Reliability Modelling of Redundant Safety Systems without Automatic Diagnostics Incorporating Common Cause Failures and Process Demand

Siamak Alizadeh [1,a] , Srinivas Sriramula [2,*]

[1] School of Engineering, University of Aberdeen, AB24 3UE, Aberdeen, UK.

[a] Email Address: Siamak.Alizadeh@hotmail.co.uk; Tel: +44 (0)7726 295920.

[2] Lloyd's Register Foundation Centre for Safety & Reliability Engineering, University of Aberdeen, AB24 3UE, Aberdeen, UK.

[*] Corresponding Author: Dr Srinivas Sriramula; Email Address: s.sriramula@abdn.ac.uk; Tel: +44 (0)1224 272778; Fax: +44 (0)1224 272497.

Abstract

Redundant safety systems are commonly used in the process industry to respond to hazardous events. In redundant systems composed of identical units, Common Cause Failures (CCFs) can significantly influence system performance with regards to reliability and safety. However, their impact has been overlooked due to the inherent complexity of modelling common cause induced failures. This article develops a reliability model for a redundant safety system using Markov analysis approach. The proposed model incorporates process demands in conjunction with CCF for the first time and evaluates their impacts on the reliability quantification of safety systems without automatic diagnostics. The reliability of the Markov model is quantified by considering the Probability of Failure on Demand (PFD) as a measure for low demand systems. The safety performance of the model is analysed using Hazardous Event Frequency (HEF) to evaluate the frequency of entering a hazardous state that will lead to an accident if the situation is not controlled. The utilisation of Markov model for a simple case study of a pressure protection system is demonstrated and it is shown that the proposed approach gives a sufficiently accurate result for all demand rates, durations, component failure rates and corresponding repair rates for low demand mode of operation. The Markov model proposed in this paper assumes the absence of automatic diagnostics, along with multiple stage repair strategy for CCFs and restoration of the system from hazardous state to the “as good as new” state.

Keywords: Markov analysis; Safety instrumented systems; Common cause failure; Process demand; Hazardous event frequency.

1.0 Introduction

Safety systems are widely used to respond to hazardous events e.g. high pressure, high temperature, gas release etc and to mitigate their consequences to humans, the environment, and plant / financial assets. A safety system should provide an independent layer of protection by implementing the safety function through various techniques. In this regard Safety Instrumented Systems (SISs) have acquired specific attention in hazardous industries due to their prominent role in preventing undesirable events. The required functionality and reliability of a safety system are usually deduced from overall hazard and risk analyses. Without adequate design,

fabrication, installation, construction, commissioning and maintenance the safety system may fail to provide the necessary risk reduction. Hence, a number of standards and guidelines have been developed to assist in designing and implementing safety systems. One such standard is IEC 61508 [1], that outlines key requirements to all phases of the SIS life cycle of Electric, Electronic and Programmable Electronic Systems (E / E / PES). The principles introduced in this generic standard are also reflected in its sectorial standards, such as IEC 61511 [2] for the process industry.

The SIS performance must be verified using a suitable methodology. No specific technique is recommended in IEC 61508 or IEC 61511, although some of these are cited in their appendices. Amongst these methods proposed for analysing the SIS reliability are Simplified Equation (SE) [1,3], Reliability Block Diagram (RBD) [4,5], Fault Tree Analysis (FTA) [6,7] and Markov Analysis [8–10]. More recently, Petri Nets (PN) approach has also been introduced to model the SIS reliability [11]. A comparison of these techniques conducted by Rouvroye and Brombacher concludes that Markov analysis covers most aspects for quantitative safety evaluation [12]. Furthermore, Guo and Yang [4] highlighted that Markov analysis shows more flexibility and is the only technique that can describe dynamic transitions among different system states. Jin et al. [13] utilised Markov analysis to calculate hazardous event frequency (HEF), which also relates to the safety performance of SIS. Innal [14] investigated the performance of different modelling approaches and concluded that Markov methods are the most suitable, predominantly due to their flexibility (see also [9,15]). Although Markov analysis is one of the most comprehensive techniques used today, it is very time consuming to construct the model for a large and complex system manually as the number of states increases with the number of system components. Moreover, it is very difficult to handle large Markov models as they require a substantial amount of calculation. Therefore, it has been widely recognised that the design of Markov models for a complex SIS architecture is challenging and error prone [13].

Bukowski [9] presented a simple Markov model of SIS that explicitly incorporates process demand. This model includes both dangerous detected and undetected modes of failure in conjunction with process demand, imposed by process system. Jin et al. [13] further developed the model created by Bukowski [9] and incorporated the safe failure rate for safety instrumented system and repair rate for dangerous undetected failures. A Markov chain was generated by Liu

et al. [16] for a 1oo2 system which extends the application of Markov analysis to redundant configurations subject to process demand. The Markov transition diagram introduced by Liu et al. [16] overlooks the impact of CCF by exclusion, imposing a deficiency on the reliability model for 1oo2 systems. In this paper we intend to address this limitation by embedding CCF for a 1oo2 redundant structure as well as other established component failure modes, in addition to incorporating process demand. Furthermore, this model is deemed as one step closer to analysing actual behaviour of the redundant configuration since CCF influences reliability and safety performances of the safety systems and cannot be discarded.

The main objective of the present article is to explore the relationships between the CCF and SIS reliability and safety performance when incorporating both the demand rate and the demand duration by using Markov methods. Typical SIS configurations consist of 1oo1, 1oo2, 1oo3 and 2oo3 [14]. In this study, only the first two configurations are considered, a 1oo1 safety system (i.e. a single unit) and a 1oo2 redundant safety structure. The Markov models of systems with more components will be complex and the salient features of the approach will easily disappear in the technical calculations. The reliability model developed as part of this research is based on Markov chains for their ability to model safety systems precisely and correctly in low demand. The paper proposes the integration of the following parameters: dangerous undetected failures, common cause failure, safe failures, repair rates, process demand and demand duration.

The proposed reliability model is flexible to accommodate different repair strategies. In this paper only the multiple stage repair strategy of CCF has been considered however, where single stage repair for CCF is possible (e.g. removal of the vibration source, unblocking the common header etc.) the proposed Markov chain can be re-arranged to accommodate an alternative repair strategy of redundant configuration. The remainder of this article is organized as follows: Section 2 discusses the modelling considerations and Section 3 consists of SIS fundamentals. Section 4 is devoted to Markov Analysis and Section 5 entail the analysis of 1oo1 and 1oo2 safety systems followed by a numerical analysis studied in Section 6. Applications of the developed model are discussed in Section 7 based on the results obtained, and conclusions are outlined at the end of this section.

2.0 Modelling Considerations

2.1 Safe state

The primary objective of SIS design is to lead the Equipment Under Control (EUC) to a safe state in response to a demand. As the EUC have various modes of operations e.g. start-up, shutdown, normal operation etc., it is not always straightforward to define the safe state. In some cases, the safe state is to retain the original state of the EUC prior to occurrence of the demand such as a Dynamic Positioning (DP) system. In other cases, the safe state corresponds to cease the operation of EUC e.g. when equipment is overheated etc. It is common that the EUC remains in the safe state after the SIS has responded to a demand in the process hydrocarbon industry. The SIS is only reset back to the original state upon deciding to restart the EUC. For instance in the event of a loss of containment e.g. gas leakage, the Emergency Shutdown (ESD) system ceases the process by closing dedicated Emergency Shutdown Valves (ESDVs). The ESD system maintains this state, until the remedial action for repair of the leak point has been undertaken and the operators have decided to restart the EUC. When the safe state is defined, the next step is to design SIS, taking cognisance of “fail-safe” position. This means that upon foreseeable SIS failures such as loss of power supply etc, the SIS automatically leads the EUC to a safe state.

2.2 Hazardous event

A hazardous event is defined as a significant deviation from the normal operating conditions that may, if not controlled develop into an accident [5]. As discussed previously, a preventative SIS contributes to reduce the likelihood of such events and SISs are used as mitigation measures that aim to control and reduce the severity of the consequences. The term Hazardous Event Frequency (HEF) is used in this article for quantification of safety performance of SISs. Youshiamura et al. [17] offered three categories of hazardous events including repeatable-hazardous, renewable hazardous and non-renewable fatal hazardous events, these can be explained as:

- Repeatable-hazardous event, where the hazardous event does not necessarily lead to severe consequences, even if the SIS fails.

