A Safety Analysis Approach to Clinical Workflows: Application and Evaluation

Safety Analysis of Clinical Workflows

Lamis Al-Qora'n, Neil Gordon, Martin Walker, Septavera Sharvia, Sohag Kabir
Department of Computer Science
University of Hull
Hull, United Kingdom

***Abstract*—Clinical workflows are safety critical workflows as they have the potential to cause harm or death to patients. Their safety needs to be considered as early as possible in the development process. Effective safety analysis methods are required to ensure the safety of these high-risk workflows, because errors that may happen through routine workflow could propagate within the workflow to result in harmful failures of the system's output. This paper shows how to apply an approach for safety analysis of clinical workflows to analyse the safety of the workflow within a radiology department and evaluates the approach in terms of usability and benefits. The outcomes of using this approach include identification of the root causes of hazardous workflow failures that may put patients' lives at risk. We show that the approach is applicable to this area of healthcare and is able to present added value through the detailed information on possible failures, of both their causes and effects; therefore, it has the potential to improve the safety of radiology and other clinical workflows.**

Keywords*—*clinical workflows; safety analysis; radiology; HiP-HOPS

I. Introduction

Clinical workflow as defined by [1] is a term that is used to describe the healthcare activities that are performed carefully by more than one member to accomplish a clinical process (e.g. treatment or diagnosis) and to produce a certain clinical service.

Due to the growing number of adverse events, risk management of healthcare activities, the issue of patient safety, medical errors prevention and adverse events reporting are broadly studied nowadays. 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 American hospitals and over one million injuries [1]. Moreover, around 425,000 patients (5% of total) admitted to hospitals in England and Wales each year experience adverse events from medical errors [2].

So, clinical workflows can be described as safety critical workflows because they have the potential to cause harm or death to patients. Their safety needs to be considered as early as possible in their development process, where the safety analysis results can be used to refine the models and to derive more detailed functional models and specifications of the workflow.

In [3] an approach to safety analysis of clinical workflows was proposed, which is explained in the next section. The approach is applied to a case study and an evaluation of the approach and its benefits is shown through the paper.

II. An Approach for Safety Analaysis of Clinical Workflows

The following figure shows an approach for safety analysis of clinical workflows proposed by [3]:

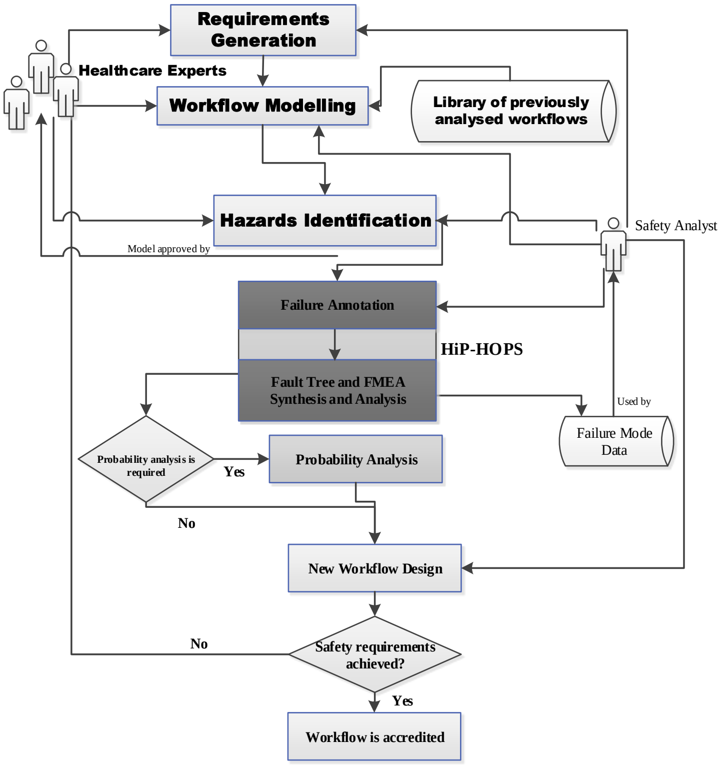


Fig.1. An Approach to Safety Analysis of Clinical Workflows [3]

The approach is designed to support the development and safety analysis of clinical workflows. It starts with the process of requirements generation where the workflow is documented in order to understand it, then the workflow documentation is translated into models by the safety analyst and the healthcare team. After that the safety analyst - in cooperation with the healthcare team - start the process of hazards identification in order to extend the models with the local behavior of each component, and then in an automatic manner the tool (Hierarchically-Performed Hazard Origin and Propagation Studies (HiP-HOPS)) generates both Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA) results. These results are qualitative in the sense that they show how the failure of a single component or combinations of failures of different components can lead to system failure. If the results of qualitative analyses are enough then the new workflow design can be generated based on the outcomes of the analyses. Otherwise, if quantitative analysis is required then it has to be done before starting with the new workflow design. Finally, if the workflow requirements are achieved then the workflow can be accredited.

