achieve the evaluation aim was gathered through semi-structured interviews. Semi-structured interviews were chosen because the results obtained through semi-structured interviews can be compared with each other since all of the interviewees are asked to express their views about the same themes in a consistent way.

The chosen sample was deemed appropriate since the participants from the first group have knowledge about the approach; they were involved in the application process. Moreover, given the common features and characteristics of clinical processes, the second group of the four clinical experts from other fields was used to gauge their perspectives on the SAFE-FLOW approach. Involving those external participants added a contribution to the evaluation as the information given by them evaluated SAFE-FLOW itself and the models used, beyond purely focusing on the clinical content. Finally, the third group reflected an academic evaluation of the overall process.

Over the period of four weeks, 16 interview requests were sent out to various experts, using the sampling technique described above. Ten interviews were conducted over a period of five weeks. This show a high response rate of 62 percent, where 6 experts did not respond.

After considering the time available for evaluating the proposed approach and the available experts in the field a sample size of ten interviews, each between 30 and 60 minutes was considered appropriate.

While participants of the first group were involved in the original case study, the two other groups were not involved in it. The reason behind having the two other groups was to address any potential reinforcement issues where the first 5 interviewees had been involved in the original application of the process and this could have affected the resulting data. Getting agreement of data and results from other experts concurrently and having this iterative interaction between data and analysis is the essence of achieving reliability and validity (Morse *et al.*, 2008).

Interviewing another four experts who were not involved in the case study enabled new participants to be brought into the study in order to provide comparison data and to increase the scope and the appropriateness of the overall data (Morse *et al.*, 2008). The last interview with the academic expert was intended to assess and potentially confirm the validity of the approach and the validity of the results from the evaluation process itself.

Before conducting the actual interviews, a pilot test was performed for each set of questions in which questions were checked with participants. This helped to determine the flow in the questions and to refine them.

Regarding the steps followed to standardise the interviews in order to achieve reliability and accordingly validity, questions were read exactly as worded, with clarification where required. When the experts' answers to certain questions were not complete, they were asked to give a clear answer or further clarification. The interviewer recorded some of the interviews and took written notes to record the answers in the other interviews.

5. **Justifying conclusions through qualitative analysis and findings**

The data was analysed and the conclusions were reviewed to produce the final findings. The inductive approach used is a systematic procedure for analysing qualitative data. A general inductive approach for analysis of qualitative evaluation data in which the analysis is guided by specific evaluation objectives (Thomas, 2006) is used here to derive patterns and categories through interpretations made from interviews.

That is to say, the data analysis, which identifies domains and topics to be investigated, is guided by the evaluation objectives. The analysis was carried out through multiple reviews and interpretations of the interviews' raw data. As stated by Thomas (2006), although the findings that are derived using this way are influenced by the evaluation objectives outlined by the researcher, they are arose directly from the analysis of raw data not from prior expectations. The evaluation objectives support the analysis and provide it with a focus or a domain.

The primary mode of analysis is the development of categories from the raw data into a model or a framework that contain the key themes identified by the evaluator and the evaluator shapes the findings by his/her assumptions and experience (Thomas, 2006).

Thomas (2006) suggests analysing the raw data by more than one evaluator; in this research, this was substituted with having an overall evaluation with an independent academic evaluator (the third group in the evaluation approach).

The interview data was analysed, with repeated reviews of the data in order to get a general sense of the overall implications and the relevant themes were identified. After this identification of the key themes, the material was organised into segments of text to clarify the interpretation of the information and to label the data with appropriate terms. Two levels have been defined in the course of this data analysis, these are patterns and categories.

Each interview was divided into three main sections, each consisting of a number of different questions, which were designed to answer one of the evaluation questions:

Usability of the used models and usability of SAFE-FLOW	**Models ability to represent workflows**	**Improving the safety of clinical workflows**
How easy were the used models to be understood by healthcare staff? How practical was the involvement of staff in the safety analysis process?	Can the models used effectively represent clinical workflows? Do they reflect components and communications within these workflows?	How helpful is the used tool in identifying the failure modes and their effects? How helpful is SAFE-FLOW in improving clinical workflows and their safety?

Figure 28 the interviews' main sections

Research questions, evaluation questions, and interviewees' opinions were grouped to form patterns. Patterns were grouped according to relevance to categories and themes.

The first interview section discusses the usability of the used model and the pragmatism of SAFE-FLOW. A direct question about how easy the used models were to be understood was asked. 80% (8 out of 10) of the participants considered the used models easy to understand with some explanation from the analyst. The same participants stated that reasonable understanding could be achieved if there is an available support and clarification were available for the parts that they did not understand. The academic expert (the third group) stated that the model could benefit from incorporation of the concepts embodied in PROforma (Advanced Computation Laboratory Cancer Research UK, 2000).On the other hand, (20% (2 out of 10) who were healthcare experts thought that using other easier modelling languages (e.g. flowcharts) to model the workflow had the potential to make their job easier and to increase their understanding of the models. They clarified that they understood that the purpose of using such a modelling language is its compatibility with the analysis tool. However, they suggested that mapping the resultant models to one of the other modelling techniques, such as flowcharts, would be more helpful and easier for them to understand and follow. This is feasible, but the resulting models may require mapping into more than one diagram to represent all the features that are encapsulated within the model.

The following table demonstrates how participants' opinions were used to build patterns and categories.

Table 11 Participants' opinions regarding the usability of the models

Examples of Keywords used by interviewees (opinions)	**Patterns**	**Category**
• Reasonable understanding • Graphical representation	Ease of model understanding.	Usability of the models
• Mapping to more common models • User friendly	Vagueness of models.	

These positive results about the usability of the models used forms an important contribution toward the usability of SAFE-FLOW. This is because modelling of the workflow is one of the most important phases of SAFE-FLOW. Vagueness of the models, which was mentioned by 20% of the participants, can be resolved by mapping the final resulted models to a more user-friendly model.

All participants were asked questions regarding the models' capability to represent different workflow components, interactions and concepts. The capability of the models used to represent those concepts was explained and different workflow features were discussed with the participants. The purpose of such discussions was to look for any concepts that may not be reflected by the used models. The following table shows the resulted patterns and categories from this group of questions.

Table 12 Participants' opinions regarding the ability of the models to represent clinical workflow concepts

Examples of Keywords used by interviewees (opinions)	Patterns	Category
• System understanding • Expressing tasks and processes	Representing different components	Representing clinical workflows
• Communications between processes • Communications between humans and systems	Representing interactions between components	
• Sub processes and sub tasks • conditional tasks	Representing workflow concepts	

The results of this section showed that the models used are able to represent most of the workflow features. Sometimes, a complementary point of view to be taken into consideration while modelling the workflows is the temporal dimension (workflow dynamics), so that sequences in scenarios and degradations of components are considered (Weber *et al.*, 2012). Pandora (Walker, 2009) is identified as a potential future solution which can help in solving this problem.

The complex sequence of interactions between medical practitioner and patients can be modelled effectively. The healthcare team play an important role in the modelling process because they are involved in such interactions and can validate their correctness.

Interviews then took the path of asking an open question about how helpful the used approach was to improve clinical workflows. The purpose of this open question is to assist in answering the main research question. There was extensive agreement among the participants about the ability of SAFE-FLOW to improve the safety of clinical workflows; all of the participants agreed with this. Regarding enhancing patient safety through the application of SAFE-FLOW, 90% (9 out of 10) of the participants stated that well-defined and detailed workflows have the potential to improve patient safety. Because the approach used demonstrated its ability to improve the safety of the workflows, they believed that it has the potential to enhance patient safety. This group indicated their acceptance for the analysis results and explained that having such workflow specifications and confirming the safety of the steps involved in the workflow would have a good impact on the flow of the work in departments and overall in hospitals. The experts appreciated the ability of SAFE-FLOW to focus on processes and how the approach could be employed for several applications in clinical workflows. They added that SAFE-FLOW not only contributes to the safe delivery of clinical services but also to advancing and improving this delivery and this will have a direct effect on enhancing patient safety.

Only 10% (1 out of 10) of the participants differed. This participant was a nurse with eight years' experience. This participant considered the safety analysis process as extra work and added that the background and experience of the healthcare employees can help them to estimate potential failures while accomplishing a certain task; they can judge the consequences of their errors and accordingly avoid them. Moreover, this participant specified that there are other factors that affect patient safety and whilst SAFE-FLOW may improve the safety of clinical workflows and positively affect patient safety; other factors can obstruct enhancing patient safety.

In addition, 60% (6 out of 10) of the participants specified that the safety hazards of applying a change to the clinical workflow must be compared to the safety risks of not applying it, or of applying a different change. The hazards related to a certain change may be different from those related to the original workflow. Furthermore, including a change (e.g. incorporating a new information system) can create hazards that are specific to certain clinical services. SAFE-FLOW is found to be helpful in overcoming this issue as it can be used to compare those hazards and to compare safety analysis results. Those participants assumed that safety analysis should be performed when a healthcare organisation adopts new systems that introduce new workflows. They added that this could have a direct effect on improving patient safety. Other participants did not raise this issue and this was not scheduled within the interview questions.

Furthermore, all participants (100%) agreed that the resulting workflow models and the analysis results could be used as an educational tool to train healthcare staff, especially unexperienced staff members. Careful planning and modelling of the processes and tasks involved in the workflow and accepting them in a standard theoretical workflow would help to overcome having vague workflows in the operational phase. This can help in avoiding imprecise workflows that can confuse inexperienced medical staff and increase the chances for errors, especially for processes and tasks that are irregularly executed. Therefore, such workflow design and analysis can provide a clear picture of a staff member's role in delivering a specific clinical service.

In addition, participants specified that using the resulting workflows in the training process have the potential to promote the level of awareness of the trainees through identifying errors that may cause adverse events and therefore may threaten patient safety. Such awareness has the potential to help in establishing a solid base for the safety culture within healthcare organisations and accordingly improve and enhance patient safety.

The following table demonstrates the participants' opinions about improving clinical workflows by using SAFE-FLOW.

Table 13 Participants' opinions about improving clinical workflows and their safety through using SAFE-FLOW

Examples of Keywords used by interviewees (opinions)	Patterns	Category
• to improve work • to perform their tasks effectively • to reduce errors and mistakes	Improvement in skills associated with accomplishing processes.	Improving the safety of clinical workflows
• innovative technique • redesign and create solutions • redesign to improve safety	Novel way of thinking Refining workflows to improve safety	
• many factors can affect the improvement of patient safety • may not lead to patient safety	Safety analysis plays a role in enhancing patient safety.	

The following figure shows how clinical workflows can be improved by the use of SAFE-FLOW:

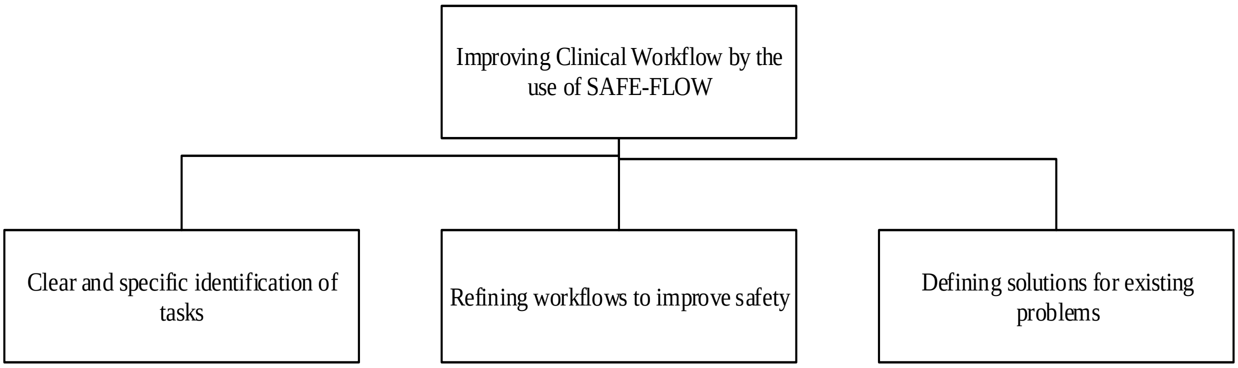

Improving Clinical Workflow by the use of SAFE-FLOW
Clear and specific identification of tasks
Refining workflows to improve safety
Defining solutions for existing problems

Figure 29 Characteristics that contribute to improving clinical workflows

Three of the interviewees (all were clinicians who were not involved in the case study) raised some concerns regarding having different workflows for the same clinical service in different hospitals. This inconsistency may hinder using the reusability characteristic, which is claimed by SAFE-FLOW. However, this was clarified to them, as SAFE-FLOW suggests that each hospital should aim at accomplishing the analysis process for its own workflows. Hospitals should not rely on the analysis results of other hospitals although they can benefit from such analysis if it is available to them. Besides, it was explained to the participants that the resulting workflow models are reusable and maintainable; that is if a certain workflow has been modelled for a certain department, then the analyst can use it as a subcomponent in another workflow and it can be easily maintained as well if there is a need to do this.