- Renewable hazardous events, where the consequence of the hazardous event is detrimental to the EUC and possibly the SIS, but not in a way that prevents the systems from being restored to the original status within a reasonable timescale.
- Non-renewable fatal hazardous events, where the damage is extensive, and no recovery is possible. The Piper Alpha accident in 1988 is an example of an event of this category.

2.3 Layers of Protection

Independent protection layers are often, prescribed to ensure that the desired risk reduction is achieved for the equipment under control. Protection layers can be implemented by physical barriers such as mechanical systems, instrumented protective functions or in the form of administrative procedures. The sequence of protection layers as illustrated by the "onion model" [2,18] starts from the centre and proceeds outwards, first with layers contributing towards reducing frequency and then with consequence reducing layers [13]. The primary objective of the frequency reducing measures is to prevent a hazardous event from occurring e.g. gas leakage, whilst the consequence reducing protection layers aim to cease the development of an undesirable event into accidents (e.g. explosion, fires etc.) which may harm humans, the environment, or material and financial assets.

A SIS can be used in both capacities. High demand SISs are often of the first category of protection layers to reduce the likelihood of hazard occurrence, and low demand SISs designed to address the latter. In the reliability performance quantification, it is essential to take the sequence of activation of protection layers into cognisance. Where a SIS is used to mitigate the consequences of a hazardous event, and it appears as the last layer of protection, then the failure of SIS may directly lead to an accident.

2.4 Safety systems

The term "safety-related system" or "safety system" applies to those systems that solely or in conjunction with other systems, achieve and/or maintain a safe status for equipment under control [19]. A safety system is an independent protection layer designed to be activated by hazardous events. The safety systems may be network-based or require wire infrastructure. The network based safety systems are frequently used in a wide range of safety applications due to

ease of deployment and as a result of advancement in electronic miniaturisation and radio communication.

3.0 Safety Instrumented Systems

Safety Instrumented Systems (SISs) are widely utilised across process industry to prevent the occurrence of hazardous events, such as excessive high pressure hydrocarbon gas leading to loss of containment and subsequent fire / explosion. These systems are installed as preventative measures to reduce the likelihood of such events. Furthermore, SISs can be used to mitigate the consequences of undesirable events such as initiation of an active fire protection system upon detection of fire in a process module. A SIS typically comprises of three main elements including input device(s) such as sensors, transmitters etc; logic solver(s) including programmable logic controllers, relay logic systems etc and final element(s) such as safety valves. A SIS may perform one or more Safety Instrumented Functions (SIFs) to achieve or maintain a safe state for the EUC including equipment and/or system the SIS is protecting against a specific process demand [5]. As it is the SIF that provides protective function against a specific hazardous scenario, the reliability modelling is always conducted with respect to a specific SIF. Nevertheless, we refer to reliability of SIS (in line with most of the publications in the literature) although what we essentially refer to is one SIF. In this paper, the reliability modelling is presented for a single subsystem of identical elements, however it is comparatively effortless to extend the computation to the entire SIF.

3.1 Low demand and High demand

IEC 61508 identifies two distinct modes of SIS operation including low demand and high demand based on two criteria: (i) The frequency at which the SIS is expected to operate in response to demands, and (ii) The expected time interval that a failure may remain unrevealed, taking into account the proof test frequency.

In accordance with IEC 61508, a SIS is operating in the high demand mode if the demand rate is greater than once per year, or greater than twice the frequency of proof tests. Typical high-demand SISs are DP systems for ships and offshore mobile vessels, and anti-lock braking systems for automobiles. If the demands continuously occur, the mode of operation is known as

continuous. A SIS is operating in low demand mode when the demand rate is less than once per year, and less than twice the proof test frequency. Examples of low demand SISs include Emergency Shutdown Systems (ESD), Fire & Gas (F&G) detection systems and Process Shutdown Systems (PSD). The duration of demand may also vary from instantaneous up to a rather long period e.g. weeks. This article is focused on SISs in low demand applications only.

3.2 PFD and Integrity level

The requirements of safety function outlined in [1,2] present a probabilistic approach for the quantitative evaluation of the safety performance. This has led to the introduction of probability into the assessment of the integrity level and in particular the concept of probability of failure on demand (PFD) and probability of failure per hour (PFH). The qualification of SIF performance is determined by Safety Integrity Level (SIL). The international standard IEC 61508 establishes 4 classification of SILs, where SIL 4 corresponds to the highest and SIL 1 to the lowest integrity level requirements [1]. In order to claim that a SIF provides a certain integrity level, it is necessary (but not sufficient) to achieve a certain reliability performance. In order to quantify the reliability, the standard recommends PFD as a reliability measure for low demand SISs and PFH for high demand SISs. In accordance with IEC 61508, a SIL should be allocated to each SIF.

3.3 Failure modes and Testing strategies

When SIS components fail, the SIS response to the component failures is either a safe or dangerous failure of the SIS [1]. Safe failures are characterised by a spurious alarm or trip which causes the system to fail safe, e.g. the component operates without demand [19]. Safe failures do not have any effect on the ability of the SIS to perform its functions. The safe failure rates are denoted by λ_S. Dangerous failures are characterised as failures which cause the system to fail dangerous, e.g. the component does not operate on demand. Dangerous failures may prevent the SIS from performing its function. The dangerous failure rates are denoted by λ_D and the overall failure rate of a component λ is obtained from $\lambda = \lambda_D + \lambda_S$.

Dangerous failures are divided into further two subcategories i.e. detected and undetected failures. Dangerous Detected (DD) failures are identified by online diagnostic testing, whereas Dangerous Undetected (DU) failures remain hidden until revealed by proof testing (or functional

testing) in real demand or during a spurious trip when the SIS is fully operated. Similarly the safe failures are divided into Safe Detected (SD) and Safe Undetected (SU) failures. Splitting the dangerous and safe failures into detected and undetected failures, the overall component failure rate consists of the summation of these four main elements:

$$\lambda = \lambda_{DD} + \lambda_{DU} + \lambda_{SD} + \lambda_{SU} \quad (1)$$

where λ_{DD} represents DD failure rate, λ_{DU} is DU failure rate, λ_{SU} denotes SU failure rate and λ_{SD} signifies the SD failure rate. Proof tests are normally performed at regular time intervals to reveal and correct DU-failures before a demand occurs. Although the necessity of proof testing for high demand SISs is not always evident [13], it is essential to perform a proof test for low demand SISs to check that a DU-failure does not remain hidden for a long time.

3.4 Diagnostic testing

The main purpose of diagnostic testing is to reveal certain types of failures such as signal transmission errors without fully operating the main functions of the component and interrupting the equipment under control. Diagnostic testing is a feature that is usually embedded within programmable electronic components. Diagnostic tests are run frequently, usually every few seconds, minutes, or hours. The time interval between the occurrence of dangerous detected failures and detection via diagnostic testing is negligible. For low demand SISs, this allows adequate time to conduct repair activities and restore the component function prior to the next process demand. This assumption may not be valid for high demand SISs as the process demand and diagnostic test frequency could be in the same order of magnitude [13]. The fraction of dangerous failures that is diagnosed by testing is often referred to as the diagnostic coverage [1,2]. IEC 61508 defines the Diagnostic Coverage (DC) rate as the ratio between the failure rate of detected failures and the total failure rate [20]. As such, the DC rate for dangerous detected represents the effectiveness of the diagnostic test and is given as:

$$DC_D = \frac{\lambda_{DD}}{\lambda_D} = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \quad (2)$$

DC rate distinguishes both the dangerous and safe failures into detected and undetected, resulting in four distinct failure modes [21] as:

$$\lambda_{DD} = DC_D.\lambda_D \qquad \lambda_{DU} = (1 - DC_D).\lambda_D$$
$$\lambda_{SD} = DC_S.\lambda_S \qquad \lambda_{SU} = (1 - DC_S).\lambda_S \tag{3}$$

The total failure rate is expressed by the following equation considering the estimated DC:

$$\lambda = DC_D.\lambda_D + (1 - DC_D).\lambda_D + DC_S.\lambda_S + (1 - DC_S).\lambda_S \tag{4}$$

The impact of diagnostic testing should be carefully incorporated at design stage taking into account the influencing elements such as process demand frequency, diagnostic test coverage, the diagnostic test interval and time required for completion of the repair.