FTA [4] is a common safety analysis technique through which root causes of an undesired event are identified. It is a deductive technique which determines how an undesired event (often termed the *top event*) can be caused by lower level failures (or events) or their combinations. Quantitative analysis of the FTA can be implemented to calculate the probability of the top event and qualitative analysis is performed to identify the necessary and sufficient combinations of events which can cause the top event (termed Minimal Cut Sets (MCS)). Quantitative analysis of a fault tree, which follows qualitative analysis, can help to estimate the probability of the top event occurring from the given failure rates of basic failure modes of the system. Failure Mode and Effect Analysis (FMEA), on the other hand, is an inductive safety analysis technique that examines the effect of lower level (component) failures towards the higher-level system failures. FTA and FMEA has a wide use in exploring and analysing healthcare issues related to patient safety (e.g. [5]; [6]; [7]), and they showed their ability to analyse clinical processes. Automated FTA and FMEA would present and provide more efficiency in analysing clinical processes.

HiP-HOPS which was initially proposed by [8], is a state-of-the-art technique, which has been prominently used in mechanical systems to effectively identify weak points in system design. It is a predictive safety analysis technique which enables semi-automated FTA and FMEA. In other words, it incorporates, automates, and integrates a number of classical techniques. The current implementation of the HiP-HOPS has the design optimisation capability that can help to select component and subsystem among different alternatives as well as helps to decide the level and location of replicated components.

HiP-HOPS works in combination with a number of frequently used system modelling tools or packages (e.g. Matlab Simulink), from which it receives block diagrams of systems being analysed and associated failure behaviour. It includes three main phases: a modelling phase, a synthesis phase, and an analysis phase where MCSs and FMEA are generated. The process starts when designers build a model of the system, then they annotate the model and its components with detailed failure information. Internal failure information can be annotated into the components as a set of Boolean expressions that are manually added to each component to describe how failures of the component output can be caused by a single input failure and/or a combination of input failures and/or by internal malfunctions of the component itself. These expressions essentially represent the component fault trees of the system components describing the generation, propagation, and transformation of failures between the inputs and outputs of the components. After defining the behaviour of a component, the component can be stored in the library to allow greater degree of reusability.

Qualitative analysis is performed based on the logical failure behaviour of the components and it starts with a top event (system failure) and traverses the model by following the propagation of the failures backwards from the top level of the system towards the basic component level. The outcome of this process is a fault tree showing the failure behaviour of the whole system. As this fault tree is relatively complex therefore it is minimised by applying logical rules to obtain minimal cut sets. As part of the qualitative analysis, FMEA is also generated from the fault trees.

In addition to the logical failure behaviour of the components, numerical data (e.g. failure rate, severity of the component) can also be entered for the components. Quantitative analysis can be performed based on the numerical data entered for the components. As seen in Figure 1, the quantitative analysis is optional in the proposed approach. However, if quantitative analysis is required and sufficient data for the analysis are available then it is possible to quantify the fault tree to get the probability of the top event. As MCSs of the fault tree are represented as the conjunction (AND gate) of the statistically independent basic failure modes therefore the probability of a MCS be obtained using the following equation.

$$P(MCS_i) = \prod_{j=1}^{n} P(BE_j) \qquad (1)$$

Where $P(MCS_i)$ is the probability of the minimal cut set *i* and $P(BE_j)$ is the probability of the basic event *j*.

Since the top event is represented as the disjunction (OR gate) of the MCSs, therefore, the top event probability can be calculated as [9]:

$$P(top\ event) = 1 - \prod_{i=1}^{n} (1 - P(MCS_i)) \qquad (2)$$

where $P(top\ event)$ is the probability of the top event.

In the clinical workflows, a lot of human activities are involved; therefore, human errors are expected to constitute a great proportion of the basic failure modes. It is relatively easy to quantify the failure probability of mechanical components; in contrast, it is difficult to quantify the probability of the human error due to the uncertainty involved in quantifying human behaviour. So, uncertainty in human behaviour may require to be considered in the quantitative analysis. One possible way is to translate the fault tree into Bayesian Networks (BNs) using the method shown in [10] and then perform the probabilistic analysis because BNs are considered as efficient methods for performing probabilistic inference under uncertainty.

HiP-HOPS can in general be applied to systems that involve data, information or material flow. However, in our case "components" may represent clinical processes, humans, tasks, or any other components of a clinical workflow architecture.

HiP-HOPS was proposed by [11] to analyse the safety of the workflow of a home Telemonitoring system. This paper applies an integrated approach which utilises HiP-HOPS to conduct safety analysis of a RIS/PACS workflow. The result of the analysis is the root causes of different failures, and their direct and indirect effects on both the workflow and the patients themselves.