Moreover, one of the concerns raised by one clinician was that experienced healthcare experts often have their unique way of delivering a certain clinical service. Sometimes, the processes and tasks can be different from any other established workflows and it is difficult for them to follow these workflows. This means that those experts may close their eyes to these workflows, which means putting them on the shelf without being used.

One other important concern that was raised by the same clinician is that successful application requires close collaboration between the safety analyst and the healthcare team. If this is not achieved then the application of SAFE-FLOW may produce incorrect results that may put patient life at risk.

The following table summarises the results and the patterns and categories produced regarding the challenges and concerns of the healthcare staff about the application of SAFE-FLOW in practice.

Table 14 Participants' concerns about the application of SAFE-FLOW

Examples of Keywords used by interviewees (opinions)	Patterns	Category
• Different hospitals have different workflows	Reusability of analysed components	Challenges of effective application
• Experienced staff would not look at this • The resulted workflows may not be used	Experience can affect the utility	
• Not cooperative • Extra work • I do not have time for this	Cooperation of staff	

To conclude, using this approach has the potential to reveal patterns of diagnostic and procedural failures that suggest areas for improvement. Systematic analysis of such failures and finding their root causes can identify potential preventive strategies, which can help in promoting the safety culture, and accordingly enhance patient safety.

Overall, the previous analysis and findings have the potential to justify the evaluation conclusions. This goes under justification of the conclusions under synthesis and analysis.

6. Establishing the Validity of the Findings from Qualitative Analysis

In qualitative research, validity tells if the findings of a study are true or not (Guion *et al.*, 2011). In other words, it determines whether the research truly measures that which it was intended to measure (Joppe, 2000). Several methods are in use to give quality, credibility and trustworthiness to a qualitative research including triangulation, saturation, member checking and self-disclosure (reflexivity). Therefore, these methods can be used to establish the validity of qualitative research.

For this part of the study, the aim was to demonstrate validation through triangulation. Three groups of experts were interviewed. The first group represented experts who were involved in the case study, the second group involved experts from healthcare who had not been involved initially, and the third group included an academic expert who had knowledge about the healthcare and the tool used. The choice of expert for the last part was key, since the professionals who involved in the application process were experts on the application; they were not experts in validation. So the third part of the validation (triangulation) was based on a discussion with an academic expert with experience in healthcare; this interview added an extra level of confidence in the SAFE-FLOW application. Note that the approach has also been documented and reviewed through peer review with conference and journal publications (Al-Qora'n *et al.*, 2013; Al-Qora'n *et al.*, 2014a; Al-Qora'n *et al.*, 2014b; Al-Qora'n *et al.*, 2014c).

In summary, the two groups of application area experts who were involved in the evaluation stated its value and that the outputs appeared correct. This was reiterated when reviewed by the expert, who was interviewed to confirm the validity of the results. In conclusion, the use and application of SAFE-FLOW was demonstrated to an acceptable quality level. SAFE-FLOW has the potential to help in avoiding the patient harm through focusing on the design of the work system and processes. Clinical workflows need to be designed in a way that can ensure producing high quality and safe patient care.

This redesign process can be efficient and effective through the specification of those tasks and processes that can lead to harm.

The experts stated that redesigning workflows to improve the information flow and coordination should consider all the important tasks that can lead to serious problems and threaten patients’ life. If the redesign considers this, it can enable the achievement of benefits in quality and safety of care.

Moreover, the interviews with experts identified that implementing the changes in the workflow has the potential to create opportunities to create and improve awareness and learning for those involved in patient care, as well as helping to improve the interactions, because faulty and inconsistent interactions can lead to adverse consequences. Patient safety can be maintained with a better understanding of the healthcare system, which is dependent on understanding of different components of the system and the ongoing interactions between these components.

Replacing certain tasks with more reliable tasks can help in improving the efficiency and effectiveness of the workflow. For example, adopting bar code administration technology can reduce medication errors. It is very important to examine tasks that require changes to provide better and safer care. One of the important factors that has the potential to harm patients is the lack of recognition of the importance of the workflow design in various aspects of the care process. Experts confirmed that the SAFE-FLOW approach can provide an analysis that is better in the identification of faults and their effects than existing practice, such as casual brainstorming or informal assessment by experts. For example, sometimes it is straightforward to identify a particular task or its omission as the immediate cause of an incident. However, the analysis using SAFE-FLOW can explicitly reveal the series of events leading up to adverse outcomes.

Using a structured and a systematic approach as executed in SAFE-FLOW means that the process to consider in any investigation is, to a significant extent, already mapped out and recorded. In other words, using the SAFE-FLOW approach can help to ensure a comprehensive investigation and facilitate the production of formal and safe workflows.

The expected outcome of the evaluation resulted in the best practice guidelines and improvements to the guidance for using SAFE-FLOW.

7. **Sharing the findings and lessons learnt**

The findings and the lessons learnt should be shared for effective evaluation. The evaluation results can be made available for the hospitals who intend to use SAFE-FLOW. The results can be summarised in a simple format that can be easily understood by decision makers.

In addition to the previous steps, the framework suggests a number of standards for effective evaluation. The purpose is to answer the question: **'Will this evaluation be effective?'**.

The standards that can be used to judge the quality of the evaluation are **utility, feasibility, propriety, and accuracy.**

Utility of the evaluation results: The evaluation results are used to provide relevant information about SAFE-FLOW and the results can be prepared in a simple format that can be available to primary users of the evaluation (e.g. decision makers in hospitals) before their decision to use it.

This ability to make the evaluation information ready to serve intended users can be considered as a positive point about the utility of the evaluation.

Feasibility of the evaluation activities: The planned evaluation activities (specifically the interviews) were realistic within the available time, and the expertise available to hand.

Propriety of the evaluation: The evaluation engages those staff members who are most directly affected by SAFE-FLOW and who will participate in its application within hospitals.

Accuracy of the evaluation: the evaluation results need to produce reliable information, which can meet the needs of the hospitals that intend to use SAFE-FLOW. Fairly, the results revealed by the evaluation have the potential to be reliable.

5.1.3 Comparison with Other Methods for Analysing the Safety of Clinical Workflows

SAFE-FLOW showed that the modelling language used here could be usefully applied to improve the management of information and interactions in healthcare practices. It has the potential to represent the patient care process. The communications among different agents can be shown and managed using these models. Then, the additional value with such models is the availability of computer support for the model generations as well as the capability of automated safety analysis to validate the model design. As the most important feature that is needed to be analysed and validated in the case of clinical workflows is the safety of the workflow, SAFE-FLOW showed the ability to analyse the model. The resultant models are usable and feasible, i.e., while working with the healthcare experts it was found that the used models achieved a high level of usability as they were easily understood by the experts.

Moreover, the identification of the workflow problems and failures and their causes shows the weaknesses of the workflow and provides the foundation for safety enhancement and quality improvement initiatives. SAFE-FLOW is helpful in identifying the motivators and contributors to the potential adverse events, thus eliminating as many root causes as possible, and supports setting up suitable safeguards.

In other words, after the analysis process, the analyst would be able to know what to change, add, or delete in the model depending on the analysis results. Consequently, the analyst can solve workflow problems through updating workflow models, possibly by removing the sources of failures in the model and replacing them with more reliable components or processes.

In comparison with other methods which are already in use for safety analysis (e.g. Bayesian Networks (BNs) which is primarily used for quantitative analysis), the modelling phase in SAFE-FLOW requires less technical knowledge. For example, modelling workflows in BNs to facilitate safety analysis requires specialised technical knowledge and there are no well-defined rules to create BNs of a workflow for safety analysis purposes. As a result, a system can have a number of equivalent BNs and if the causal relationships between different nodes are not well defined then BNs can become unnecessarily complex and non-coherent. Therefore BNs of a workflow may be not be understandable by healthcare experts, thus it may not be possible to involve the healthcare experts in the early design phase though their involvement is highly required. However, BNs are efficient methods to perform quantitative analysis under uncertainty and a coherent and relatively simple BN can be created by translating other representations, e.g. Fault Trees into BNs.

As mentioned earlier, analysts can benefit from the capability of BNs by using them in the stages where the healthcare experts are not involved. In SAFE-FLOW, healthcare experts are no more involved in the safety analysis process after the workflow has modelled. Therefore, when the HiP-HOPs tool generates fault trees then they can be translated into BNs, thus benefiting from the strength of the BNs while involvement of the healthcare experts is also ensured.

In comparison with Petri nets and as explained in detail in section 3.2.5, SAFE-FLOW supports the necessary compositional reasoning and verification for clinical workflows. Although using coloured Petri nets can solve this problem, using them can produce large and complicated nets.

Even though other modelling techniques can be beneficial, for example, finite state machines can be used to model the workflow, it is not easy to analyse the state machines directly to obtain safety related information about the workflow. In this case, a state machine based model will need to be transformed into other models e.g. fault trees, Markov chains, Bayesian Networks. Another issue of a state machine based approach is that they increasingly face a state explosion problem, i.e., for a relatively complex workflow, the number of states required to model the complete failure behaviour of the workflow grows exponentially with the number of components of the workflow; thus they are difficult to create and analyse.

The analyst in cooperation with the healthcare experts does the process of hazards identification. The hazards should be specified for each component and possible failures for each component and their causes are discussed. After that, the process of failure annotation needs to be done by the analyst who should have experience in using HiP-HOPS. In terms of usability, HiP-HOPS has a graphical user interface that is easy to use once the analyst is trained on using it.

In comparison with other model checking (Clarke *et al.*, 1999) or simulation approaches, HiP-HOPS is less automated than these approaches. However, it is generally faster and more scalable and can be used to complement other techniques such as simulation. Recent work on the systematic application of HiPHOPS and model checking (Sharvia and Papadopoulos, 2011) also opens the opportunity to extend the analysis with model checking in future. HiP-HOPS also serves as a useful foundation for related technologies such as optimisation (Adachi *et al.*, 2011). In addition, the model optimisation capability of HiP-HOPS can produce different alternative models to achieve safety requirements and can help to select components and subsystems among different alternatives as well as helps to decide the level and location of replicated components.

Finally, in comparison with the current state of practice, SAFE-FLOW provides many advantages over the manual process that is often used to identify hazards and analyse them. As mentioned previously, the automation has a very positive impact on improving clinical workflows. Moreover, providing such systematic analysis has the potential to provide large benefits through the safety analysis process with relatively little effort.

5.2 Summary and Recommendations

The evaluation, which was accomplished over three levels, demonstrated the applicability and the usability of SAFE-FLOW and its efficacy in enhancing patient safety. SAFE-FLOW contributed in the definition and identification of possible failures as well as in their effective treatment. In particular, SAFE-FLOW has the potential to help both healthcare staff and safety analysts to identify their roles, responsibilities and their needs from the workflow.

Hospitals need to invest in keeping their patients safe and offer a significant portion of their budgets to support such efforts. However, they need to make sure they are getting value for money by using systematic approaches to do so, as well as by engaging all the healthcare workers with these approaches.

SAFE-FLOW is a model- based approach where early models can be constructed and used in the later stages. These models can be used as a communication medium between the analyst and the healthcare team. The simple structure of the analysis results makes it easier to reuse the results.

The following characteristics are beneficial to SAFE-FLOW:

1. SAFE-FLOW benefits from the detailed input model which are at a high level of abstraction.
2. The models are graphical models and can be considered as media for communication.