3.5 Common Cause Failures

The importance of CCFs is highlighted by various researchers. Hokstad et al. [22] and Lundteigen et al. [23] investigated the importance of CCF in SIS performance assessment. A CCF is a failure affecting several or all of the redundant components simultaneously, potentially leading to failure of the safety function and subsequently SIS failure in response to a process demand. As such, during the design process, potential CCFs and their impacts on the SIS functionality shall be identified and eliminated where deemed practical or reduced as far as reasonably practicable [22,23]. The introduction of the common cause expression in reliability analysis of safety systems allows for computing the influence of these failures on the PFD of a SIS [24,25]. In this regard calculating the PFD for a redundant system can take cognisance of such failures by directly introducing them into the failure probability evaluation process [26]. Considering the limitations in obtaining CCF data in the process industry in the absence of a sole database, the CCF model in this article is developed parametrically.

Several models have been considered in the literature [22] for assessment of CCF to evaluate the impact on overall reliability of SIS. These methods include the β factor model [27], the PDS method [28], the model of Multiple Greek Letters (MGL) [29], the α factor model [30], the Boundary model [19] and the system Cut-off model [19]. This paper uses the β factor model for assessment of CCF. The β factor model recommended by IEC 61508 [5,25] is the simplest, most commonly used model which implies a fixed proportion of the failures arising from a common cause [19]. In this model due to lack of data associated with CCF, β is usually estimated by

experts, using the checklist approach [31,32]. Rahimi et al. [33] discussed how human and organizational factors may influence CCF in SIS and outlined the challenges in assessing the β factor. In accordance with the β factor model, the total failure rate of a component (λ^T) is the sum of CCF (λ^C) and independent failures (λ^I) [21]:

$$\lambda^T = \lambda^I + \lambda^C \tag{5}$$

The factor β is defined as the failure probability due to a common cause given the occurrence of a failure [23,24], given as:

$$\beta = \frac{\lambda^C}{\lambda^T} = \frac{\lambda^C}{\lambda^I + \lambda^C} \tag{6}$$

The total failure rate of a component (λ^T) is then equivalent to:

$$\lambda^T = \lambda^I + \lambda^C = (1-\beta)\lambda^T + \beta\lambda^T \tag{7}$$

Taking into account that the detected and undetected failure modes are divided into independent and common cause failures, the CCF quantification is as follows:

$$\lambda^T = \lambda^I_{DD} + \lambda^C_{DD} + \lambda^I_{DU} + \lambda^C_{DD} + \lambda^I_{SD} + \lambda^C_{DD} + \lambda^I_{SU} + \lambda^C_{DD} \tag{8}$$

The various rates of the detected and undetected dangerous failures become:

$$\begin{cases} \lambda^I_{DD} = (1-\beta_D).\lambda_{DD} = (1-\beta_D).DC.\lambda_D \\ \lambda^C_{DD} = \beta_D.\lambda_{DD} = \beta_D.DC.\lambda_D \\ \lambda^I_{DU} = (1-\beta_U).\lambda_{DU} = (1-\beta_U).(1-DC).\lambda_D \\ \lambda^C_{DU} = \beta_U.\lambda_{DU} = \beta_U.(1-DC).\lambda_D \end{cases} \tag{9}$$

where β_D and β_U represent the proportion of detected and undetected common cause failures related to the DC rate, respectively [10]. In this paper Safe failures and Dangerous failures are considered according to the description provided in Section 3.3. As the objective of Markov model is to determine the PFD, only the dangerous failures of the components are considered. Additionally, in the proposed Markov model the rate of independent failures is segregated from

the total failure rate, such that $(1-\beta_U)\lambda_{DU}$ is used instead of λ_{DU} for independent DU failures. Subsequently CCF rates, $\beta_U\lambda_{DU}$, leading to subsystem unavailability/failure are clearly identified for redundant subsystems. This provides an opportunity for the design engineers/analysers to study general behaviour of the system, for instance to measure the probability of system operating with only one of the components in failed states which can be used as a risk based approach for prioritisation of maintenance backlog for safety systems.

4.0 Markov analysis and Hazardous Event Frequency

Markov Analysis (MA) is one of the reliability methods proposed in IEC 61511 [2] to evaluate system reliability. It is a holistic approach to model the behaviour of dependable system where the rate of change in system status (known as transition) from one state to another is constant. The basic principle of Markov analysis is that a system can exist in different states, which enables modelling system dynamics such as failure modes of the components, and repair and test strategies. Furthermore, this method allows CCF to be explicitly incorporated into the Markov models and hence the need for implicit incorporation of CCF models is reduced [22]. The Markov chains presented in this article follow homogeneous process indicating that transition probabilities are time independent, i.e. components of the system fail at constant failure rate and are restored at constant restoration rates [10,16]. This assumption is consistent with useful life of components i.e. maturity phase of bathtub curve.

A Markov chain is a transition diagram and graphical representation of system dynamics where the nodes correspond to system states (e.g. failure/repair) and the vectors represent the transition probabilities. This allows the model to take into account various dependencies between system status and to conduct a dynamic analysis of the system [24]. Assuming the transition probability from state i to j at time t is denoted by $p_{ij}(t)$, the transition rate is obtained from:

$$q_{ij} = \frac{d}{dt}p_{ij}(t) = \lim_{t\to 0}\frac{p_{ij}(t)}{t} \tag{10}$$

where q_{ij} represents transition rate from state i to state j which depends only on states i and j. The transition rate matrix $Q = [q_{ij}]$ of size $(r \times r)$ is constructed from all transition rates q_{ij} (where $q_{ii} = -\sum_{i\neq j} q_{ij}$) as follows:

$$Q = [q_{ij}] = \begin{bmatrix} q_{11} & \cdots & q_{1n} \\ \vdots & \ddots & \vdots \\ q_{r1} & \cdots & q_{rn} \end{bmatrix} \quad (11)$$

As Q is a transition rate matrix, the sum of each row of Q is equal to zero and all transition rates q_{ij} $(i \neq j)$ are equal to or greater than zero. Using Kolmogorov Forward Equations [5]:

$$\acute{P}(t) = P(t).Q \quad (12)$$

where $P(t) = [P_0(t), P_1(t), \dots, P_r(t)]$, $P_i(t)$ is the probability that the system is in state i at time t, and $\acute{P}(t)$ is the time derivative of $P(t)$. The probability of a system being in state i in an irreducible continuous time Markov process when $t \to \infty$ is irrespective of the initial state of the system and constant:

$$\pi_i = \lim_{t\to\infty} P_i(t) \quad i = 1,2, \dots, r \quad (13)$$

&

$$\lim_{t\to\infty} \acute{P}_i(t) = 0 \quad i = 1,2, \dots, r \quad (14)$$

The vector $\pi = [\pi_1, \dots, \pi_r]$ represents the steady state probabilities and the fact that the sum of the steady state probabilities is always equal to 1. The following linear system of equations can be used for a homogeneous Markov chain to calculate the steady state probabilities [5]:

$$\begin{cases} \pi.Q = 0 \\ \sum_{i=1}^{r} \pi_i = 1 \end{cases} \quad (15)$$

The steady state probability for state i, π_i, is the long-run probability that the system is in state i. It can also be interpreted as the mean proportion of time the system is in state i [13]. The system transits to the hazardous state when a demand is present whilst the SIS is failed dangerously. In a Markov model, the frequency of entering a hazardous state can be obtained directly from the transition diagram. The hazardous event frequency (HEF) is equal to the visit frequency to state 0, from any other state [5]:

$$HEF = \sum_{i=1}^{r} q_{i0}\,\pi_i \tag{16}$$

In this article, we aim to investigate the reliability performance of safety system with redundant components assuming that the steady state unavailability (due to dangerous failure) corresponds to the average PFD. This takes into account the process demand rate and duration of demand for safety systems operating in low demand mode. A framework for Markov analysis of redundant safety systems incorporating process demand is illustrated in Figure 1.