III. Application of the Approach to a Case Study

Radiology Information Systems (RIS) and Picture Archiving and Communication Systems (PACS) technology has advanced dramatically in recent years, including the technology of acquiring, storing, retrieving, displaying, and distributing clinical images [12]. It has become a mature technology and has been commonly implemented in a number of developed countries [13]. Different systems have been designed and developed to assist different workflows in the radiology departments in several hospitals. In Jordan for example, RIS/PACS are implemented in a number of private, government, and military hospitals. To investigate the concerns that medical staff have due to the adoption of RIS/PACS systems, we conducted a number of interviews in one of the Jordanian hospitals. These were followed by another set of interviews to document the workflow in the radiology department in the same hospital, where RIS/PACS has been adopted. We found that faults and errors in the workflows might lead to harmful failures in the outputs (e.g. producing a report that has 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.

With this prevalence of RIS/PACS in healthcare institutions, there is a growing need to analyse their workflow safety, both ensuring the safety of the workflow design and the safety during the operational phase. In other words, securing the design of the theoretical workflow in terms of safety issues, and then making sure about following this workflow in the operational phase. 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 [14].

A RIS as defined by [15] is a computer system designed to support operational workflow and business analysis within a radiology department; it is a repository of patient data and reports which contributes to the electronic patient record (EPR) or electronic health record (EHR). [15] 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 propagate to affect the EHRs, which may put clinicians in a situation where they make wrong diagnosis and consequently put patients' lives at risk.

The interviews showed that one of the main concerns about adopting the RIS/PACS systems is the potential lack of reliability and thus lack of safety of these systems; this is due to the difference between the theoretical workflow and the operational workflow. Furthermore, even the theoretical workflow possibly has many problems with its safety, as where the safety issue was not addressed specifically during the workflow design. This leads to output failures of different parts of the workflow and eventually failure of the final output of the system. These failures of outputs can be defined by output deviations, where an output deviation outlines a set of Boolean expressions that shows the causes of the output failure, and the relationships between them. These causes can involve internal failures, input deviations, or both.

There is a scarcity of published literature addressing the problem of analysing the operational workflow and its safety. It is uncommon to have a formal automated safety analysis in healthcare for the management of healthcare systems' operational workflows such as the workflow within the radiology department. Little information is available regarding operational errors in RIS/PACS workflows (e.g. [7]). Research to date has not identified efficient automated approaches for workflow errors risk reduction. Many aspects of RIS/PACS design can be changed through the safety analysis of the workflow, as a flawed workflow design has the potential to decrease the efficiency and increase user errors during the operational phase of the workflow.

In the face of these limitations, this paper identifies potential significant errors in a RIS/PACS workflow by means of the following:

- Using an integrated safety analysis approach to analyse the safety of the RIS/PACS workflow
- Using the results of the empirical study to document and model both the detailed processes and the in depth tasks of one failure scenario of this workflow.
- Collecting data regarding occurrence of the workflow errors and their prevention in the same scenario environment.
- Discussing current approaches to reduce the risk of errors in the RIS/PACS workflow.

The following sections show the application of each step in the approach to analyse the safety of the workflow with this radiology department.

A. *Requirements Generation*

While documenting the requirements we found that 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 our case, 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. 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 our case) or by coming immediately from the HIS, then this information (which includes 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 work list (MWL) where the orders are scheduled to be sent to the image acquisition modality. Here at the image acquiCsition 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. At 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 Tele-radiology), and produce a report as an output. This report is to be passed to the clinician to make the diagnoses and give a medicine or recommend for another procedure such as an operation.

This paper considers one of the workflow scenarios; the purpose is to analyse possible failures of this scenario and to find out the root causes of these failures. This scenario is the workflow for a computerised tomography (CT) scanner. A 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.

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, a pregnancy check must be done to make sure that the woman who will start the exam 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 Contrast Media (CM) for the CT scan. Another preparation guideline is to ask the patient to drink another 500ml of water after arriving to 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 jewels 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.

An injection of the contrast is often given before or throughout the scan. CM contains iodine and appears as white areas on the scans, which help the radiologist to differentiate between certain organs or tissues and the other structures. The contrast may be ingested as a drink, or 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 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 an hour at least 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 goes home, for example, again asking the patient to drink 500ml of water to rehydrate the body after the CM injection.

B. *Workflow Modelling*

Workflow model should specify the systems involved in producing a medical service and different agents who are interacting with these systems. Moreover, it should specify the dataflow as well as the sequence of event. The following figure shows the workflow within the considered radiology department. Matlab Simulink was used for the modelling process. The information from the EHR is relayed back to the HIS component.