Decision makers and healthcare organisations should make sure of the following:

1. All the staff involved in the workflow should be considered for training sessions.
2. The delivery of accurate treatment is staff members’ responsibility.
3. The workflow needs to be carefully analysed to ensure that staff can work without having unchecked faults.

4. It is important when planning any changes like adopting new systems or changing the organizational procedures to reflect these changes in the workflow, and apply SAFE-FLOW to the new workflow.

Safety analysts need to make sure of the following:

1. Systematically identify all hazards and deal with important risks.
2. Make sure that the risk left behind is acceptable.
3. Provide effective and genuine solutions.

6 Conclusion and Future Work

This chapter concludes the thesis with a summary of the key findings, contributions of the thesis, and gives some suggestions for future work. It starts with summarising how the outcomes of this thesis achieve the research objectives and answer the research questions posted in Chapter 1.

6.1 Summary of Key Findings

At the beginning of this thesis, the following main research question and-sub questions were asked:

> **How can established dependability analysis techniques be adapted to improve the safety of clinical workflows?**

1. *To what extent can existing safety analysis methods and lessons learnt from industry help in improving the safety of clinical workflows?*
2. *How can workflows be captured in a model, and given that, how can that model be made compatible with model-based safety analysis approaches?*
3. *How can safety analysis be used as part of a robust methodology for designing dependable clinical workflows and improving patient safety?*
4. *How can new workflow analysis methods be evaluated in terms of their impact on the safety of clinical workflows?*

To answer these research questions, several objectives were defined. In the following discussion, those objectives are revisited to summarise how and to what extent they have been achieved.

Objective 1. To examine related safety analysis methods in high-risk industries and investigate their strengths and limitations.

The purpose of this objective is to establish a conceptual and realistic basis for the review of methods that have been used for the analysis of adverse events in healthcare. The thesis investigated the characteristics of the most related safety analysis methods and identified the potential for reusing these methods in healthcare. The review of these methods presented in Chapter 2 provides understanding of the fields of application, advantages, quality of outputs, positive points, negative points and clearness of the steps. This helped to identify some deficiencies in the available methods for analysing safety analysis of clinical workflows as well as the possibility for some of them to be beneficial for this purpose.

There are many ways to categorise these methods. In this thesis, MBSA was found to be effective in understanding and analysing clinical workflows. HiP-HOPS is the tool that was selected to represent MBSA. The tool demonstrated its ability to provide a systematic and integrated safety analysis in a simple and a clear manner. Its strength lies in its ability to allow a degree of automation in the analysis process, guide the redesign process, provide some reuse, and to be extended to enable optimisation and dynamic behaviour. By using this tool, the failure analysis of workflows can be made based on the composition of failure analysis of its components, which makes the analysis easily adaptable. Therefore, SAFE-FLOW was developed based on the use of HiP-HOPS.

The thesis showed that reusing safety analysis methods that have been used in other industries in healthcare is a practical and efficient way to improve workflow safety without having to reinvent the wheel. The discussion that was presented in Chapter 2 showed that safety analysis methods that have been used in other domains can be transferred to healthcare.

Objective 2. To develop appropriate link between traditional components for such dependability approaches and the constituents of a healthcare workflow, in other words, to capture workflows in models that are compatible with model-based safety analysis approaches. This involves investigating how inputs to tools can be constructed, in particular, how to define and model the workflow components.

The intention behind this objective is to capture workflows in models that are compatible with the inputs for safety analysis tools. In other words, the purpose is to define and model the workflow components. Challenges to achieving this include the modelling of the healthcare processes, modelling of the involved agents and the interactions between different agents within the workflow.

Therefore, business process modelling techniques that are used in healthcare were investigated, compared and reviewed. Although many of those techniques can be helpful in representing healthcare processes and in identifying key hazards, they can be poor in analysing such hazards. The purpose here is to represent healthcare processes and analyse them for their safety.

The research attempted to understand the healthcare environment and how different constituents can be modelled and analysed. Then, modelling constructs were defined and explained in detail in Chapter 3 to show how to model different workflow concepts and to model their failures. SAFE-FLOW showed its ability to model most of the workflow concepts and demonstrated that it can be simple enough to build and analyse clinical workflows.

Objective 3. To develop the SAFE-FLOW approach for the systematic safety analysis of clinical workflows.

This thesis has developed SAFE-FLOW, a novel approach for safety analysis of clinical workflows and has considered the critical nature of the clinical components. SAFE-FLOW is based on the use of HiP-HOPS tool. HiP-HOPS tool was chosen as a result of the arguments provided in Chapter 2. In Chapter 3, the development of SAFE-FLOW has been introduced and the detailed steps of SAFE-FLOW have been explained.

The process starts with documenting the workflow, which must be done by a safety analyst and a healthcare team. This is followed by the model construction by the analyst and then validating the model with the healthcare team. To enable the analysis, the analyst and the healthcare team identify hazards and specify their safety levels. The model is then annotated with failures to allow the HiP-HOPS tool to automatically perform fault tree and FMEA synthesis and analysis. The analysis results are used to refine the models through the offered feedback about failure causes and the identification of the weak points. This helps the analyst to revise the workflow design and design new workflow models that eliminate the sources of failures through replacing the components that can cause failures with safer components. Then these models are checked again with the healthcare team and the analysis is repeated until reaching an acceptable failure level or until achieving the best safety results. If probability analysis is required, this can be done after obtaining FTA and FMEA analysis results, as long as some form of useful probabilistic data is available for root causes.

Therefore, the thesis presented an approach for safety analysis of clinical workflows that has the potential to offer official clinical workflows to be used by healthcare workers. This is the novel contribution of this thesis, as in typical healthcare practice, FMEA and FTA are used to analyse several adverse events instead of analysing the workflow models themselves, and workflow modelling usually lacks the safety analysis functionality.

Objective 4. To examine the applicability of SAFE-FLOW to realistic clinical workflows using empirical research.

The applicability of SAFE-FLOW is tested on the workflow of a radiology department and the results showed the feasibility and the applicability of SAFE-FLOW. Data was collected in a radiology department and a healthcare team that consists of five people was formed to help in the application process. The detailed steps that are involved in SAFE-FLOW provide effective methods to enable the communication between the analyst and the healthcare workers. Chapter 4 explained the case study in detail.

Objective 5. To systematically evaluate the benefits and limitations of SAFE-FLOW.

The usability and propriety of the used models were tested and positive results were achieved. Moreover, utility and feasibility of SAFE-FLOW were evaluated. The evaluation design is explained in detail in Chapter 5, and it can be helpful in evaluating the use of any safety analysis method in healthcare. This evaluation design provides another contribution of this thesis.

Answering the Main Research Question

Safety analysis is an area that has long history of development and a wide range of applications. In healthcare, the safety analysis process is often perceived as a complex and a difficult task, which can consume a large amount of time, resources and efforts. However, the results of conducting a systematic evaluation for the application of integrated safety analysis of clinical workflows showed that if it is well organised; healthcare providers can recognise large benefits from the safety analysis process with relatively little effort.

The evaluation process in Chapter 5 gathered evidence that the use of SAFE-FLOW has the potential to provide benefits to the existing care process. Results also showed that such a systematic safety analysis is of extreme importance, as it has the ability to illustrate the expected and the unexpected hazards. Such safety analysis is essential to arrive at how clinical workflows can be improved for existing and future users. It also proved that it can help healthcare experts to better understand how the care processes work. However, putting this into practice remains one of the biggest challenges that may face the application of SAFE-FLOW. As the accepted workflows should not be kept on the shelf, instead they should be used by healthcare experts to guide them to the correct and safe practice.

Primarily, SAFE-FLOW guarantees a better understanding of clinical workflows where healthcare providers are provided with detailed workflows that support the understanding of the tasks, people, systems and interactions involved in the workflow. Furthermore, such modelling and analysis results can be used for refining the workflow where the analyst and healthcare providers work together to redesign and improve the workflow through relieving the sources of potential failures. This would help in minimising the failure probability to acceptable levels or at least help in adding safety mechanisms to mitigate the effects of failures

6.2 Contributions of the Research

The thesis aimed to demonstrate the potential value of computer-based dependability approaches to healthcare. Using such systematic approaches to build and analyse the safety of clinical workflows holds many benefits to healthcare experts, managers, workflow analysts, and other workflow participants.

Thus, this thesis examined the use of workflow modelling and safety analysis technologies to reduce medical errors, improve the safety of clinical workflows, and accordingly improve patient safety. In particular, it proposed the SAFE-FLOW approach through which clinical workflows are documented, modelled, analysed for their safety, and finally redesigned based on the analysis results. The analysis is repeated until safe workflows are reached. Then the thesis provided a systematic evaluation of SAFE-FLOW.

Thus, the contributions of this thesis may be summarised as follows:

1. It addressed the issue of the apparent lack of techniques available for analysing the safety of clinical workflows by establishing a systematic approach that offers more powerful analysis capabilities. This can help in performing a comprehensive safety analysis for the workflows as well as in designing well-structured workflow processes and activities.

2. It examined the applicability and benefits of SAFE-FLOW for analysing workflows through a realistic case study. The results of the application showed that the approach is generic and can be used to analyse the impact of software, hardware, and human errors on these workflows, which has the potential to improve the safety of clinical workflows and consequently contribute to improving patient safety.

3. The identification of root causes for failures within clinical workflows allows greater understanding of the factors that contribute to adverse events that can potentially lead to a

serious clinical risk. Moreover, it enabled the identification of weak points in the clinical workflow, which can then be effectively addressed and improved. It can be used to create comprehensive hazards analysis associated with the analysed workflow.

4. It evaluated SAFE-FLOW through a systematic and a realistic evaluation plan. First, a usability testing was performed. Then a framework for the evaluation of a health program was applied to evaluate SAFE-FLOW, and finally SAFE-FLOW was compared to other methods that can be used for the same purpose. The evaluation design presented in the thesis provides a systematic and generic methodology that can be used to evaluate further approaches for safety analysis in healthcare.

5. Overall, the thesis provides academics, specialists and decision makers with SAFE-FLOW, a systematic approach for safety analysis of clinical workflows. It also offers empirical data and a systematic evaluation for the application of SAFE-FLOW, and makes the evaluation results available for those who may consider using SAFE-FLOW.

The findings of the evaluation provided valuable insights into the usability and feasibility of using SAFE-FLOW. SAFE-FLOW drew the map for the root causes of workflow failures and helped to redesign workflows to achieve safety requirements. This is the major contribution of this work, as to date there is a lack of automated tools which allow the modelling and analysis of real-world workflows. SAFE-FLOW provides an effective means to accomplish this goal; it is able to provide a valid theoretical framework consisting of modelling processes and sub- processes and their interactions. The study findings contribute towards a larger research effort being proposed for reducing medical errors and enhancing patient safety.

Furthermore, as SAFE-FLOW supports a large part of the workflow development process (in particular the design phase) the clinical service quality (which is the output of the clinical workflow) is improved and maintained through specifying the exact safe steps or paths which can lead to the service. Therefore, if developing a workflow management system is required, then SAFE-FLOW improves the quality of the design phase, this leads to a better quality in the following software engineering stages.

It is generally believed that a high-quality design can produce a high-quality product. In practice, it can be assumed that if a high-quality approach is maintained for analysing the safety of clinical workflows, its output has the potential to help in preparing high-quality and safe workflows that can contribute to enhancing patient safety. It is hoped that SAFE-FLOW and the recommendations on healthcare safety analysis in this thesis go some way into filling this gap in safety analysis within the healthcare context.

To conclude, the major contribution of this thesis is that it provides valuable insights into how to model and analyse the safety of clinical workflows. It offers a clearly defined approach for use in the safety analysis of clinical workflows. The approach has been successfully applied in several published studies, evaluated for its ability to improve clinical workflows, and made available for use by healthcare organisations.

6.3 Limitations of the Research

- Safety engineering in healthcare faces different challenges; it needs to contribute significantly in the analysis of safety critical workflows. The thesis established SAFE-FLOW as an integrated approach for safety analysis of clinical workflows; the approach has been applied to a case study, and it is hoped that this can be developed further, where a special interface for healthcare can be automated as a part of HiP-HOPS.
- Testing the abilities of SAFE-FLOW on only one location can be insufficient. Having access to more locations has the potential to open a broader range of unpredictability, where having access to a larger population can introduce the possibility of various workflow architectures and accordingly better analysis results.