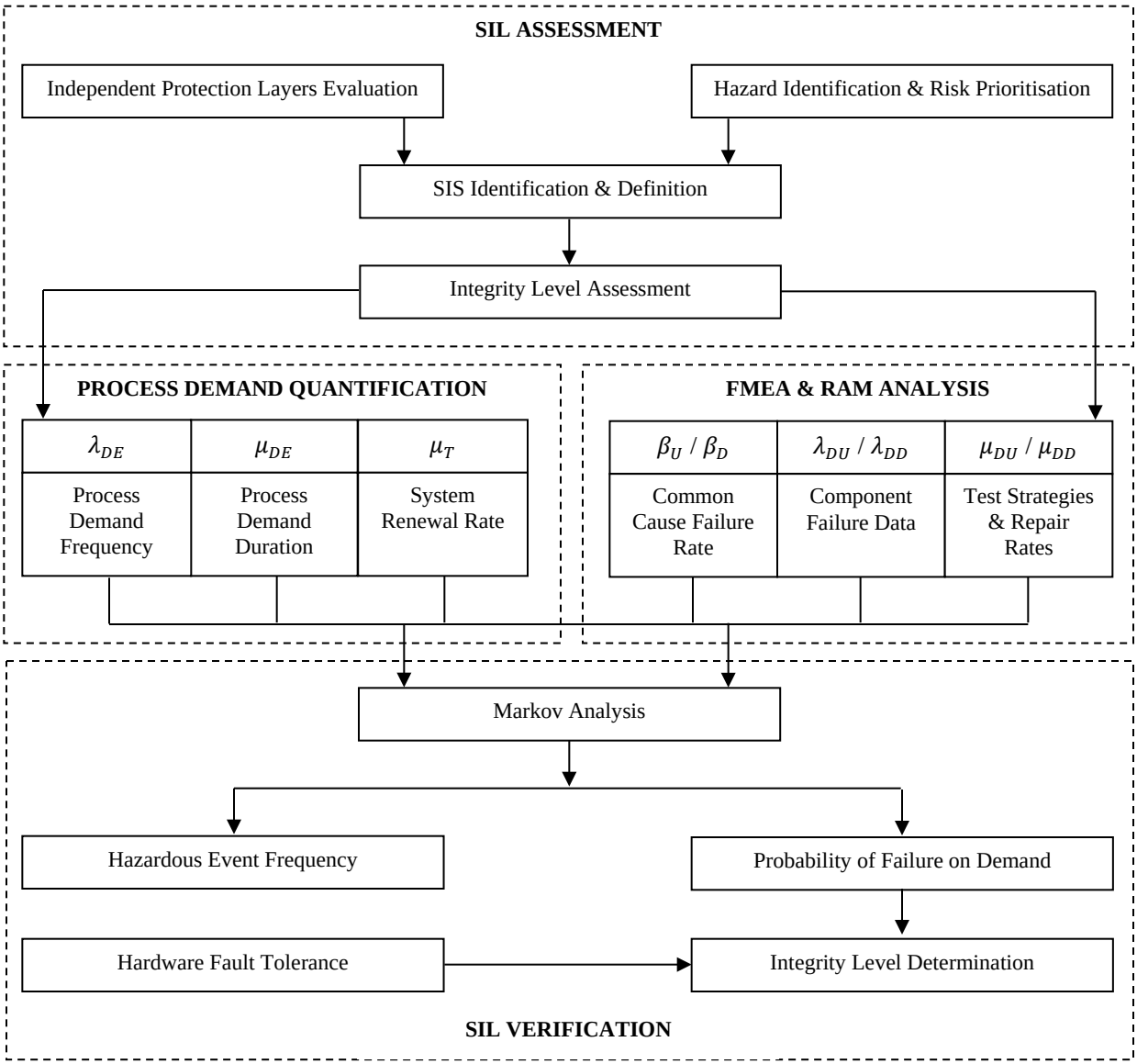

Figure 1 – Framework for Markov Analysis of Redundant Safety Systems Incorporating Process Demand

5.0 Markov Analysis of Safety Systems

In this section two reliability models for 1oo1 and 1oo2 safety systems are compiled using Markov analysis technique. The reliability models are developed by establishing a set of technical assumptions, defining system states, setting test strategies and outlining performance indicators for each system individually.

5.1 1oo1 Safety System

We start by analysing a 1oo1 simple safety system of pressure relief valve. In order to achieve this, the Markov model for a 1oo1 SIS [5] is re-constructed and then amended accordingly to adopt characteristics of a simple pressure relief system [16].

5.1.1 Assumptions

The underlying assumptions of this SIS model are as follows:

- All failure rates (dangerous / safe, detected / undetected) are constant in time; i.e. the times to failure are exponentially distributed.
- Failures occur independently and their severities are constant over time.
- The system is studied over one test interval.
- Proof tests are carried out periodically in line with test intervals of the system.
- Proof tests are comprehensive and 100% accurate.
- The system can be considered “as good as new” post completion of a repair or a proof test.
- The process demand rate is constant, i.e. the time between demands is exponentially distributed.
- The process demand duration is exponentially distributed.
- The restoration time from hazardous state is exponentially distributed.
- Single repair / maintenance team is available onsite.

5.1.2 Definition of System States

The system’s situation consists of the combined effect of the SIS state and process demand levied on the SIS. A SIS is in “available” state when it is able to respond to a process demand upon occurrence. In this case the SIS is not failed due to DD or DU failure and has not been

spuriously activated; SIS is defined as “functioning” state when it is responding to a process demand. The “safe state” means that the EUC is in a state where it is safe regardless of whether there is a demand, or not.

A state transition diagram [5] for the 1oo1 system is shown in Figure 2. The system transition rates including dangerous undetected / detected and associated repair rates are listed as follows:

- λ_{DU} DU failure rate - the frequency that a DU failure occurs per hour
- λ_{DD} DD failure rate - the frequency that a DD failure occurs per hour
- μ_{DU} DU repair rate - the frequency that an active repair of DU occurs per hour
- μ_{DD} DD repair rate - the frequency that a reset from the DD state occurs per hour

The system transition rates due to safe failures (both detected and undetected) and associated repair rate are:

- λ_S safe failure rate - the frequency that a safe failure occurs per hour
- μ_S restoration rate - the frequency that a reset from the safe state occurs per hour

Furthermore, the transition rates due to imposition of process demand and system reinstatement when process demand is nullified are as follows:

- λ_{DE} process demand rate - the frequency that a process demand occurs per hour
- μ_{DE} demand reset rate - the frequency that the process demand recovers per hour

Lastly, system restoration from the hazardous state to the fully functional state is:

- μ_T renewal rate - the frequency that a renewal from hazardous state occurs per hour

5.1.3 Testing strategies and Repair rates

In addition to diagnostic testing, the system under study is subject to frequent proof testing, also known as functional testing. It is assumed that the proof tests are carried out after regular time intervals of length *t*.

Assuming the repair actions are commenced immediately after detection of the failure, the equipment downtime is limited to the actual repair time. Hence, the DD repair rate, μ_{DD}, can be obtained from the Mean Time To Repair (MTTR) as follows:

$$\mu_{DD} = \frac{1}{MTTR} \tag{17}$$

However, the equipment downtime for DU failures are not limited to the repair time only as the failure is unknown and has not yet been revealed by a diagnostic test. The undetected failures can be revealed upon discharge of a process demand or by proof testing assuming these tests are comprehensive and 100% accurate in detecting unrevealed failures. The average downtime for undetected failures consists of:

- unknown downtime - the average downtime prior to detection of the failure which is equivalent to half of the test intervals i.e. $\tau/_2$ [5].
- known downtime - the equipment downtime due to repair assuming the remedial actions are commenced immediately after detection of the failure during proof testing. The time to perform a proof test is often negligible and hence excluded from average downtime.

The DU repair rate, μ_{DU}, for an undetected failure can be calculated as:

$$\mu_{DU} = \frac{1}{MTTR + \tau/_2} \tag{18}$$

Of the two contributors to the downtime of undetected failures, the unknown part is generally dominating the overall downtime of equipment.