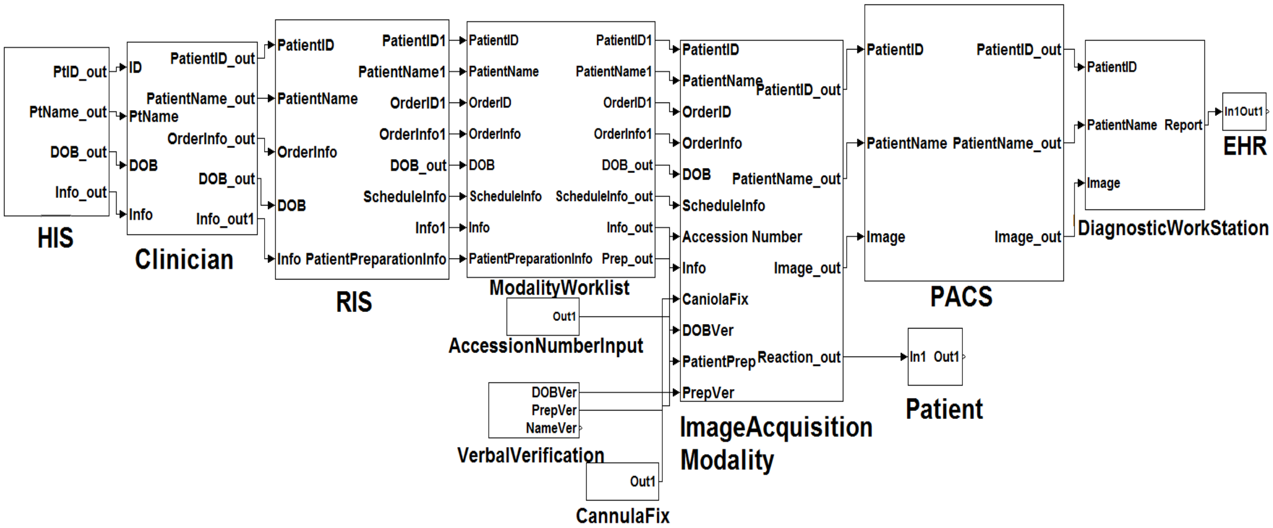


Fig.2. RIS/PACS Workflow

The EHR is modelled as a subcomponent of the HIS and it has the following information:

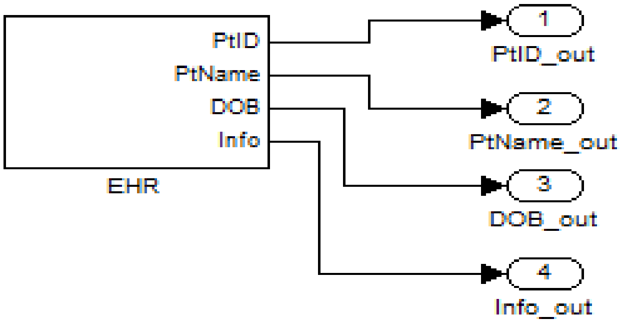


Fig.3. EHR Component

The CM is modelled as a separate component (subcomponent of the ImageAcquisitionModality):

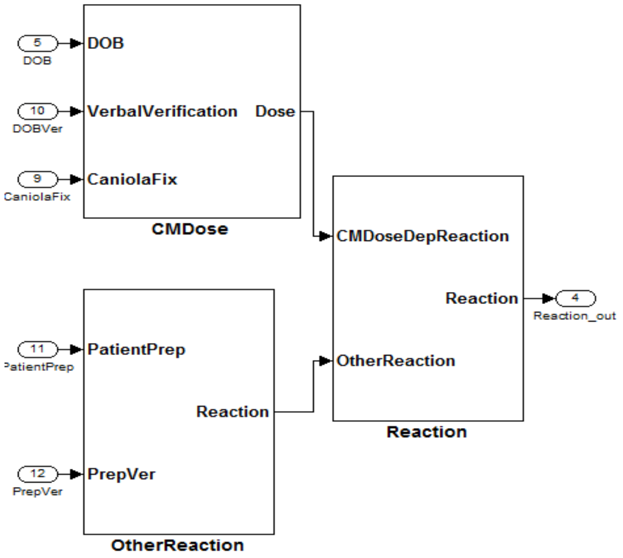


Fig.4. The CM Component

C. Hazards Identification

After the analyst builds the model, the accuracy of the model is discussed with the healthcare experts in the hospital as well as the possible ways the whole workflow can fail. Possible faults in each component are specified. After that the analyst job will be to prepare the logical failure expressions which are appropriate for the failure annotation.

Errors may happen at any point where there is a data entry. This paper focuses on the failures caused by DoB errors in the CT scan workflow scenario.

A CT scan is considered as a safe procedure, although there can be reactions to contrast media CM which usually cannot be predicted [16].

For example, the dose of contrast media which is given to the patients is different for adults and children. Therefore, date of birth is an important factor for specifying the amount of CM to administer. Giving the patient an overdose of CM has reactions that affect patient health and put the patient in a hazardous situation.