- The consideration and understanding of the healthcare environment was critical. However, some other challenges related to accessibility were found to be even more challenging. For performing the case study at the hospital, authorisations had to be obtained first. Moreover, due to the limited time of healthcare experts, their involvement in the safety analysis process and the interviews were organised out of their working hours (mainly at weekends). Such research needs support and a helping hand from the staff of the healthcare institution.
- Once SAFE-FLOW is in use in the hospital, there must be enough support without imposing undue strains on available resources. A qualified analyst and cooperative staff would help to accomplish the analysis process. SAFE-FLOW has the potential to be sustainable, as it does not depend on the people themselves. However, if changes in existing staff bring new staff who are not cooperative this may lead to an incomplete analysis process. This problem can be solved by a solid code of practice that forces the new staff to get involved in the safety analysis process.
- Clinicians are typically untrained in information systems; due to their workload, they often resist the extra effort required to code data and conform to newly compulsory workflows. Thus, deployments typically have unintended consequences related to user experience. Different hospitals may have different workflows, which makes the process of individual analysis somewhat difficult. Using semi-automated software tools may help to increase uptake compared to manual (paper-based) or non-automated analysis.

6.4 Future Work

The aim of demonstrating the value and benefits of computer science based dependability approaches to clinical workflows has been achieved to a certain extent. SAFE-FLOW provides the foundation for potential future work, outlined below.

6.4.1 Improving Workflow Modelling

In addition to the guidelines provided in Chapter 3, developing a special workflow-based interface for healthcare (in line with the comments from evaluation) can be beneficial to help analysts to directly model clinical workflows. Graphical representation of healthcare components can support the modelling with clear concepts about the modelling of clinical components.

6.4.2 Comprehensive Safety Analysis (Incorporating more Scenarios)

While the thesis showed how to use SAFE-FLOW to analyse two RIS/PACS workflow failure scenarios, this identified the need for further investigation with a comprehensive analysis for all scenarios. Moreover, since clinical workflows can diverge, further consideration of dissimilar cases has the potential to escalate the application of SAFE-FLOW, e.g., radiotherapy workflows usually have highly complex and multi-step processes that make them susceptible to adverse events.

6.4.3 Incorporating Administrative Processes

The case study included in the thesis focuses on the care processes. Incorporating other processes like the administrative processes can help in developing a more comprehensive analysis.

6.4.4 Application of Probability Analysis

In addition, the application of probability analysis in future studies may aid in giving a complete analysis and at this point human factors uncertainty (uncertainty in probabilistic analysis due to human factors) needs to be taken into consideration.

6.4.5 Considering the Order of Events

The development of analytical approaches that consider the order in which events occur, in addition to whether they occur or not, could be another research area to be considered for future research. This will help to capture failures caused by inappropriate sequences of activities that are otherwise correct when performed in a different order.

6.4.6 Usability of SAFE-FLOW

Usability can be improved, for example, through developing a special healthcare interface to HiP-HOPS. Moreover, developing a glossary for more general clinical workflow concepts will probably be useful.

References

ABUJUDEH, H. H. & KAEWLAI, R. 2009. Radiology Failure Mode and Effect Analysis: What Is It? 1. *Radiology,* 252**,** 544-550.

ACCIRAD 2013. Patient Safety in External Beam Radiotherapy- Guidelines on Risk Assessment and Analysis of Adverse Events and near Misses.

ADACHI, M., PAPADOPOULOS, Y., SHARVIA, S., PARKER, D. & TOHDO, T. 2011. An approach to optimization of fault tolerant architectures using HiP-HOPS. *Software: Practice and Experience,* 41**,** 1303-1327.

AGUILAR-SAVEN, R. S. 2004. Business process modelling: Review and framework. *International Journal of Production Economics,* 90**,** 129-149.

Al-Qora'n, L., Sharvia, S., Gordon, N. & Papadopoulos, Y. 2013. Safety Analysis of a Remote Patient Monitoring System with a Guideline Based Decision Support. In*: proceedings of Med-e-Tel,* April 10-12 2013 2013 Luxembourg. 322-327.

Al-Qora'n, L., Sharvia, S., Gordon, N. & Walker, M. 2014. Safety analysis of clinical workflows: The case of the workflow within a radiology department, *Science and Information Conference (SAI), 2014* (pp. 72-78). IEEE.

Al-Qora'n, L., Gordon, N., Sharvia, S., Walker, M. & Papadopoulos, Y. 2014. An Approach to Safety Analysis of Clinical Workflows, Athens: ATINER'S Conference Paper Series, No: COM2014-1157. (The same paper is published in *Athens Journal of Health* September 2014, pages 201-216).

Al-Qora'n, L., Gordon, N., Walker, M., Sharvia, S., & Kabir, S. 2014. A Safety Analysis Approach to Clinical Workflows: Application and Evaluation, *International Journal of Advanced Computer Science and Applications* (IJACSA), Special Issue on Extended Papers from Science and Information Conference 2014, 2014, 4(3).

AMMENWERTH, E. & DE KEIZER, N. 2003. An inventory of evaluation studies of information technology in health care: trends in evaluation research 1982-2002. *Studies in Health Technology and Informatics,* 107**,** 1289-1294.

ANTOCH, G., FREUDENBERG, L. S., BEYER, T., BOCKISCH, A. & DEBATIN, J. F. 2004. To enhance or not to enhance? 18F-FDG and CT contrast agents in dual-modality 18F-FDG PET/CT. *Journal of Nuclear Medicine,* 45**,** 56S-65S.

Arnold, A., Point, G., Griffault, A., & Rauzy, A. 1999. The AltaRica formalism for describing concurrent systems. *Fundam. Inform., 40*(2-3), 109-124.

AVIZIENIS, A., LAPRIE, J.-C. & RANDELL, B. 2001. *Fundamental concepts of dependability,* University of Newcastle upon Tyne, Computing Science.

AZEVEDO, L. S., PARKER, D., WALKER, M., PAPADOPOULOS, Y. & ARAUJO, R. E. 2013. Automatic Decomposition of Safety Integrity Levels: Optimization by Tabu Search. *In:* SAFECOMP 2013-Workshop CARS (2nd Workshop on Critical Automotive applications: Robustness & Safety) of the 32nd International Conference on Computer Safety, Reliability and Security, 2013. NA.

BANACH, R. & BOZZANO, M. 2013. The mechanical generation of fault trees for reactive systems via retrenchment I: combinational circuits. *Formal Aspects of Computing***,** 25(4), 573-607.

BASTOS, R. M. & RUIZ, D. D. A. 2002. Extending UML activity diagram for workflow modeling in production systems. 2002. Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS), 2002. IEEE, 3786-3795.

BATES, D. W. 2002. The quality case for information technology in healthcare. *BMC Medical Informatics and Decision Making,* 2**,** 7.

BATTLES, J. & LILFORD, R. 2003. Organizing patient safety research to identify risks and hazards. *Quality and Safety in Health Care,* 12**,** ii2-ii7.

BEDFORD, T. & COOKE, R. 2001. *Probabilistic risk analysis: foundations and methods*, Cambridge University Press.

BELHAJJAME, K., VARGAS-SOLAR, G. & COLLET, C. Year. A flexible workflow model for process-oriented applications. *In:* Web Information Systems Engineering, 2001. Proceedings of the Second International Conference on, 2001. IEEE, 72-80.

BENYOUCEF, M., KUZIEMSKY, C., AFRASIABI RAD, A. & ELSABBAHI, A. 2011. Modeling healthcare processes as service orchestrations and choreographies. *Business Process Management Journal,* 17**,** 568-597.

BERTOLINI, C., SCHÄF, M. & STOLZ, V. 2012. Towards a formal integrated model of collaborative healthcare workflows. *Foundations of Health Informatics Engineering and Systems.* Springer Berlin Heidelberg, 2012. 57-74.

BIEBER, P., DELMAS, R. & SEGUIN, C. 2011. DALculus–theory and tool for development assurance level allocation. *Computer Safety, Reliability, and Security.* Springer.

BOBBIO, A., PORTINALE, L., MINICHINO, M. & CIANCAMERLA, E. 2001 b. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering & System Safety,* 71**,** 249-260.

BOOCHEVER, S. S. 2004. HIS/RIS/PACS integration: getting to the gold standard. *Radiol Manage,* 26**,** 16-24.

BOUCHET, M.-L. 2007. Design and Usability of Digital Libraries: Case Studies in the Asia Pacific. *Library Hi Tech,* 25**,** 437-438.

BURGMEIER, J. 2002. Failure mode and effect analysis: an application in reducing risk in blood transfusion. *Joint Commission Journal on Quality and Patient Safety,* 28**,** 331-339.

CAI, Y. 2012. Comparative Analysis of the Workflow Modeling. *In:* International Conference on Management of e-Commerce and e-Government (ICMeCG), 2012, 2012. IEEE, 226-229.

CASTIGLIA, F. & GIARDINA, M. 2011. Fuzzy Risk Analysis of a Modern γ-Ray Industrial Irradiator. *Health Physics,* 100(6), 622-631.

CHIASSON, M. W. & DAVIDSON, E. 2004. Pushing the contextual envelope: developing and diffusing IS theory for health information systems research. *Information and Organization,* 14**,** 155-188.

Clarke E. M., 2008, The Birth of Model Checking, 25 Years of Model Checking, pp 1-26, Springer-Verlag Berlin, Heidelberg, Germany, [Online] https://www7.in.tum.de/um/25/pdf/Clarke.pdf, [Last access on] 14/8/2014.

CLARKE, E. M., GRUMBERG, O. & PELED, D. 1999. *Model checking,* MIT press.

CLOHISY, J. C., CARLISLE, J. C., TROUSDALE, R., BEAULE, P. E., MORGAN, P., STEGER-MAY, K., SCHOENECKER, P. L. & MILLIS, M. 2009. Radiographic evaluation of the hip has limited reliability. *Clinical Orthopaedics and Related Research,* 467**,** 666-675.

CORAS 2000. CORAS: A Platform for Risk Analysis of Security Critical Systems. Online: http://www.ewics.org/attachments/security-subgroup-boppard-2002/CORAS+framework.pdf [Accessed 10/9/2014].

COUTINHO, J. S. 1964. Division of Engineering: Failure- Effect Analysis. *Transactions of the New York Academy of Sciences,* 26**,** 564-584.

CRANE, M. 2012. 12 Worst Medical Technology Dangers. Online:

http://www.medscape.com/features/slideshow/tech-dangers [Accessed 09/11/2013].

DABNEY, J. B. & HARMAN, T. L. 2001. *Mastering Simulink 4,* Prentice Hall PTR.

DOBSON, J., SOMMERVILLE, I. & DEWSBURY, G. 2007. Introduction: Dependability and Responsibility in Context. *Responsibility and Dependable Systems.* Springer.

DONNELLY, L. F., DICKERSON, J. M., GOODFRIEND, M. A. & MUETHING, S. E. 2009. Improving Patient Safety: Effects of a Safety Program on Performance and Culture in a Department of Radiology. *American Journal of Roentgenology,* 193**,** 165-171.

DUMAS, J. S. & REDISH, J. 1999. *A practical guide to usability testing*, Intellect Books.

EKAETTE, E., LEE, R. C., COOKE, D. L., IFTODY, S. & CRAIGHEAD, P. 2007. Probabilistic Fault Tree analysis of a Radiation Treatment system. *Risk Analysis,* 27**,** 1395-1410.

EMSLIE, S., KNOX, K. & PICKSTONE, M. 2002. Improving Patient Safety: Insights from American, Australian & British Healthcare: *Based on the Proceedings of a Joint ECRI and Department of Health Conference to Introduce the National Patient Safety Agency*. ECRI, 2002.

ERICSON, C. A. 2005. *Hazard analysis techniques for system safety*, Wiley. com.

ESHUIS, R. & DEHNERT, J. 2003. Reactive petri nets for workflow modeling. *Applications and Theory of Petri Nets 2003.* Springer Berlin Heidelberg, 2003. 296-315.

FISCHER, L. 2001. Workflow handbook 2001. Lighthouse Point: Future Strategies.