5.1.4 System Description

A Markov model for a simple safety instrumented system of 1oo1 was originally introduced by Rausand & Høyland [5]. The states of the considered 1oo1 system are given in Table 1. In the transition diagram (Figure 2), state 5 represents the initial and normal operating state, where the SIS is available and there is no demand for activation of the SIS. The safe state is represented by

state 4 indicating that the EUC is safe regardless of whether there is a demand or not, and hence no hazardous event can happen. The transitions between states 5 and 4 are due to safe failure (e.g. spurious activation) and restoration.

Table 1 – States of 1oo1 System

State	Property	Demand State
0	Hazardous State	On Demand
1	Dangerous Undetected Failure	No Demand
2	Demand State	On Demand
3	Dangerous Detected Failure	No Demand
4	Safe State	N/A
5	Fully Functioning State	No Demand

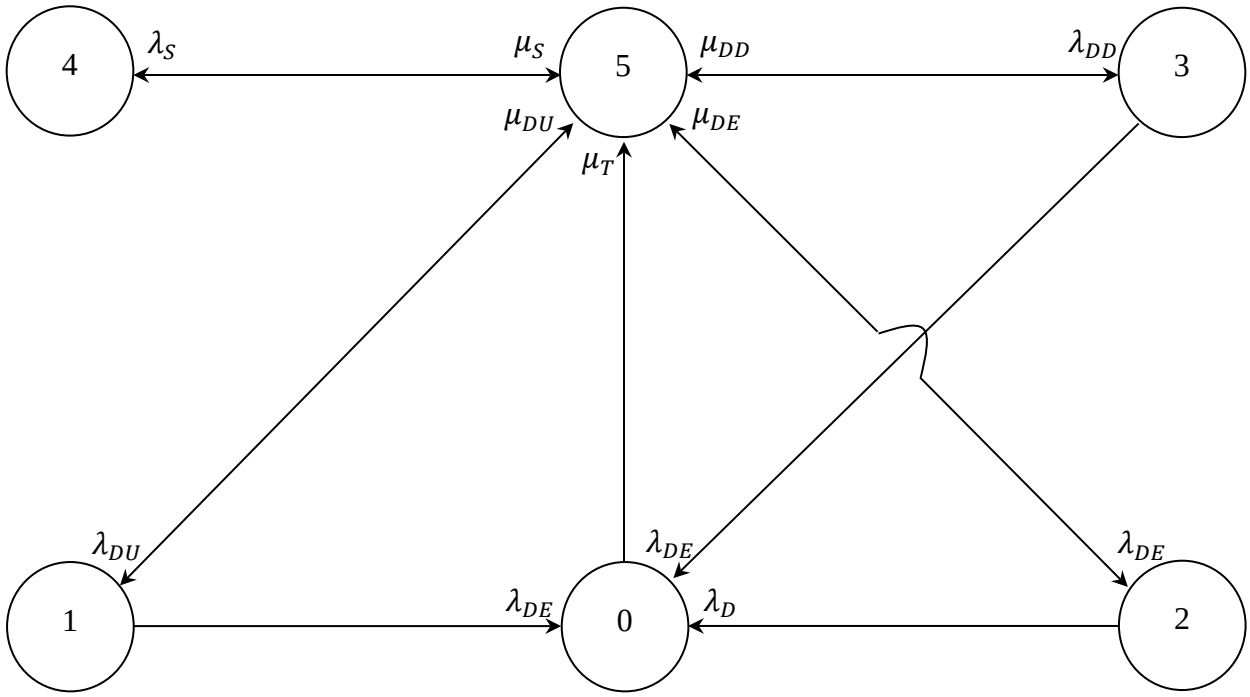

Figure 2 – State Transition Diagram for a 1oo1 SIS

In state 3, the SIS sustains a DD-failure while there is no process demand on the SIS. State 1 is similar to state 3, but the SIS has a DU-rather than a DD-failure. The system enters hazardous state 0 from state 2 when either of DD or DU failure occurs whilst the SIS is responding to a process demand in functional status. The hazardous event (state 0) represents a state where the

SIS endures a DU- or DD-failure and there is a demand for activation of the SIS. The corresponding states linked to hazardous event are 1 – 3.

A Pressure Relief Valve (PRV) is used as a simple safety system to examine the application of the above model. The primary dangerous failure mode for a PRV is “fail to open” on demand. Safe failure modes of PRV comprised of “spurious operation”, “fail to close” and “leakage in closed position”. Taking into consideration that the DD failure rate for a PRV is 0 in accordance with PDS Data Handbook [34], the state model diagram can be simplified as shown in Figure 3:

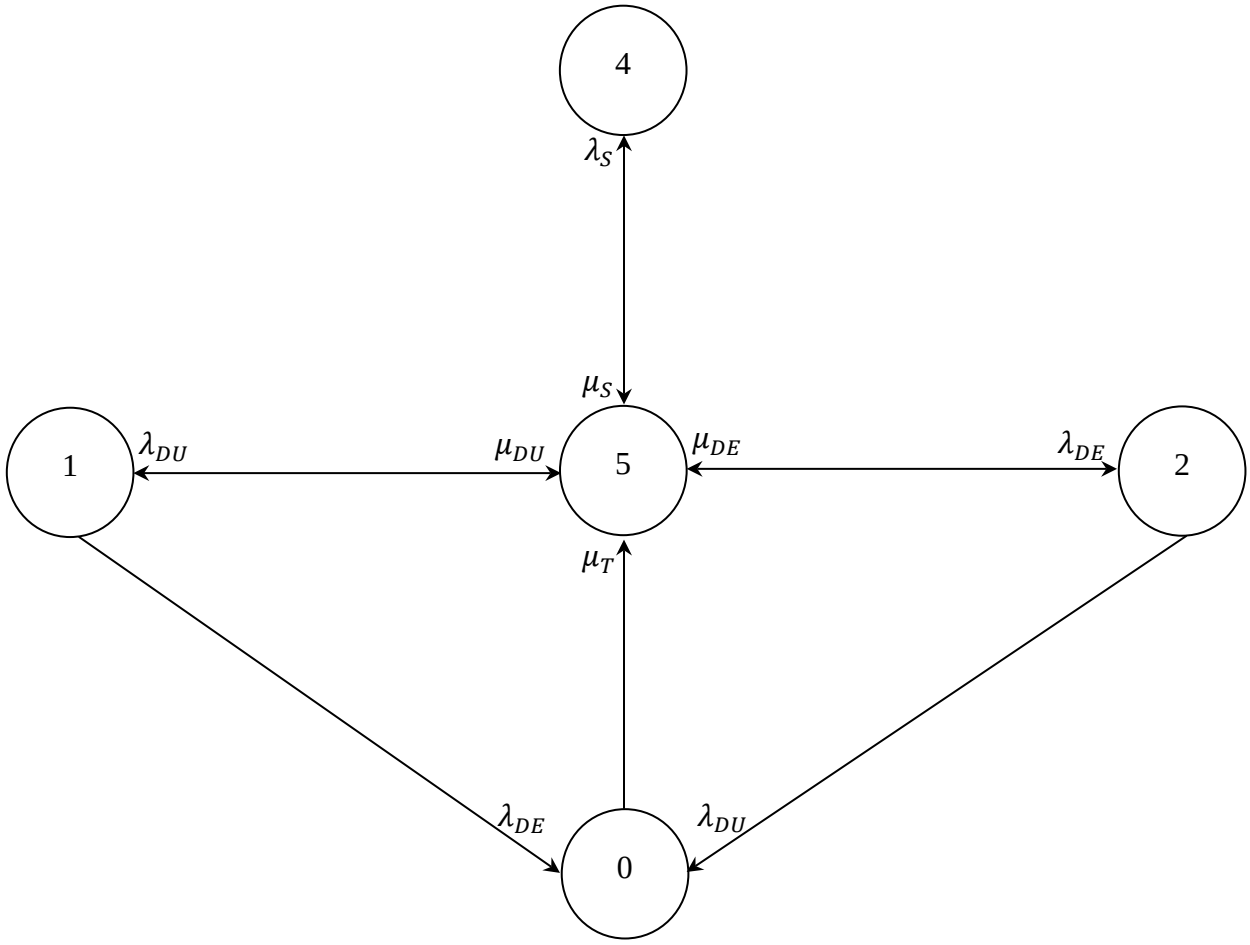

Figure 3 – State Transition Diagram for a 1oo1 PRV

The selection of PRV has resulted in model simplification due to the elimination of λ_{DD} and associated transitions from state 5 to 3 and state 3 to 0. This elimination leads to a reduction of Markov transition rate matrix and the associated computational efforts for numerical analysis of

the system. It should be noted that PRVs are in fact considered as mechanical devices and not classified as a SIS since the other two primary constituents of SIS including sensor / transmitter and logic solver elements of the system do not exist. However, considering PRV as the final element of a SIS, the Markov model that was originally developed for SIS can be simplified to represent the failures modes of mechanical devices such as a PRV. In other words, the 1oo1 PRV is an exceptional case of general 1oo1 SIS with process demand incorporated.