Faults may occur at different points in the workflow and need to be identified.

D. Failure Annotation

Failure annotation is performed using the HiP-HOPS tool; all the components need to be annotated with possible faults. HiP-HOPS then analyses the model to give the fault trees that detects the possible failures and provide the root causes for them. In addition, it provides us with information about their effects on the output of the workflow.

HiP-HOPS has a simple language for annotating the components with reusable failure logic. For example,

O-Out = O-In or InternalFailure

On the left is the output deviation, which represents a failure propagated from an output port of the component. On the right is the cause of that deviation, consisting of the basic deviations or basic events. Both input and output deviations consist of a user-defined failure class representing the type of failure (e.g. O= omission) and the name of the port question. We can annotate the same component with multiple output deviations, and failure annotations as well can be applied to subcomponents, in other words, it can be hierarchical.

So, the interview's data are analysed to document the RIS/PACS system's workflow. Then the documented information is used to model the workflow to enable the automated analysis. After that, possible hazards are identified and failure expressions are now ready to be annotated into the model for several scenarios. As explained earlier this failure expressions 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 first scenario analysis focuses on having side effects or bad reactions by the patient. As described by the system 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 V-Patient.Out1.

The patient's DoB is entered into HIS together with other information. Value failure of DoB which could be caused by wrong data entry is represented as V-DoB_out, also omission of the DoB causes problems and it is classified here as output deviation of the HIS. Omission of DoB is represented here as O-DoB_out. Moreover, HIS internal malfunctions can cause the 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. Clinician might make data entry errors which are represented here as IDDataEntryError or DoBDataEntryError. The output deviations are represented as V-PatientID_out and V-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, RIS may suffer from failure of the preparation data, which is PrpDataEntryError. Therefore, output deviations at 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: O-DoB_out, V-DoB_out, V-PatientPreparationInfo, and O-PatientPreparationInfo.

ModalityWorkList is a database, which 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 first 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 DoB and the failure of the preparation information output either as a value failure or omission of this value. These are represented as V-DoB_out, V-Prep_out, and O-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 which 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: O-DOBVer and O-PrepVer.

Fixing the cannula for the contrast medium is considered as well 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 V-Out1.

The CM dose is considered as a subcomponent of the image acquisition modality and failure of this is giving the wrong dose for the patient. This is represented as V-Dose, which can be caused by either wrong dose calculation or wrong measurement. 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 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 annotated as well with possible failures. The output deviation of this component is having any type of reactions by the patient. This is represented as V-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.

We did not annotate both the PACS and the diagnostic workstations component with failure information for the purpose of this scenario. We assumed that 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 the other possible failures of the workflow.

There are other scenarios that may possibly cause defective results, but again, for simplicity, they are not covered in this paper. For example, when the patient gives information to the clinician, the patient might not tell the right information about his situation and the clinician might not check. Those two conditions together result in creating the wrong history for the patient. When the clinician has the wrong information, he or she will ask for the wrong exam order that in turn causes the wrong examination description. At the time of the examination, if the patient did not tell and the radiographer did not verify this, and he or she has the wrong exam description, these conditions together might give a false report for the patient, which results in an incorrect procedure or the wrong medication.

Another failure that can potentially cause patient harm but is not considered in this paper is when images are mislabelled for the wrong patient and/or the wrong study. These kinds of failures result in images that are incorrectly associated with the patient's EHR and may lead to incorrect diagnoses, medication, or procedures.

Other failures might happen because of an incorrect entry for the DoB of the patient, which occurs when the clinician enters the wrong DoB in both the HIS and the RIS. These faults together result in the wrong DoB of the patient which cause an incorrect dose of both radiation and the CM. Here the patient is under the risk of extra dose of radiation and dose dependent reactions of CM. The dose dependent reactions of CM are analysed in this paper.

E. *Fault Tree and FMEA Synthesis and Analysis*

We annotated the components of the model with the corresponding logical failure information and then performed the root cause analysis. At present, as sufficient numerical data for the components are not available therefore the numerical data associated with components are not entered as part of the annotation. HiP-HOPS synthesises and analyses the system fault trees and produces the FTA and FMEA results, which shows how the value failure in an input and the component failures (or their combinations) can lead to the failure in causing unintended reactions or side effects towards the patients.