FITZGERALD, R. 2001. Error in Radiology. *Clinical Radiology,* 56**,** 938-946.

GEHLOT, V. & HAYRAPETYAN, A. 2001. Systems modeling and analysis using colored Petri Nets: a tutorial introduction and practical applications. Proceedings of the 45th annual southeast regional conference, 2007. ACM, 514-514.

GILCHRIST, W. 1993. Modelling failure modes and effects analysis. *International Journal of Quality & Reliability Management,* 10(5).

GRAN, B. A., FREDRIKSEN, R. & THUNEM, A. P.-J. 2007. Addressing dependability by applying an approach for model-based risk assessment. *Reliability Engineering & System Safety,* 92**,** 1492-1502.

GREEN, M. 2013. Error and Injury in Computers and Medical Devices. Available: http://www.visualexpert.com/Resources/compneg.html [Accessed 4/5/2013].

Guion, L., Diehl, D., McDonald, D. 2011. Triangulation: Establishing the Validity of Qualitative Studies, Institute of Food and Agricultural Sciences, University of Florida

GUITE, K. M., HINSHAW, J. L., RANALLO, F. N., LINDSTROM, M. J. & LEE, F. T. 2011. Ionizing radiation in abdominal CT: unindicated multiphase scans are an important source of medically unnecessary exposure. *Journal of the American College of Radiology,* 8**,** 756-761.

HANNAN, T. J. 1999. Detecting adverse drug reactions to improve patient outcomes. *International Journal of Medical Informatics,* 55**,** 61-64.

HEIMDAHL, M. P. 2007. Safety and software intensive systems: Challenges old and new. *In:* 2007 *Future of Software Engineering*, 2007. IEEE Computer Society, 137-152.

Holt, A., et al. 19983. Coordination systems technology as a programming environment. Electrical Communication, 57 (4) (1983), pp. 307prog

HUANG, H.-Z., TONG, X. & ZUO, M. J. 2004. Posbist fault tree analysis of coherent systems. *Reliability Engineering & System Safety,* 84**,** 141-148.

HUGHES, R. G. & MITCHELL, P. H. 2008. Defining Patient Safety and Quality Care.

IDEF. 2003. Family of Methods web page. Available: http://www.idef.com [Accessed 27/12/2014].

INVERARDI, P., MUCCINI, H. & PELLICCIONE, P. 2005. Dually: Putting in synergy UML 2.0 and ADLs. *In:* 5th Working Conference on Software Architecture, 2005. IEEE, 251-252.

Johnson, Robert W. 2010. Beyond-compliance uses of HAZOP/LOPA studies. Journal of Loss Prevention in the Process Industries 23.6 (2010): 727-733.

Joppe, M. 2000. The Research Process.

JOSHI, A., WHALEN, M. & HEIMDAH1, M. P. E. 2006. Model-Based Safety Analysis Final Report. *NASA contractor report, NASA/CR- 2006-213953.*

JUN, G. C. T., WARD, J. & CLARKSON, P. 2005. Mapping the healthcare process in order to design for patient safety. *In:* ICED 05: 15th International Conference on Engineering Design: Engineering Design and the Global Economy, 2005. Engineers Australia, 2189.

JUN, G. T., WARD, J., MORRIS, Z. & CLARKSON, J. 2009. Health care process modelling: which method when? *International Journal for Quality in Health Care***,** mzp016.

KALLIO, T. & KAIKKONEN, A. 2005. Usability testing of mobile applications: A comparison between laboratory and field testing. *Journal of Usability Studies,* 1**,** 23-28.

KAPLAN, B. 1987. The medical computing "lag": Perceptions of barriers to the application of computers to medicine. *International Journal of Technology Assessment in Health Care,* 3**,** 123-136.

KAPLAN, B. & HARRIS-SALAMONE, K. D. 2009. Health IT success and failure: recommendations from literature and an AMIA workshop. *Journal of the American Medical Informatics Association,* 16**,** 291-299.

KHAKZAD, N., KHAN, F. & AMYOTTE, P. 2011. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering & System Safety,* 96**,** 925-932.

KNEZEVIC, J. & ODOOM, E. R. 2001. Reliability modelling of repairable systems using Petri nets and fuzzy Lambda–Tau methodology. *Reliability Engineering & System Safety,* 73**,** 1-17.

KNIGHT, J. C. 2002. Safety critical systems: challenges and directions. *In:* Proceedings of the 24rd International Conference on Software Engineering, 2002. IEEE, 547-550.

KOHN, L. T., CORRIGAN, J. M. & DONALDSON, M. S. 2000. *To err is human: building a safer health system,* National Academies Press.

KRUSKAL, J. B., SIEWERT, B., ANDERSON, S. W., EISENBERG, R. L. & SOSNA, J. 2008. Managing an Acute Adverse Event in a Radiology Department1. *RadioGraphics,* 28**,** 1237-1250.

KWAN, M. M. & BALASUBRAMANIAN, P. 1998. Adding workflow analysis techniques to the IS development toolkit. *In:* Proceedings of the Thirty-First Hawaii International Conference on System Sciences, 1998. IEEE, 312-321.

LAHOZ, C., ROMANI, M. & YANO, E. 2012. Dependability Attributes for Space Computer Systems: Quality Factors Approach.

LAKIN, R., CAPON, N. & BOTTEN, N. 1996. BPR enabling software for the financial services industry. *Management services,* 40**,** 18-20.

LAM, W. K. 2005. *Hardware Design Verification: Simulation and Formal Method-Based Approaches (Prentice Hall Modern Semiconductor Design Series),* Prentice Hall PTR.

LANGSETH, H. & PORTINALE, L. 2007. Bayesian networks in reliability. *Reliability Engineering & System Safety,* 92**,** 92-108.

LEAPE, L. L., LAWTHERS, A. G., BRENNAN, T. A. & JOHNSON, W. G. 1993. Preventing medical injury. *QRB. Quality Review Bulletin,* 19**,** 144-149.

LENZ, R. & REICHERT, M. 2007. IT support for healthcare processes–premises, challenges, perspectives. *Data & Knowledge Engineering,* 61**,** 39-58.

LEVESON, N., DULAC, N., MARAIS, K. & CARROLL, J. 2009. Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems. *Organization Studies,* 30**,** 227-249.

LEVESON, N. G. & STOLZY, J. L. 1987. Safety analysis using Petri nets. *IEEE Transactions on Software Engineering,* 386-397.

LIU, D., WANG, J., CHAN, S. C. F., SUN, J. & ZHANG, L. 2002. Modeling workflow processes with colored Petri nets. *Computers in Industry,* 49**,** 267-281.

LIU, T. & CHIOU, S. 1997. The application of Petri nets to failure analysis. *Reliability Engineering & System Safety,* 57**,** 129-142.

LUTZ, R. R. 2000. Software engineering for safety: a roadmap. *In:* Proceedings of the Conference on The Future of Software Engineering, 2000. ACM, 213-226.

MAGLOGIANNIS, I., ZAFIROPOULOS, E., PLATIS, A. & LAMBRINOUDAKIS, C. 2006. Risk analysis of a patient monitoring system using Bayesian Network modeling. *Journal of Biomedical Informatics,* 39**,** 637-647.

MAHADEVAN, S., ZHANG, R. & SMITH, N. 2001. Bayesian networks for system reliability reassessment. *Structural Safety,* 23**,** 231-251.

MARX, D. & SLONIM, A. 2003. Assessing patient safety risk before the injury occurs: an introduction to sociotechnical probabilistic risk modelling in health care. *Quality and Safety in Health Care,* 12**,** ii33-ii38.

MAYER, R. J., MENZEL, C. P., PAINTER, M. K., DEWITTE, P. S., BLINN, T. & PERAKATH, B. 1995. Information integration for concurrent engineering (IICE) IDEF3 process description capture method report. DTIC Document.

MILLER, A. & HEGI-JOHNSON, F. 2012. Software Agents in Clinical Workflow, Clinical Guidelines and Clinical Trial Medicine. *In:* DESAI, N., LIU, A. & WINIKOFF, M. (eds.) *Principles and Practice of Multi-Agent Systems.* Springer Berlin Heidelberg, 2012. 561-574.

MOHKTAR, M. S., BASILAKIS, J., REDMOND, S. J. & LOVELL, N. H. 2010. A guideline-based decision support system for generating referral recommendations from routinely recorded home telehealth measurement data. *In:* Annual International Conference of Engineering in Medicine and Biology Society (EMBC). IEEE, 6166-6169.

MORCOS, S. 2014. Acute serious and fatal reactions to contrast media: our current understanding.

MORCOS, S. & THOMSEN, H. 2001. Adverse reactions to iodinated contrast media. *European radiology,* 11**,** 1267-1275.

Morse, Janice M. et al. "Verification Strategies for Establishing Reliability and Validity in Qualitative Research." International Journal of Qualitative Methods 1.2 (2008): 13-22.

MURFF, H. J., PATEL, V. L., HRIPCSAK, G. & BATES, D. W. 2003. Detecting adverse events for patient safety research: a review of current methodologies. *Journal of Biomedical Informatics,* 36**,** 131-143.

MUTIC, S., BRAME, R. S., ODDIRAJU, S. & MICHALSKI, J. M. 2010. System mapping of complex healthcare processes using IDEF0: a radiotherapy example. *International Journal of Collaborative Enterprise,* 1**,** 316-331.

(NHS)National Patient Safety Agency 2007. Health Risk Assessment Made Easy. Available: http://www.nrls.npsa.nhs.uk/resources/?EntryId45=59825.

NIELSEN, J. 1994. *Usability engineering,* Elsevier.ONG, M.-S. & COIERA, E. 2010. Safety through redundancy: a case study of in-hospital patient transfers. *Quality and Safety in Health Care,* 19**,** 1-7.

OUVRY, A. 2002. Workflow analysis and modeling in medical IT projects. *Medicamundi,* 46**,** 47-55.

PAPADOPOULOS, Y. 2013. Safety and Reliability of Computer Systems and Software. University of Hull.

PAPADOPOULOS, Y. & MCDERMID, J. A. 1999. Hierarchically performed hazard origin and propagation studies. *Computer safety, reliability and security.* Springer Berlin Heidelberg, 1999. 139-152..

PAPADOPOULOS, Y., TRAN, A., FAURE, J. M. & GRANTE, C. 2006. Component Failure Behaviour: Patterns and Reuse in Automated System Safety Analysis. SAE Technical Paper.

PAPADOPOULOS, Y., WALKER, M., PARKER, D., RÜDE, E., HAMANN, R., UHLIG, A., GRÄTZ, U. & LIEN, R. 2011. Engineering failure analysis and design optimisation with HiP-HOPS. *Engineering Failure Analysis,* 18**,** 590-608.

PAPADOPOULOS, Y., WALKER, M., REISER, M.-O., WEBER, M., CHEN, D., TÖRNGREN, M., SERVAT, D., ABELE, A., STAPPERT, F. & LONN, H. 2010. Automatic allocation of safety integrity levels. *In:* Proceedings of the 1st workshop on critical automotive applications: robustness & safety, 2010. ACM, 7-10.

PARÉ, G., AUBRY, D., LEPANTO, L. & SICOTTE, C. 2005. Evaluating PACS success: a multidimensional model. *In:* Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005. IEEE, 147c-147c.

Parker, D. J. 2010. *Multi-objective optimisation of safety-critical hierarchical systems* (Doctoral dissertation, The University of Hull).

PARKER, D., WALKER, M., AZEVEDO, L. S., PAPADOPOULOS, Y. & ARAÚJO, R. E. 2013. Automatic decomposition and allocation of safety integrity levels using a penalty-based genetic algorithm. *Recent Trends in Applied Artificial Intelligence.* Springer.

PATEL, N. V. 2000. Healthcare modelling through role activity diagrams for process-based information systems development. *Requirements Engineering,* 5**,** 83-92.

PATKAR, V., SOUTH, M. & THOMSON, R. 2008. From guidelines to careflows: modelling and supporting complex clinical processes. *Computer-based medical guidelines and protocols: a primer and current trends,* 139**,** 44.

PATTON, M. Q. 1990. *Qualitative evaluation and research methods,* SAGE Publications, inc.

PETRI, C. A. 1962. Kommunikation mit automaten.