5.1.5 Performance indicators

The transition rate matrix of a 1oo1 PRV can be constructed from all transition rates as:

$$Q = \begin{bmatrix} q_{00} & \cdots & q_{05} \\ \vdots & \ddots & \vdots \\ q_{50} & \cdots & q_{55} \end{bmatrix} \tag{19}$$

The steady state equations [5] corresponding to the state transition diagram in Figure 3 can be obtained from:

$$\begin{aligned} (\lambda_{DE} + \mu_{DU})P_1 &= \lambda_{DU}P_5 \\ (\lambda_{DU} + \mu_{DE})P_2 &= \lambda_{DE}P_5 \\ \mu_T P_0 &= \lambda_{DE}P_1 + \lambda_{DU}P_2 \\ \mu_S P_4 &= \lambda_S P_5 \end{aligned} \tag{20}$$

Taking into account that the sum of steady state probabilities is equal to 1:

$$P_0 + P_1 + P_2 + P_4 + P_5 = 1 \tag{21}$$

The 1oo1 PRV system will not be able to respond to a process demand when it is in state 1, hence the PFD of the safety system is given by:

$$PFD = P_1 \tag{22}$$

The frequency (per hour) of entering into the hazardous state is equivalent to the visit frequency to state 0, from any other state as follows:

$$HEF = \lambda_{DE}P_1 + \lambda_{DU}P_2 \quad (23)$$

5.2 1oo2 Safety System

A typical architecture for safety systems is 1oo2 in which the system is able to provide the necessary safety function as long as at least one of the two components is operational. Inclusion of redundancy in design improves the reliability of the system when compared to simplex structures. However, this introduces a new risk in the form of CCF, which occurs when two or more components fail simultaneously due to a common stressor. Using the 1oo1 system as a platform, Liu et al. [35] introduced a Markov model for a 1oo2 pressure relief system excluding CCF. In this article we intend to introduce a new 1oo2 redundant PRV system by inclusion of CCF as well as incorporating process demand within the reliability model.

5.2.1 Assumptions

The general underlying assumptions listed in section 5.1.1 are all valid. In addition, the specific assumptions of this 1oo2 model are as follows:

- Repair of CCF is carried out for individual components (i.e. 2 stage repairs).
- CCF can occur even if one of the channels is in failed state (e.g. power interruption).

5.2.2 Definition of system states

Similar to the simple configuration, the 1oo2 safety system consists of the combined effect of the SIS states and process demand levied on the safety system. Consistent with the 1oo1 system, DD failures are excluded for modelling purpose since the DD failure rates, λ_{DD}, for PRV are annulled; subsequently μ_{DD} is omitted. The system transitions due to dangerous undetected as a result of failure, λ_{DU}, and associated repair, μ_{DU}, are intact. Similarly, the system transition rate due to safe failures (both detected and undetected), λ_S, and associated repair rate, μ_S, are identical to the 1oo1 system. Furthermore, the process demand and its reset rates as well as renewal rate for the 1oo1 system can be adopted for a 1oo2, assuming that the redundant system

can be used as a replacement of simple architecture in the same industrial application to enhance reliability. The system transition rates in a redundant safety system as outlined in Section 3.5 are λ_{DU}^{I} for independent failures and λ_{DU}^{C} for undetected CCFs where β_U represents an undetected CCF factor. Repair rate of DU failures, μ_{DU}, will suffice for the repair of CCFs as noted within the underlying assumptions of the model and no requirement for introduction of an additional repair rate is identified.

5.2.3 Testing strategies and Repair rates

Since the DD failures are not applied to the safety system under study, the diagnostic testing and subsequently DD repair rate, μ_{DD}, is not deemed as applicable. This means that only repairs of DU failures are required to be incorporated in the model. As discussed in Section 5.1.3 undetected failures can be revealed upon discharge of a process demand or by proof testing assuming perfect testing results in detection of unrevealed failures. Considering that the equivalent Mean Down Time (MDT) for an undetected failure of a 1oo2 redundant architecture is obtained from $MTTR + {\tau}/{3}$, the DU repair rate, μ_{DU}, for an undetected failure can therefore be calculated as [36]:

$$\mu_{DU} = \frac{1}{MDT} = \frac{1}{MTTR + {\tau}/{3}} \tag{24}$$

Since the repair of undetected CCF is assumed to be conducted in two stages as opposed to single stage repair, no further repair rate is considered in the model. It shall be noted that for single stage repair of undetected CCF, the system behaves like a single channel system and the mean down time element in Equation (18), MTTR $+ {\tau}/{2}$, is an adequate representation.

5.2.4 System Description

The possible states of the system are listed in Table 2. The nodes in Figure 4 correspond to the system states and arrows represent system transition from one state to another. Starting with system in fully functional status and no process demand (i.e. state 5), the safety system fails safely and transits from state 5 to 6 with a failure rate of $2\lambda_S$. This is a minimum of two

independent safe failures and includes safe detected and safe undetected which leads to four distinct failure rates in total (SD and SU failures for both components 1 and 2). The system will transit to state 6, whichever of those failures occurs earliest.

Table 2 – States of a 1oo2 SIS System

State	Property	Demand State
0	Hazardous	On Demand
1	2 DU	No Demand
2	2 Functional	On Demand
3	1 Functional, 1 DU	On Demand
4	1 Functional, 1 DU	No Demand
5	2 Functional	No Demand
6	Safe	N/A

Safe failure in this model is only considered for one component of the redundant system and safe failure of 2 components (sequential and/or concurrent) is not entailed within this reliability model. Hence, the system unavailability solely due to safe failures is not foreseen. Single DU or spurious activation does not impact system ability to respond to a process demand and hence has no impact on its availability. In this case safety system is defined as in "functioning" state. In state 2, the safety system is responding to a process demand when both components are functional. Upon fulfilment of the process demand the system transits back to the original state 5. The transition rate from state 2 to 3 and state 5 to 4 is $2(1-\beta_U)\lambda_{DU}$, which is the minimum of two independent DU failures. This failure rate excludes the dangerous undetected CCFs since any of the components can fail independently. In state 3, the safety system is responding to a process demand with only one component functioning whereas in state 4 no demand is levied on the system. The safety system alternates between states 3 and 4 depending on manifestation of a process demand or removal of the demand when it ends. Upon identification of the failed component during proof test and its repair in any of the states 3 or 4 with μ_{DU} repair rate, the system transits to the previous states, 2 and 5 respectively.