The following figure shows the FTA result. For simplicity, V-Reaction is represented as Unintended Reaction in the FTA and FMEA table:

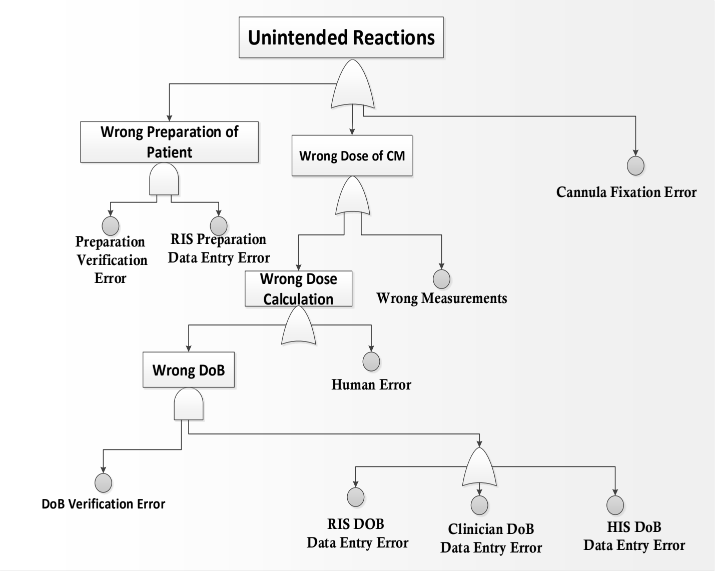
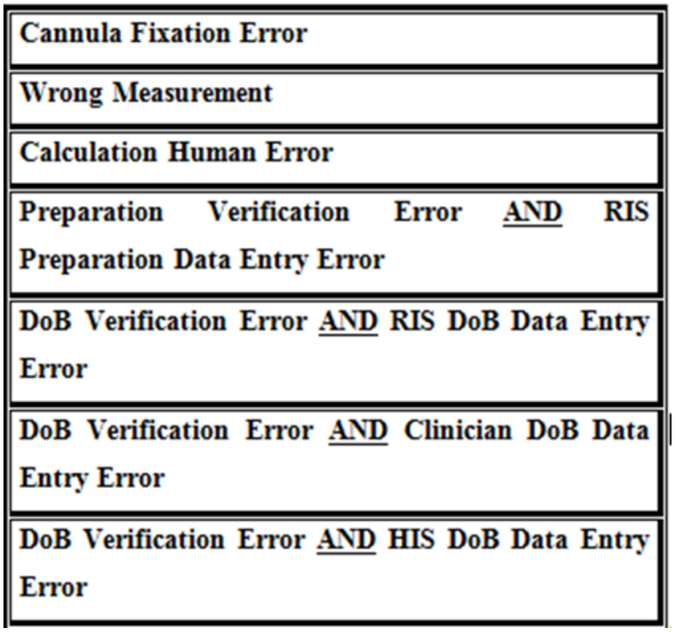


Fig.5. FTA Result

The following list shows the MCS [4] from the FTA:

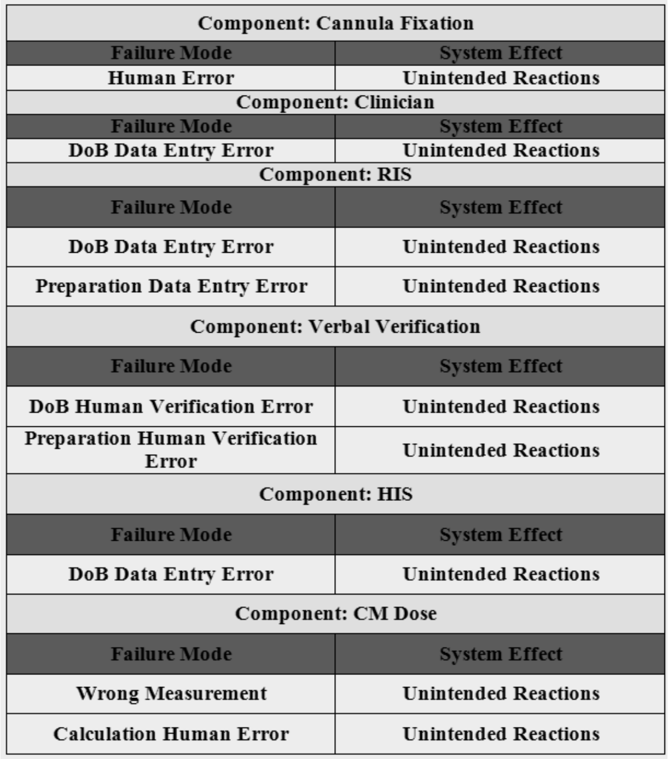
TABLE.I. MCS FROM FTA



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

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

TABLE.II. FMEA TABLE



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 failures may lead to the failure of the first scenario (which is in this case getting unwanted reactions 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 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 extra dose of radiation because 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 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 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 the reactions.
- 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.
- Wrong measurements to calculate the dose of CM can directly cause the unwanted reactions. This might happen because of not understanding the units of measurements, or using wrong 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 wrong 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, the unintended reactions towards the patient will occur.