PETTIT, R. & GOMAA, H. 2000. Validation of dynamic behavior in UML using colored Petri nets.

Advanced Computation Laboratory, Cancer Research UK. 2000. PROforma. Available:http://www.openclinical.org/gmm_proforma.html [Accessed 19/10/2015].

RAHEJA, D. & ESCANO, M. C. 2009. Fault Tree Analysis - System Safety in Healthcare. *Journal of System Safety***,** 13-15.

REASON, J. 1990. *Human error*, Cambridge university press.

REID, P. P., COMPTON, W. D., GROSSMAN, J. H. & FANJIANG, G. 2005. *Building a better delivery system: a new engineering/health care partnership*, National Academies Press.

ROSENBAUM, S. 1989. Usability evaluations versus usability testing: When and why? *Professional Communication, IEEE Transactions on,* 32**,** 210-216.

ROSSI, D. & TURRINI, E. 2006. What your next workflow language should look like. *In:* 2nd International Workshop on Coordination and Organization, 2006. Citeseer.

Royal College of Radiologists. 2008. Radiology Information Systems. Available: http://www.rcr.ac.uk/docs/radiology/pdf/IT_guidance_RISApr08.pdf

RUFFOLO, M., MANNA, M., COZZA, V. & URSINO, R. 2007. Semantic clinical process management. *In:* Twentieth IEEE International Symposium on Computer-Based Medical Systems, 2007. CBMS'07, 2007. IEEE, 518-523.

SCHEDLBAUER, M. 2007. Workflow Modelling with UML Activity Diagrams. Online: http://www.batimes.com/articles/workflow-modeling-with-uml-activity-diagrams.html [Accessed 02/06/2014].

SCHRENKER, R. A. 2006. Software engineering for future healthcare and clinical systems. *Computer,* 39**,** 26-32.

SHARVIA, S. 2011. *Integrated Application of Compositional and Behavioural Safety Analysis.* PhD Thesis, University of Hull.

SHARVIA, S. & PAPADOPOULOS, Y. 2011. an Approach towards Integrated Safety Assessment *In:*IEEE 7th International Conference on Automation Science and Engineering 2011 Trieste. Trieste: IEEE Explore.

SHISHKO, R., & ASTER, R. (1995). NASA Systems Engineering Handbook. *NASA Special Publication*, *6105*.

SHUKLA, N., KEAST, J. E. & CEGLAREK, D. 2014. Improved workflow modelling using role activity diagram-based modelling with application to a radiology service case study. *Computer Methods and Programs in Biomedicine*.

Smart Cities Project. 2011. Improving Business Processes and Delivering Better E-Services.

SPATH, P. L. 2003. Using failure mode and effects analysis to improve patient safety. *AORN Journal,* 78**,** 15-37.

STARFIELD, B. 2000. Medical Errors - A Leading Cause of Death. *Journal of Medical Association (JAMA),* 284.

STATHIAKIS, N., CHRONAKI, C., SKIPENES, E., HENRIKSEN, E., CHARALAMBUS, E., SYKIANAKIS, A., VROUCHOS, G., ANTONAKIS, N., TSIKNAKIS, M. & ORPHANOUDAKIS, S. 2003. Risk assessment of a cardiology eHealth service in HYGEIAnet. *In:* Computers in Cardiology, 2003, 2003. IEEE, 201-204.

TAITZ, J., GENN, K., BROOKS, V., ROSS, D., RYAN, K., SHUMACK, B., BURRELL, T. & KENNEDY, P. 2010. System-wide learning from root cause analysis: a report from the New South Wales Root Cause Analysis Review Committee. *Quality and Safety in Health Care* (2010): qshc-2008..

THOMAS, D. R. 2006. A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation,* 27**,** 237-246.

THOMAS, E. J. & PETERSEN, L. A. 2003. Measuring errors and adverse events in health care. *Journal of General Internal Medicine,* 18**,** 61-67.

THORNTON, E., BROOK, O., MENDIRATTA, M., HALLETT, D. & KRUSKAL, J. 2011. Application of Failure Mode and Effect Analysis in a Radiology Department. *RadioGraphics,* 31**,** 281-293.

U.S. Department of Health and Human ServicesSERVICES. 1999. Framework for Program Evaluation in Public Health. *Morbidity and Mortality Weekly Report.*September. Vol. 48. No. RR-11.

VAN DER AALST, W. M. 1993. *Interval timed coloured Petri nets and their analysis*, Springer Berlin Heidelberg, 1993.

VAN DER AALST, W. M. 1998. The application of Petri nets to workflow management. *Journal of Circuits, Systems, and Computers,* 8**,** 21-66.

VESELY, W. E., GOLDBERG, F. F., ROBERTS, N. H. & HAASL, D. F. 1981. Fault tree handbook. DTIC Document.

WALKER, M. 2009. *Pandora: A Logic for The Qualitative Analysis of Temporal Fault Trees.* PhD Thesis, University of Hull.

WARD, J., LYONS, M., BARCLAY, S., ANDERSON, J., BUCKLE, P. & CLARKSON, P. 2007. Using fault tree analysis (FTA) in healthcare: a case study of repeat prescribing in primary care. *Patient Safety Research: Shaping the European Agenda*.

WARD, P. T. 1986. *Structured Development for Real-Time Systems: Vol. I: Introduction and Tools,* Pearson Education.

WATERMAN, A. D., GARBUTT, J., HAZEL, E., DUNAGAN, W. C., LEVINSON, W., FRASER, V. J. & GALLAGHER, T. H. 2007. The emotional impact of medical errors on practicing physicians in the United States and Canada. *Joint Commission Journal on Quality and Patient Safety,* 33**,** 467-476.

WATSON, H. 1961. Bell Telephone Laboratories. Launch control safety study. Bell Telephone Laboratories, *Murray Hill, NJ USA*.

WEBER, P., MEDINA-OLIVA, G., SIMON, C. & IUNG, B. 2012. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence,* 25**,** 671-682.

WEINSTEIN, R. A., LINKIN, D. R., SAUSMAN, C., SANTOS, L., LYONS, C., FOX, C., AUMILLER, L., ESTERHAI, J., PITTMAN, B. & LAUTENBACH, E. 2005. Applicability of healthcare failure mode and effects analysis to healthcare epidemiology: evaluation of the sterilization and use of surgical instruments. *Clinical Infectious Diseases,* 41**,** 1014-1019.

WOLOSHYNOWYCH, M., ROGERS, S., TAYLOR-ADAMS, S. & VINCENT, C. 2005. The investigation and analysis of critical incidents and adverse events in healthcare. (2005): 19.

Workflow Management Coalition. 1996. Wrokflow Management Coalition Terminology and Glossary. Brussels.

WREATHALL, J. & NEMETH, C. 2004. Assessing risk: the role of probabilistic risk assessment (PRA) in patient safety improvement. *Quality and Safety in Health Care,* 13**,** 206-212.

YUSOF, M. M., KULJIS, J., PAPAZAFEIROPOULOU, A. & STERGIOULAS, L. K. 2008. An evaluation framework for Health Information Systems: human, organization and technology-fit factors (HOT-fit). *International Journal of Medical Informatics,* 77**,** 386-398.

Appendix 1: List of Abbreviations

The following table describes the various abbreviations and acronyms used throughout the thesis; the page on which each one is defined and first used is also given.

Abbreviation	Meaning	Page
BN	**Bayesian Networks**	**36**
CDC	**Center for Disease Control and Prevention**	**54**
COPD	**Chronic Obstructive Pulmonary Disease**	**74**
CM	**Contrast Media**	**87**
CT	**Computed Tomography**	**93**
DAG	**Directed Acyclic Graph**	**36**
DFD	**Data Flow Diagram**	**61**
DOB	**Date of Birth**	**92**
EHR	**Electronic Health Record**	**88**
EPR	**Electronic Patient Record**	**88**
FMEA	**Failure Mode and Effect Analysis**	**33**
FTA	**Fault Tree Analysis**	**15**

GBDSS	**Guideline Based Decision Support System**	**74**
HAZOP	**Hazard and Operability Study**	**84**
HiP-HOPS	**Hierarchically-Performed Hazard Origin and Propagation Studies**	**39**
HIS	**Health Information System**	**54**
ICAM	**Integrated Computer Aided Manufacturing**	**62**
ICI	**Imperial Chemical Industries**	**78**
IDEF	**Integrated Definition**	**62**
IT	**Information Technology**	**14**
IOM	**Institute of Medicine**	**47**
MBSA	**Model-Based Safety Analysis**	**38**
MCS	**Minimal Cut Set**	**32**
MRI	**Magnetic Resonance Imaging**	**95**
MWL	**Modality Worklist**	**93**
PACS	**Picture Archiving and Communication Systems**	**87**
PRA	**Probabilistic Risk Analysis**	**51**
RIS	**Radiology Information System**	**87**

RCA	**Root Cause Analysis**	**50**
RAD	**Role Activity Diagram**	**59**
SADT	**Structured Analysis and Design Technique**	**62**
UML	**Unified Modelling Language**	**65**
USAF	**US Air Force**	**62**
SIL	**Safety Integrity Level**	**84**
V&V	**Validation and Verification**	**85**
WFMSs	**Workflow Management Systems**	**55**

Appendix 2: Interviews Questions

1. First Set of Interview Questions

The following questions were used in the beginning before the application of the approach to seek information about the safety culture in the hospital (in Jordan):

- In your job, you usually interact with patients who may be anxious about their health. Often they do not understand the impact and the consequences of the simple mistakes they make and sometimes the healthcare providers themselves make simple faults that can propagate to affect the results of a treatment. Therefore, I guess understanding the consequences of any faults during the treatment is very important to both the healthcare provider and the patient. I would like to know to what extent you think that having a clear and safe workflow (careflow) can affect the success of a treatment?
- Are there any preferences for models to be used for effective representation of the workflow?
- In your preferred models, what can you use to identify possible failure modes and their effects on the workflow? Alternatively, tell me if you do not want to identify such failure modes at all and why?

  (Explanation for the concept 'failure modes and their effect' was required in some cases and it was not in others)
- What do you think about having an automated process to build and analyse workflows for their safety? In other words, what do you think about an automation for the development of the workflow and showing all possible failure modes and their effect on the treatment process?
- It is clear that the healthcare team are the only people who can develop clinical workflows accurately. If your organisation employed an analyst to develop and analyse the workflows for their safety, do you mind about being involved in the development and the analysis process? To what extent are you ready to help in this?

2. Interview Questions for Evaluating SAFE-FLOW (first group and second group)

The following set of questions were used to evaluate SAFE-FLOW:

- What does ‘clinical workflows’ and ‘safety analysis’ mean for you? Can the two terms be associated with each other?

Before continuing with the interview, SAFE-FLOW was explained in detail to those participants who were not involved in the case study. Moreover, the used models was discussed to be able to answer the interview questions.

- How easy to understand did you find the models that were used in SAFE-FLOW?
- To what extent did you find that the used models were representative to different components, interactions between components and the workflow concepts?
- Do you have any preferences for models to be used for effective representation of the workflow? If yes, do you think that there is a way to analyse the safety of such models?
- In practice, the workflow is sometimes modified for many reasons. For example, to add a new information system to the workflow. Therefore, a new workflow with new safety hazards will emerge from these modifications. Do you think that the new workflow should also be analysed for its safety? And should the safety analysis results from the new workflow be compared with the safety analysis results from the original workflow? Why?
- Do you think that the approach has the potential to improve clinical workflows and their safety? In other words, how well do you think that SAFE-FLOW succeeded in meeting your needs and how good is the approach itself?
- Did you experience any difficulties during the application of SAFE-FLOW? (this question is designed for the first group participants who were involved in the case study)

- Do you think that being involved in the development and the analysis of workflows can affect your other responsibilities? (this question was for those participants who were not involved in the application process)
- Would you be happy to exactly follow a workflow that is already developed and analysed for its safety rather than thinking and following what you think that is true?
- Do you think that the resulting workflow models and the analysis results can be used as an educational tool to train healthcare staff, especially inexperienced staff members?
- Do you have any suggestions for further developments?