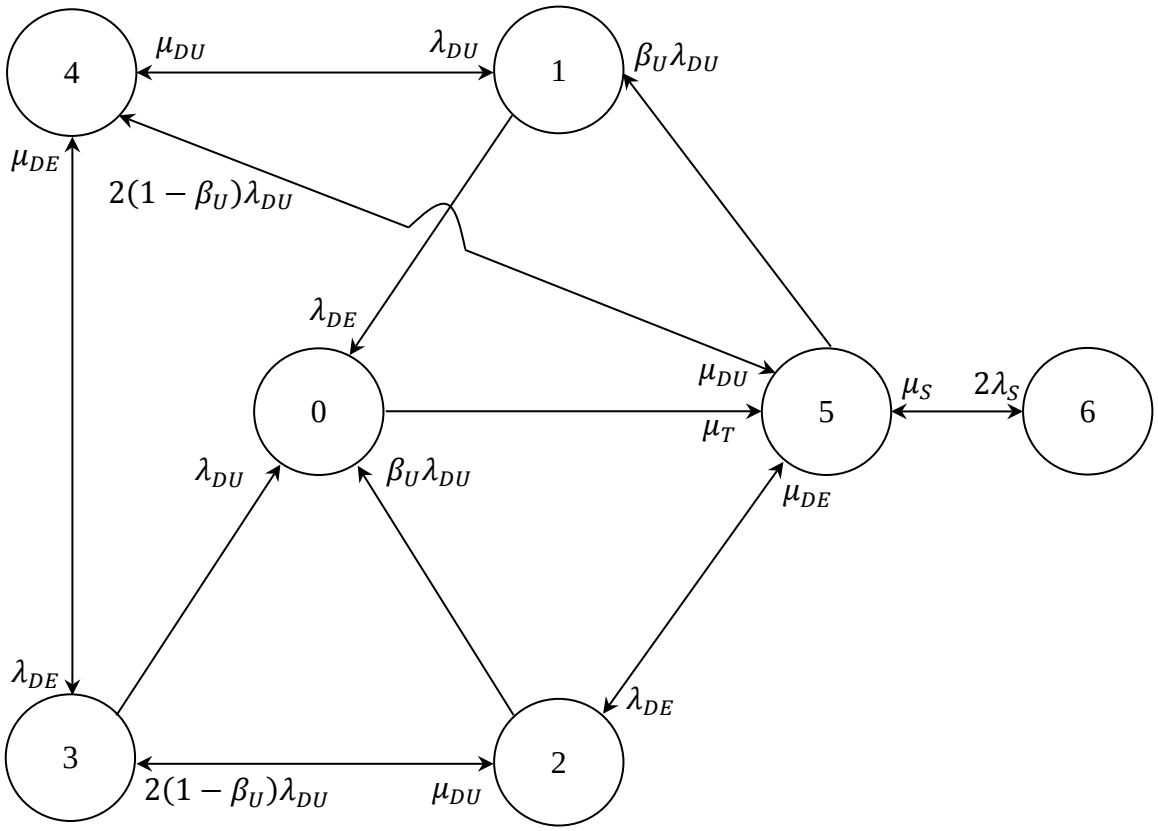

Figure 4 – State Transition Diagram for a 1oo2 System

The CCF failure can occur on 4 separate occasions, one when system is fully functional and there is no demand resulting in system transition from state 5 to state 1 with $\beta_U\lambda_{DU}$ failure rate. The CCF can also arise when system is responding to a process demand in state 2 leading to a system transition to the hazardous state 0 with the same failure rate. It is necessary to highlight that the abovementioned scenarios involve CCF only and do not entail independent failures. It is assumed that repair of CCFs are carried out in two consecutive stages for individual components, resulting in transition from state 1 to state 4 and then to state 5. No single stage repair for CCF is considered in this model and therefore no transition between state 1 and state 5 exists. Additionally, CCF may take place when one of the components is in failed status whilst the other component is functional. The transition from state 3 to 0 (on demand) or state 4 to 1 (no demand) occurs with failure rate λ_{DU} which takes both independent and CCF failures into account. Example of this scenario is excessive vibration of process pipework causing the remaining

functional pressure transmitter to fail whilst the other pressure transmitter already failed due to a separate cause.

The system enters hazardous states 0 from state 1 when a process demand occurs with λ_{DE} rate whilst both components are in failed states either due to a CCF (5-1), two sequential undetected failures, or a combination of DU and CCF (5-4-1). Alternatively the hazardous state 0 is reached from state 3 where system is responding to a process demand with the only remaining functional component (5-2-3) and it fails undetected dangerously, either due to single DU or CCF, resulting in removal of the protection layer and exposure to a hazardous event. Appearance of a CCF when system is responding to a process demand in state 2 leads to a hazardous state 0. When the system enters the hazardous state 0, a restoration action is initiated. Upon completion of the restoration with mean time $1/\mu_T$, the system is started up again in an "as good as new condition" in state 5. This can only be accomplished where the hazardous event is either repeatable or renewable in accordance with the classification identified by Youshiamura [17].

5.2.5 Performance indicators

The 1oo2 PRV system is a Markov process since the future status of the system depends on the current status, regardless of past circumstances of the system. Furthermore, the system fulfils the Markov property with stationary transition probabilities, such that the steady state probabilities $(P_i, i = 0, \dots, 6)$ can be determined from the transition rate matrix. The steady state equations corresponding to the Markov transition diagram are as follows:

$$
\begin{aligned}
&(\lambda_{DE} + \lambda_{DU} + \mu_{DU})P_4 = \mu_{DU}P_1 + 2(1-\beta_U)\lambda_{DU}P_5 + \mu_{DE}P_3 \\
&(\mu_{DU} + \mu_{DE} + \lambda_{DU})P_3 = 2(1-\beta_U)\lambda_{DU}P_2 + \lambda_{DE}P_4 \\
&(\mu_{DE} + 2 - \beta_U\lambda_{DU})P_2 = \mu_{DU}P_3 + \lambda_{DE}P_5 \\
&(\mu_{DU} + \lambda_{DE})P_1 = \lambda_{DU}(P_4 + \beta_U P_5) \\
&\mu_T P_0 = \lambda_{DE}P_1 + \lambda_{DU}(P_3 + \beta_U P_2) \\
&\mu_S P_6 = 2\lambda_S P_5
\end{aligned}
\qquad (25)
$$

Taking cognisance that the summation of steady state probabilities is unity:

$$\sum_{i=0}^{6} P_i = 1 \tag{26}$$

Similar to the 1oo1, the 1oo2 PRV system will not be able to respond to a process demand when it is in state 1, hence the PFD of the safety system is given by:

$$PFD = P_1 \tag{27}$$

The frequency (per hour) of entering into the hazardous state that corresponds to the visit frequency to state 0, from all possible states is:

$$HEF = \lambda_{DE} P_1 + \beta_U \lambda_{DU} P_2 + \lambda_{DU} P_3 \tag{28}$$

6.0 Numerical Analysis

We dedicate this section to demonstrate the application of proposed approach to compute the unavailability of pressure protection system and the frequency at which the system enters hazardous conditions. A basic example of a process system [37] is considered where the performance of a 1oo1 PRV is studied and compared with the proposed 1oo2 PRV redundant architecture.

6.1 Application - Study of Pressure Protection System

Consider a basic process system that consists of a pressure vessel containing volatile flammable liquid hydrocarbon. A simplified Piping & Instrumentation Diagram (P&ID) of the pressure vessel and associated safety systems for pressure protection are shown in Figure 5. The vessel acts as an intermediate liquid storage unit for downstream system to allow sufficient time for processing hydrocarbons. It is assumed that no further liquid processing is conducted within the pressure vessel during the liquid retention time i.e. no separation, heating or cooling effect, hence the fluid properties including primary constituents, temperature, flash point etc are intact. Control of the process fluid is handled through a Basic Process Control System (BPCS) that monitors the signal from the Level Transmitter (LT) and controls the operation of the Level

Control Valve (LCV). The ratio of the vessel liquid inflow is greater than its discharge line and as such the healthy operation of the BPCS is vital to maintain the integrity of the operations. In addition to the BPCS, a High Pressure Alarm (PAH) and a Pressure Relief Valve (PRV) are incorporated within the design as additional independent protection layers.