These errors can be avoided by adding extra functionality to the HIS or RIS or both of them (for example, bar coded patients help to avoid data entry errors by radiologists and clinicians). Moreover, adding extra tasks in the workflow may help to avoid the errors.

Human error in fixing the cannula for the CM also contributes directly to the unintended reactions. So, radiologists or nurses who perform this task should be informed about potential failures which it may cause and about their direct and indirect effects on the patient. As mentioned earlier, the numerical data for the components of the system in the case study are not considered; hence, quantitative analysis is not performed in this paper.

F. New Workflow Design and Accreditation of the Workflow

A new workflow can be proposed with some additional tasks and avoiding the potential failures. Existing critical tasks may be highlighted as important tasks to focus the attention of the healthcare team to the importance of this task.

The model optimisation capability of HiP-HOPS [17] can also produce different alternative models to help to achieve safety requirements, and in doing so it can assist in selecting component and subsystems among different alternatives as well as helping to decide the level and location of replicated components.

G. Evaluation of the Approach

To evaluate our approach the concerns about the application of the approach to analyse the safety of clinical workflows were discussed with both healthcare and technical experts in a systematic manner. The approach is found to have the required usability; it is tool based and a user friendly graphical modelling tool (Matlab Simulink) is used for the modelling process. Of course, the analyst's ability to create the models has a non-trivial impact on the accuracy of the models. However, the approach suggests that models should be checked and approved by healthcare experts before proceeding with the other steps.

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 our approach 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 our approach, healthcare experts are no more involved in the safety analysis process after the workflow has modelled. Therefore when fault trees are generated by the HiP-HOPs tool then they can be translated into BNs, thus benefit from the strength of the BNs while involvements of the healthcare experts are also ensured.

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, state machine based model will be required to be transformed to other models e.g. fault trees, Markov chains, Bayesian Networks. Another issue of state machine based approach is that they increasingly face state explosion problem, i.e., for a relatively complex workflow, number of states required to model the complete failure behaviour of the workflow grows exponentially with the number of components of the workflow, thus are difficult to create and analyse.

The process of hazards identification is done by the analyst in cooperation with the healthcare experts. 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 the HiP-HOPS. In terms of usability, HiP-HOPS has a graphical user interface which is easy to use, and it does not need an expert as it is uncomplicated in comparison with the other methods.

In comparison with other model checking [18] 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 HiP-HOPS and model checking [19] 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 [20]. And, the model optimisation capability of HiP-HOPS can produce different alternative models to achieve safety requirements and can help to select component and subsystem among different alternatives as well as helps to decide the level and location of replicated components.

Workflow models are reusable and maintainable; that is if a certain workflow has been done 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.

The safety analysis approach has the potential to affect both the workflow and the clinical service quality. The approach supports a large part of the workflow development process, in particular the design phase of the development process. The clinical service quality (which is the output of the clinical workflow) is improved and maintained through specifying the exact safe steps or baths which can lead to the service.

In the case where a workflow management system is required, then the approach has the potential to help in developing a reliable workflow management system; as the approach improves the quality of the design phase which leads to a better quality in the following software engineering stages.

It is generally accepted that a high quality product requires a high quality design. Theoretically, we can generate a hypothesis that if a high-quality safety analysis approach is maintained, its output has the potential to help in preparing high-quality and reliable clinical workflows.

Data on the applicability of the proposed approach were gathered through an informal testing shown positive usability and effective results. Our results were discussed with experts in the hospital where the data were collected and they appreciated the ability of the approach to focus on processes and how this could be employed for several applications in clinical workflows. Moreover, having the fact that our analysis results are happening in the hospital as actual failures has the potential to validate our approach.

Our approach drew the map for the root causes of these failures. 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. The approach provides an effective means to accomplish this goal, is able to provide a valid theoretical framework consisting of modelling the processes and sub processes and their error analysis. The study findings contribute towards a larger research effort being proposed for reducing medical errors and enhancing patient safety.

Dependability can be improved based on the analysis from the tool: the workflow can be adapted, with workflow components substituted with more reliable components, components can be replicated to introduce redundancy and the frequency of maintenance can be increased for critical components.

IV. Conclusions and Contributions

The automated 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, which could then be effectively addressed and improved.

The simple act of undertaking a safety analysis in this way helps to improve understanding of the behavior 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, more comprehensive analyses 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.

For example, through the simple structure in this example, the application of HiP-HOPS 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 design 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.

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

Having this detailed workflow with a detailed analysis of the failure behaviour can enable healthcare organisations to develop material to be used by medical staff in safety training workshops. These workshops should help the medical staff to build safety awareness that may be useful to avoid the expected failures in the workflow.

Using HiP-HOPS in workflow analysis in general has the potential to give effective analysis by detecting possible design flaws early before serious problems happen. This also helps to provide the medical staff the awareness they require and aids in redesigning the workflow to produce an effective and fault free workflow.