3. Third Group Interview Questions with Answers

- **What does ‘clinical workflows’ and ‘safety analysis’ mean for you? Can the two terms be associated with each other?**

Clinical workflow relates to processes associated with healthcare, typically focussed around patient matters. This may be a general process as a regular screening process (e.g. cancer) for a subsection of a population, or focussed on a specific patient and the events associated with their healthcare management, whether a clinical visit, a biopsy or testing procedure or admission to a health care institute (hospital or clinic) for a specific purpose (e.g. operation).

Safety analysis is used in engineering and design to refer to the systematic process whereby a design or artefact is subjected to, for example, a failure analysis. It can also relate to human oriented processes where health and safety guidelines are applied.

It makes sense for these two terms to be associated with each other, especially in the pursuit of more rigorous healthcare practice.

- **What do you think about having an automated approach to build and analyse workflows for their safety? In other words, what do you think about an automation for the**

development of clinical workflows and showing all possible failure modes and their effect on the treatment process?

Such an approach appears to be a logical way to try and minimise errors and learn from past practice on what are effective work flows and where problems may occur or indeed have occurred. Also the advent of wearable patient devices, utilising wifi and Bluetooth) means patient-centric information can also be incorporated into this process. This has been a research area in Medical Informatics for some time.

One of the most fully formed methods in this area of research is PROforma (Formal knowledge representation method for the development and execution of clinical guidelines) developed by Advanced Computation Laboratory, Cancer Research UK.

SAFE-FLOW is an approach that has been developed for safety analysis of clinical workflows (see Figure 1, page 2 of this document for more information about SAFE-FLOW).

To answer question 3 and question 4 see the attached document named Modelling Material).

- **How easy to understand did you find the models that were used in SAFE-FLOW?**

I find this relatively easy to understand. However, this judgement must be qualified as I have several decades of research experience in Medical Informatics (and related areas) plus nearly ten years research experience in Safety Analysis in computer science.

- **To what extent did you find that the used models were representative to different components, interactions between components and the workflow concepts?**

The presented model is relatively straightforward and not unduly complex, hence the different components and interactions between components is easily seen. However, if this model were developed and applied to more sophisticated clinical workflows, it might not be so clear. The *systematic use of colour, for example, to highlight different categories of component and interaction or the use of different geometries*

- **Do you have any preferences for models to be used for effective representation of the workflow? If yes, do you think that there is a way to analyse the safety of such models?**

I think my answer to this is covered in the above response (Q4). The PROforma model was developed by computer scientists with a vast experience of clinical applications and health informatics. That model is a unified technology for clinical decision support and disease management. The work was based on logic engineering, a distinct design and development methodology that combines concepts from knowledge engineering, logic programming, and software engineering. The principal technical results of the work are the PROforma logic language for defining clinical processes and an associated suite of software tools for delivering applications, such as decision support and disease management procedures. The SAFE-FLOW model may address a more general workflow but could benefit from incorporation of the concepts embodied in PROforma.

- **In practice, the workflow is sometimes modified for many reasons. For example, to add a new information system to the workflow. Therefore, a new workflow with new safety hazards will emerge from these modifications. Do you think that the new workflow should also be analysed for its safety? And should the safety analysis results from the new workflow be compared with the safety analysis results from the original workflow? Why?**

  Any new workflow arising from a modification to an existing model should be analysed for its safety to ensure that the modification does not compromised the model and introduce new opportunities for error and failure. The analysis of the new model should be compared to the older model as it may highlight deficiencies or areas for improvement in either.

- **Do you think that the approach has the potential to improve clinical workflows and their safety? In other words, how well do you think that SAFE-FLOW succeeded in meeting your needs and how good is the approach itself?**

I consider SAFEFLOW a useful endeavour in attempting to minimise error in clinical workflow. The case studies highlight its potential and also areas for further development. Clinical workflow has been recognised as critical for adherence to healthcare guidelines and patient safety for some time

- **Do you think that the resulting workflow models and the analysis results can be used as an educational tool to train healthcare staff, especially unexperienced staff members?**

Such systems should have a great educational benefit in training healthcare staff, and not just unexperienced staff members. Over the past decades there have been many high profile cases where clinical practice has compromised patient safety as the local clinical practice (and often with senior clinicians) has not followed the latest guidelines. A fully developed system that could incorporate current clinical and healthcare guidelines would be continually evolving. As such more experienced staff could also benefit in ensuring that they were fully conversant with any such updates and the effect they may have on their clinical practice.

- **Do you have any suggestions for further developments?**

My suggestions for development have been described throughout. In short SAFEFLOW could benefit from incorporation of some of the ideas and concepts used in PROforma. Also perhaps a cognitive scientist or psychologist used to applied psychology could analyse the system in terms of ease of use and where improvements could be made to minimise human error.

Appendix 3: Case Study: Analysis of a Tele Guideline based Decision support system for Generating Referral Recommendations using HiP-HOPS

Workflow Documentation

This case study focuses on the safety critical aspect of the system, instead of the whole development process of the Tele Guideline Based Decision Support System (GBDSS). Hence, this section presents a generic design choice that has been commonly used and recognised in home telemonitoring systems.

An example of a GBDSS for generating recommendations from routinely recorded home telehealth measurement data was described by (Mohktar *et al.,* 2010). The system was tested on a prospective chronic obstructive pulmonary disease (COPD) home telehealth trial. The objective of the GBDSS is to provide specific recommendations to both patients and carers (carers could be patient's GP, nurse, or even a patient's relative). These recommendations are given based on the patient's measurement data that are recorded by the home telehealth unit (HTU).

The workflow of this system starts by creating and sending a reminder to inform patients to perform their measurements and to respond to the questionnaires that have been scheduled for them. The data are then sent to and automatically stored in a database. Checking the data periodically is the responsibility of the system; for example, in the case of finding any missing data it resends notifications to patients to advise them to complete their measurements' tasks. If the data is complete, classification is performed to make decisions and recommendations depending on a rule-based approach to generate clinical recommendations based on the measurements. These recommendations are sent to patients and their carers. Mohktar *et al.* (2010) discussed applying this framework to support the management of COPD disease patients, although this framework could be applied to manage a number of chronic diseases in home telehealth.

The system's recommendations could be referral recommendations or home management recommendations. Every patient needs to perform some measurements and enter the values of those measurements through the home telehealth unit. Seven criteria are important to be detected: forced expiratory volume in 1 second (FEV1), fever, saturation of peripheral oxygen (SPO2) value, weight, breathlessness, general condition, and sputum. These criteria are measured using particular measurements techniques provided to patients and are used to decide on the stability of the COPD patient. Criteria status which indicate referral are decrease for FEV1, SPO2, and weight; increase in body temperature for fever; severe for breathlessness; deteriorate for general conditions, and increased amount and change of colour for the sputum. The recommendations are given depending on the following (decision tree) rules:

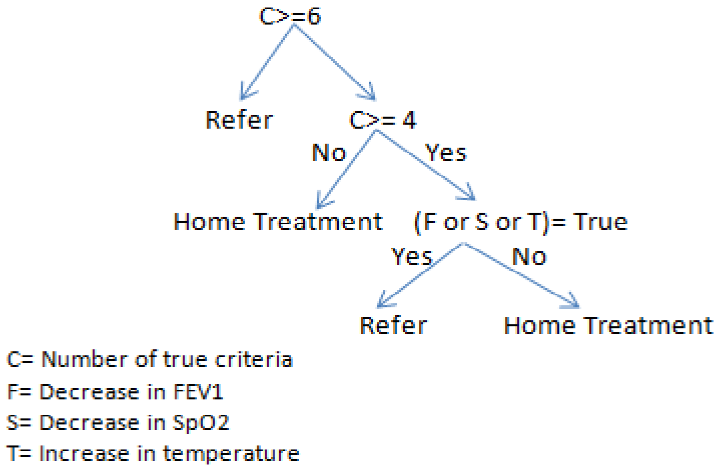


Figure 30 Decision Tree (Mohktar *et al.*, 2010)

If the number of positive criteria is greater than six, then the patient should be referred to the hospital. Otherwise, if the number of positive criteria is greater than four and any of the critical criteria (FEV1, SPO2, or Temperature) are true then the patient will be referred to the hospital. If the number of positive criteria is greater than four but none of the critical criteria is true, then the patient will not be referred and he will be recommended to stay at home.

Different types of failures may occur in the system. For example, regarding the recommendations issued to the patient, the system may experience false negative or false positive errors. False negative error occurs when the system issues a recommendation for home treatment when a referral is required. False positive error occurs when a referral recommendation is issued when only home treatment is needed.

In turn, there are various causes for each of these errors. Those causes need to be investigated. HiP-HOPS is used to effectively analyse the workflow within the system and provide root causes of these errors. Of particular concern is the false negative error, which is deemed to present severe clinical risk compared to the false positive.

Workflow Modelling

For the purpose of the analysis, the system has been modelled using Matlab Simulink. The system consists of the following high-level main components: HTU, Database, and GBDSS. The system may also include measurement equipment that reads the data required to evaluate criteria status (for example, a thermometer can be used to read temperature, which decides the Fever criterion). Measurement equipment can be included in the model, but to maintain simplicity in this case study, the required criteria are directly taken in as input to the system. These criteria are fed into the home telehealth unit and are then stored in the database. The GBDSS processes these criteria based on the classification algorithm and issues patient notifications, patient recommendations and carer recommendations accordingly.

The following figure shows the architecture of the system (Mohktar *et al*, 2010):

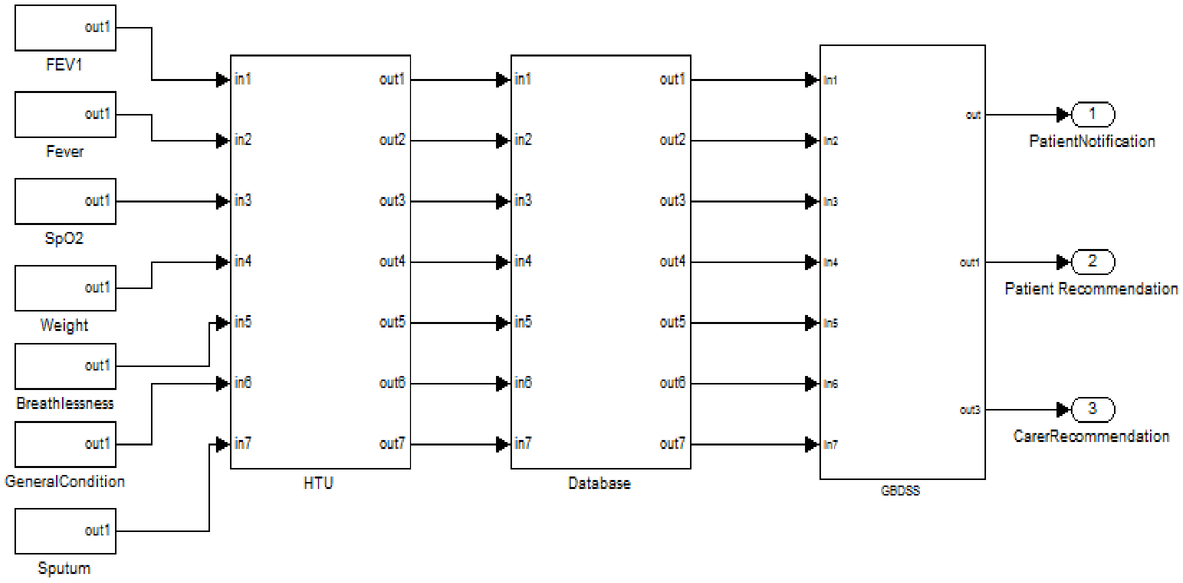


Figure 31 Architecture of the System

The modelling of the algorithm that performs classification and guideline-based decision (referral or home treatment recommendation) is simplified through the decomposition of the GBDSS. Based on the decision tree classification discussed earlier, GBDSS is decomposed to contain the following main components: CriteriaCounter, FSTEvaluator, and DecisionModule. CriteriaCounter performs the counting of the specified criteria which are calculated to be positive. If the number of positive criteria is more than or equal to six, a referral is recommended by DecisionModule. Similarly, if the number of positive criteria is less than four, home treatment is recommended. If the number of positive criteria is larger than or equal to four, FSTEvaluator would check if any of the three critical criteria (decrease in FEV1, decrease in SpO2, and increase in Temperature/Fever) is positive. DecisionModule subsequently decides whether referral or home treatment would be recommended. The following figure shows the simplified architecture and main components of the GBDSS, focusing particularly on the PatientRecommendation output.