Moreover, such modelling of the workflow and the analysis results can also be used as an educational tool for training of radiologists, nurses, and clinicians. This helps the trainees in identifying errors and preventing the potential errors from leading to adverse events.

The example presented in this paper is based on one scenario, while different scenarios need to be modelled and analysed to get a comprehensive analysis of the workflow. Moreover, conducting research of this nature on only one location is limiting, and having more sites opens a wider range of failures determination.

V. Future Work

HiP-HOPS is designed to consider local failures, where each component and its outputs/inputs has its own failure data. In clinical workflows, sometimes we may have the case where all components share the same cause of failure (e.g. human failure). The common cause failure idea allows this to be modelled, and this could be an improved way to model human failures in future.

References

[1] L. Kohn, J. Corrigan, and M. Donaldson: ‘To err is human: building a safer health system’ (National Academies Press, 2000).

[2] M. Ruffolo, M. Manna, V. Cozza, and R. Ursino: ‘Semantic clinical process management’, in CBMS, pp. 518-523

[3] L. Al-Qora'n, N.Gordon, S. Sharvia, M. Walker, Y. Papadopoulos: ‘An Approach to Safety Analysis of Clinical Workflows’, Athens: ATINER's Conference Paper Series, No: COM2014-1157.

[4] W. Vesely, F. Goldberg, N. Roberts, and D. Haasl: ‘Fault tree handbook’, No.NUREG-0492, Nuclear regulatory comission washington dc, 1981.

[5] L. Ward, M. Lyons, S. Barclay, J. Anderson, P. Buckle, and P. Clarkson: ‘Using fault tree analysis (FTA) in healthcare: a case study of repeat prescribing in primary care’, Patient Safety Research: Shaping the European Agenda, 2007.

[6] E. Ekaette, R. Lee, D. Cooke, S. Iftody, and P. Craighead: ‘Probabilistic fault tree analysis of a radiation treatment system’, Risk analysis, 2007, 27, (6), pp. 1395-1410.

[7] H. Abujudeh, and R. Kaewlai: ‘Radiology Failure Mode and Effect Analysis: What Is It? 1’, Radiology, 2009, 252, (2), pp. 544-550.

[8] Y. Papadopoulos, and J. McDermid: ‘Hierarchically performed hazard origin and propagation studies’: ‘Computer safety, reliability and security’ (Springer, 1999), pp. 139-152

[9] J. Esary, and F. Proschan: ‘Coherent structures of non-identical components’, Technometrics, 1963, 5, (2), pp. 191-209

[10] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla: ‘Improving the analysis of dependable systems by mapping fault trees into Bayesian networks’, Reliability Engineering & System Safety, 2001 b, 71, (3), pp. 249-260.

[11] L. Al-Qora'n, S. Sharvia, N. Gordon, and Y. Papadopoulos: ‘Safety Analysis of a Remote Patient Monitoring System with a Guideline Based Decision Support’, Luxembourg: Porceedings of Med-e-Tel, April 2013 pp. 322-327

[12] S. Boochever: ‘HIS/RIS/PACS integration: getting to the gold standard’, Radiol Manage, 2004, 26, (3), pp. 16-24

[13] [13] G. Paré, D. Aubry, L. Lepanto, and C. Sicotte: ‘Evaluating PACS success: a multidimensional model’, Proceedings of the 38th Annual Hawaii International Conference on. IEEE, 2005, pp. 147c-147c

[14] A. Ouvry: ‘Workflow analysis and modeling in medical IT projects’, Medicamundi, 2002, 46, (2), pp. 47-55

[15] The Royal College of Radiologists: ‘Radiology Information Systems’, 2008,[Online].Available: http://www.rcr.ac.uk/docs/radiology/pdf/IT_guidance_RISApr08.pdf

[16] F. Stacul: ‘Managing the risk associated with use of contrast media for computed tomography’, European journal of radiology, 2007, 62, pp. 33-37

[17] Y. Papadopoulos, M. Walker, D. Parker, E. Rüde, R. Hamann, A. Uhlig, U. Grätz, and R. Lien: ‘Engineering failure analysis and design optimisation with HiP-HOPS’, Engineering Failure Analysis, 2011, 18, (2), pp. 590-608.

[18] E. Clarke, O. Grumberg, and D. Peled: ‘Model checking’ (MIT press, 1999).

[19] S. Sharvia, and Y. Papadopoulos: ‘an Approach towards Integrated Safety Assessment ’, in Proceedings of the IEEE 7thInternational Conference on Automation Science and Engineering. Trieste, August 2011.

[20] M. Adachi, Y. Papadopoulos, S. Sharvia, D. Parker, and T. Tohdo: ‘An approach to optimization of fault tolerant architectures using HiP-HOPS’, Software: Practice and Experience, 2011, 41, (11), pp. 1303-1327