The following figure illustrates the architecture of the GBDSS:

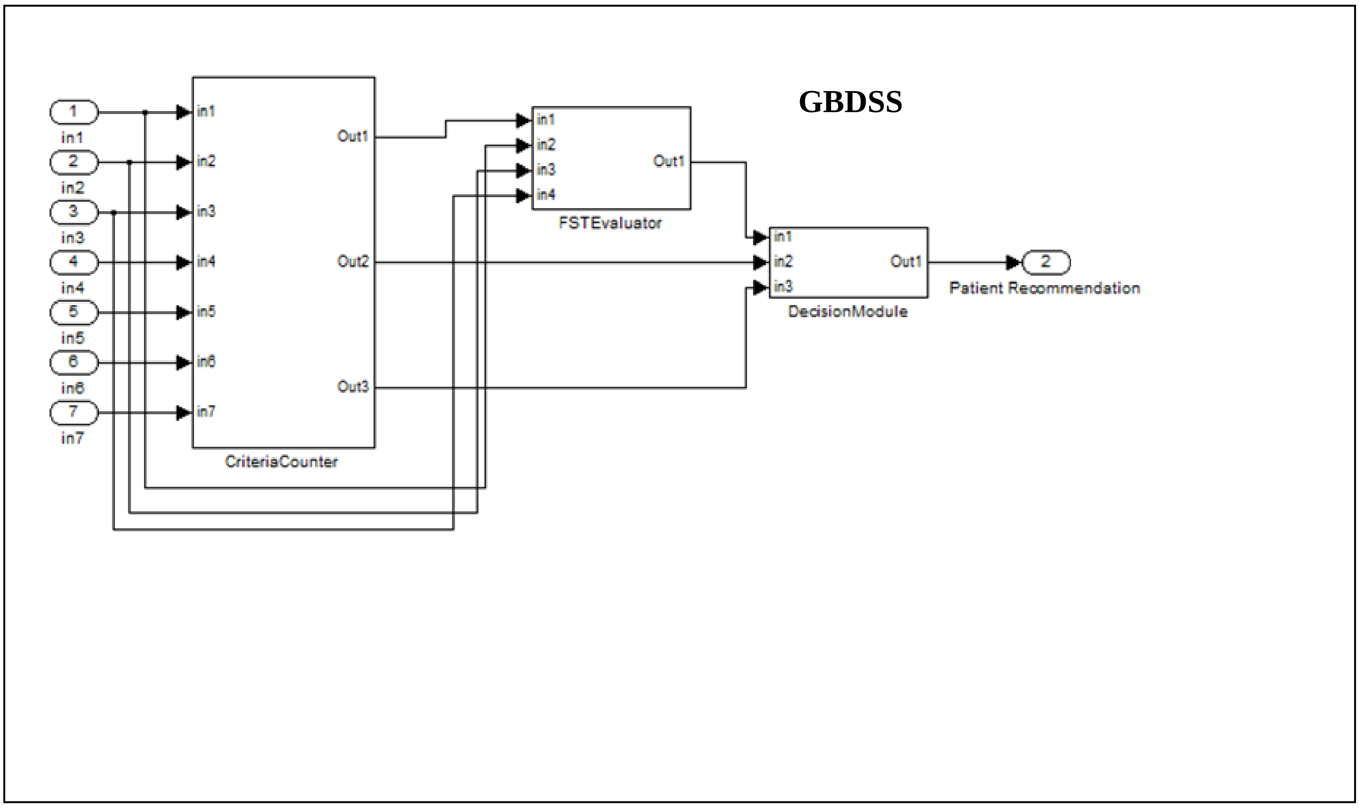


Figure 32 Architecture of the GBDSS after decomposition

Hazards Identification

The aim of the analysis is to identify the root causes of the scenario that has serious clinical risk, in this case, the false negative error where a referral recommendation was not issued when required. The analysis with HiP-HOPS, which produces these results, will allow the system designer or clinicians to understand how this situation may arise and the impact of failure in other components towards this. To do this the component failures that could potentially occur in the components within the architecture were considered, as well as the potential failures in the parameters required to decide the criteria values.

The original discussion (Mohktar *et al.*,2010) presents a Decision Tree figure 26 which allows various failure combinations depending on the number of positive criteria status. For the purposes of this analysis, only the scenario where five positive criteria are observed in the patient is presented and discussed. This will traverse the path of the decision tree where a further three critical criteria (FEV1, Fever, and SpO2) need to be evaluated. Value failure refers to any deviation of value in a parameter, criteria, input or output. Criteria failure here refers to the value failure of criteria status. This may be caused by value failure or omission failure of criteria. For simplicity, only discussion on the value failure of the criteria is presented.

Failure annotation

To enable an automated analysis, the home telemonitoring system is modelled and the model is extended with failure information. This failure information describes how failure in the component output can be caused by the propagation of failure from the component input or the internal malfunction of the component itself.

The analysis focuses on the false negative error, which can be represented by the value failure of the GBDSS output which produces the PatientRecommendation, henceforth will be referred to as “V-PatientRecommendation”. Failure is represented in the format of “V-Component Name.ComponentPort”.

Readings on the important parameters which decide the criteria status (FEV1, Fever, SpO2, Weight, Breathlessness, GeneralCondition and Sputum) are fed into the home telehealth unit via corresponding measurement techniques. Value failure in these parameters can be caused by the failure in equipment or the measurement technique or an error during the data entry. For simplicity, these are modelled as a single internal malfunction causing the value failure for each of the criteria. The internal malfunction for FEV1, Fever, SpO2, Weight, Breathlessness, GeneralCondition and Sputum, are represented as FEV1V, FeverV, SpO2V, WeightV, breathlessnessV, generalConditionV, and sputumV respectively.

Similarly, an internal malfunction of the home telehealth unit (HTUV) may also occur and cause a value failure in the output of the home telehealth unit.

Database internal malfunctions may include software or hardware malfunction, represented as DatabaseSW and DatabaseHW respectively. Similarly, the GBDSS component may experience software and hardware malfunction, which are represented as GBDSS_SW and GBDSS_HW. Each of the components in the GBDSS (CriteriaCounter, FSTEvaluator, and DecisionModule) may also have their own failure – but, again, for simplicity, it is assumed that these are free from failure and only the higher level failures in GBDSS will be propagated and analysed.

HiP-HOPS automatically navigates through the failure information backwards, starting from the system failure (V-PatientRecommendation) and connecting each failure to its causes, linking them with logical operators. This results in the automated construction of the main fault tree which can then be analysed.

V-PatientRecommendation can be directly caused by the value failure of GBDSS output Out1 (V-GBDSS.Out1). V-GBDSS.Out1 is linked to the value failure in its sub-component, DecisionModule, which is, in turn, caused by value failure in the CriteriaCounter or the FSTEvaluator.

A condition of "ConditionNonCriticalC4" has been included to represent the situation where non-critical criteria Weight, Breathlessness, GeneralCondition and Sputum are all positive. This is to allow the modelling of the situation where if all non-critical conditions are true, a single value failure in critical criteria would lead to the occurrence of the V-PatientRecommendation.

Value failure for CriteriaCounter (affecting all outputs) and FSTEvaluator could be caused by:

V-CriteriaCounter = any combination of two criteria failures.

V-FSTEvaluator = (V-Fever **AND** V-FEV1 **AND** V-SpO2**) OR** V-CriteriaCounter **OR (**ConditionNonCriticalC4 **AND** (V-Fever **OR** V-FEV1 **OR** V-SpO2)**)**.

Fault Tree and FMEA Synthesis and Analysis

Once the components of the model have been annotated with the corresponding failure information, root cause analysis can be performed. HiP-HOPS synthesises and analyses the system fault tree and produces the FTA and FMEA results which shows how the value failure in criteria and the component failures (or their combinations) can lead to the false negative error.

The following list shows the MCSs from the FTA:

Table 15 MCSs for the home telemonitoring system

- **DatabaseHW**
- **DatabaseSW**
- **GBDSSHW**
- **GBDSSSW**
- **HTUV**
- **ConditionNonCriticalC4 AND FEV1V**
- **ConditionNonCriticalC4 AND SpO2V**
- **ConditionNonCriticalC4 AND FeverV**
- ***27 combination of any two failures:***

    1. SputumV and WeightV
    2. SpO2V and WeightV

3. SpO2V and SputumV
4. GeneralConditionV and WeightV
5. GeneralConditionV and SputumV
6. GeneralConditionV and SpO2V
7. GBDSS.ConditionNonCriticalC4 and SpO2V
8. GBDSS.FSTEvalulator.ConditionNonCriticalC4 and SpO2V
9. FeverV and WeightV
10. FeverV and SputumV
11. FeverV and SpO2V
12. FeverV and GeneralConditionV
13. FeverV and GBDSS.ConditionNonCriticalC4
14. FeverV and GBDSS.FSTEvaluater.ConditionNonCriticalC4
15. FEV1V and WeightV
16. FEV1V and SputumV
17. FEV1V and SpO2V
18. FEV1V and GeneralConditionC4
19. FEV1V and GBDSS.ConditionNonCriticalC4
20. FEV1V and GBDSS.FSTEvaluater.ConditionNonCriticalC4

21. FEV1V and FeverV

22. BreathlessnessV and WeightV

23. BreathlessnessV and SputumV

24. BreathlessnessV and SpO2V

25. BreathlessnessV and GeneralConditionV

26. BreathlessnessV and FeverV

27. BreathlessnessV and FEV1V

The following presents the resultant FMEA table, which shows component failures having direct effects towards the system failure (false negative error):

Table 16 FMEA direct effects

Criteria/Component Failure	System Failure
DatabaseSW	V-PatientRecommendation
DatabaseHW	V-PatientRecommendation
GBDSSSW	V-PatientRecommendation
GBDSSHW	V-PatientRecommendation
Home Telehealth unit V	V-PatientRecommendation

Table 17 (FMEA Table with component failures having direct effects towards false negative error)

To summarise, the FTA and FMEA results shows that the following failures may lead to the false negative error:

- Any failure in the component home Telehealth unit, Database and GBDSS
- Combination of any two criteria failures - which causes the number of positive criteria to be smaller than 4 (C<4).
- In the case where four non-critical criteria are positive, any failure on one of the critical criteria.

New Workflow Design and Accepting the Workflow

The identification of these root causes allows greater understanding of the factors contributing to the undesired event which can potentially lead to a serious clinical risk. This enables the identification of weak points in the system, which could then be effectively addressed and improved. For example, through the simple structure in this example, the application of HiP-HOPS shows the ability to systematically assist in the identification of single-point failures in the systems (i.e. failure in database and GBDSS hardware and software, and malfunction in the home Telehealth unit). This information can be used to guide the improvement in the design and target the areas where highly-reliable components and fault tolerant mechanisms (for example, through duplication) can be prioritised and introduced to make the architecture more robust and fault tolerant.

HiP-HOPS not only provides a consistent and robust model throughout design and analysis, it also takes the pressure off the designer through the application of effective analysis early in the lifecycle – by detecting potential design flaws early on, they can be quickly remedied before they become serious problems. HiP-HOPS is flexible and scalable, and is therefore well-suited to be performed iteratively throughout the design phase.

Limitation and assumptions:

- The example presented in this appendix is based on the scenario where the patient experiences five positive criteria. Different numbers of positive criteria render different combinations of failures and will need to be modelled accordingly.

- In real life, however, deciding whether the number of positive criteria is correct in the first place can be non-trivial. This may be achieved by ensuring that the initial reading of parameters (from patients to HTU) is correct, for example, through a more fault tolerant measurement technique employing redundancy. As mentioned previously, this example (including the internal malfunction and failure behaviour of each component) has been simplified. Preliminary analysis can be performed to obtain a more comprehensive list of potential failures for each of the component, and these can be provided to and analysed in HiP-HOPS.

On the one hand this case study focused on analysing the false negative error (giving recommendations to patients to stay on home treatment while they need to be referred to hospital). On the other hand, the false positive error (giving referral recommendations to patients when they could stay on home treatment) is not analysed but can be.