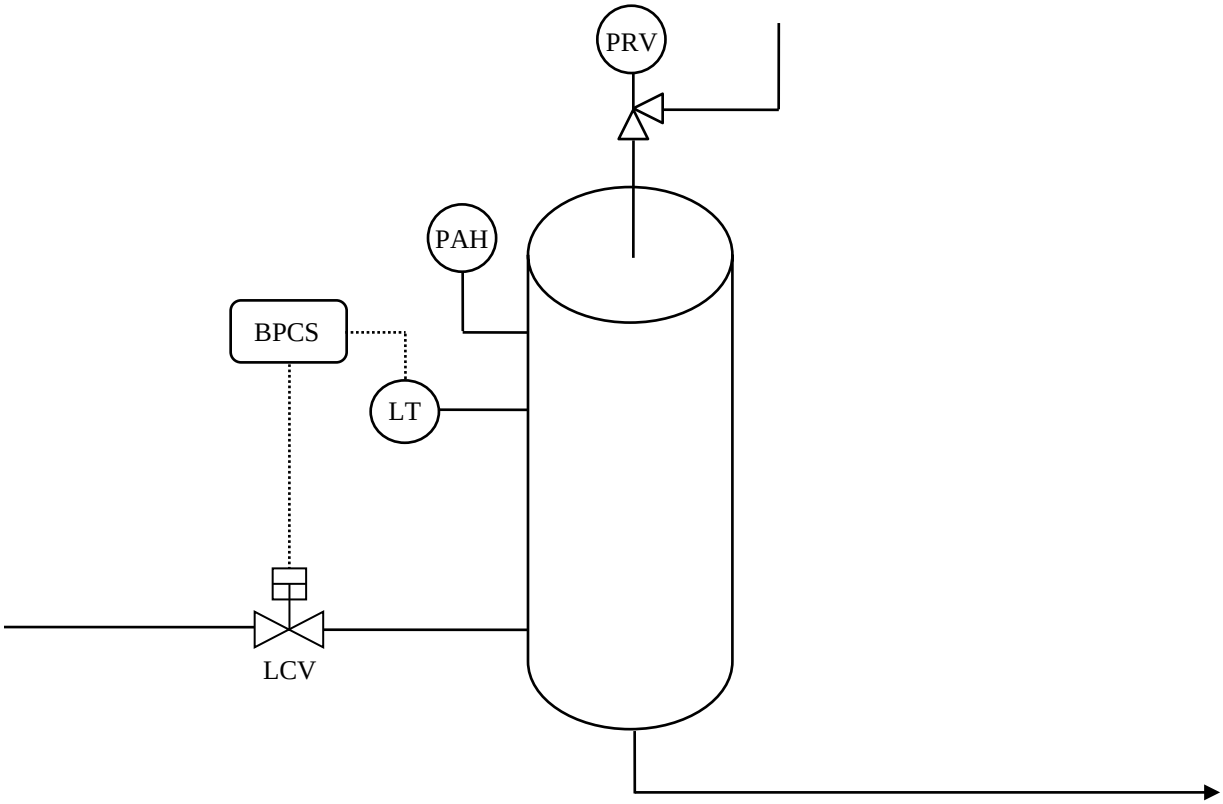

Figure 5 – Pressurised Vessel & Safety Systems

6.1.1 Hazardous scenario

The liquid level within the vessel will rise beyond its operating limit if BPCS fails. Failure of the BPCS could be either due to any of the following or a combination of these:

- Failure of the LT in detection of the level;
- The control system failure in processing the signal;
- Failure of LCV or its actuator resulting in valve seizure in open position.

Upon failure of BPCS and rise of the liquid level within the vessel, the PAH alerts the operator to undertake an appropriate remedial action e.g. shutdown the process system and stop the incoming flow. Where the PAH fails to initiate or the operator fails to respond to the alarm, a pressure relief valve releases the material to the flare system to prevent over pressurisation of the vessel. It is assumed that the flare system is suitably designed to handle excessive liquid and an automatic action will be initiated by a robust liquid control system in the flare knock out drum to restore the process to the original status within its operating limits. This hazardous condition is envisaged as a repeatable hazard.

However, failure of the pressure relief valve (i.e. fails to open) as the last protection layer, whilst the liquid level is rising within the vessel and no manual intervention is undertaken, will result in over pressurisation of the vessel and ultimately pipework / vessel rupture leading to loss of containment. It is assumed that upon loss of containment the Fire & Gas (F&G) system will initiate an executive action to shutdown the process system and prevent further liquid inflow. The vessel is equipped with a bund which is suitably sized for a full rupture and hence can remove flammable liquid upon release to reduce personnel exposure to hazardous material. In addition, the process shutdown and isolation of all potential energy sources will prevent further escalation of hazardous event if ignited i.e. fire / explosion risk. This is considered as a renewable hazard and the system can be restored to the original status upon repair of the vessel / associated pipework. Where the vapour release finds an ignition source in the absence of F&G initiation (e.g. failure or delay in detection of the flammable atmosphere in a timely manner) it results in fire or explosion event. The fire scenarios envisaged are pool fire as a result of vessel rupture and substantial sudden loss of containment, or spray fire from high pressure release due to flange / pipework leakage. The consequence of release may be an explosion for offshore installations (or flash fire for onshore assets) in the case of a delayed ignition with potential for generating high overpressure magnitude depending on the level of confinement and congestion of the area. Where fire or explosion occurs, it is considered as a non-renewable fatal hazardous event and hence is outwith the underlying assumptions of the proposed Markov model in this article.

6.1.2 Consequence evaluation

There are no safety and environmental consequences for repeatable hazard (i.e. PRV activation) since the flare system including knock out drum is suitably designed for handling excessive liquid upon PRV activation. In this case the hazardous material is contained with the hydrocarbon system and no loss of containment is expected. The consequence in this case is limited to loss of production and cost associated with restoration of the system including start-up. The consequence associated with renewable hazard (i.e. unignited events) is more serious due to loss of containment. However, initiation of F&G system results in process system shutdown and isolation of all electrical sources including activation of platform public alarm and start of evacuation process hence, fatality is discounted. Environmental consequence is also insignificant due to provision of bund and closed drain system sized for handling liquid removals.

The consequence of non-renewable hazards (i.e. ignited events) resulting in fire / explosion is significant with multiple fatalities and hence considered as typical safety outcome of these events. Environmental consequences for non-renewable hazardous event consist of discernible degradation in quality, availability or biodiversity of habitats within the protected sites and the viability of species on a widespread scale, emissions at levels well above industry norms and recovery following cessation of casual activity. Commercial considerations include long term unavailability of plant, loss of production for significant period of time, reputational damage, substantial liability costs, and non-compliance with legislation or consents with possible criminal or civil penalties in addition to the cost of plant restoration. Detrimental impacts on the prosperity or wellbeing of communities or groups of people are also foreseen for onshore assets.

6.2 Quantification of Process Demand

The results of the HAZOP study [37] identified that an overpressure condition due to failure of the control system could result in a release of the flammable material to the environment. This is one of the initiating events that could propagate into a hazardous event. Other initiating events that could lead to a loss of containment such as exposure of the pressure vessel to external fire leading to Boiling Liquid Expanding Vapour Explosion (BLEVE) are excluded from this

analysis. For this illustrative example, the overpressure condition due to failure of control system will only be examined.

6.2.1 Human Error Analysis

The likelihood of human error is estimated in this paper using the Human Error Assessment & Reduction Technique (HEART) method [38] introduced in 1985. This technique was developed to provide an easily understood and quick method that would highlight the major influences on human performance and predict the likelihood of human error. HEART is a widely used methodology that is based upon human performance literature and assumes that basic human reliability is dependent on the generic nature of the task being undertaken.

This technique defines a set of generic tasks that are classified according to the intrinsic nature of the task and assigns a nominal probability of failure for each type of generic task. The human error probability associated with each generic task can be used to give an indication of the likelihood of human error given "ideal" conditions. However, "ideal" conditions do not always exist and as such it is assumed that the predicted level of human reliability will degrade subject to the extent to which certain error-producing conditions apply. A list of generic tasks and typical error-producing conditions are available in [38]. The steps required to calculate the likelihood of human error when undertaking the task are to select an appropriate generic task, identifying any relevant error-producing conditions and assessing the effect that the relevant error producing conditions have on the likelihood of an error. Using this information the predicted human error probability can be calculated by:

Likelihood of human error = Nominal Human Unreliability x Error-Producing Condition (29)

The generic task for the PRV example is considered as “restore or shift a system to original or new state following procedures, with some checking” with nominal human unreliability of 0.003 and an error producing condition of “a mismatch between perceived and real risk” corresponding to a factor of 4 [38]. Thus, the likelihood of operator failing to respond to the alarm is estimated as 1.2×10^{-2}.

6.2.2 Process demand frequency

In this section we analyse the frequency of process demand since concurrent failure of more than one mechanism will result in demand imposition on the PRV. The process demand on PRV is generated from BPCS failure AND failure of manual control. The failure of BPCS is derived from failure of any element including transmitter, hardwire controller and final element. The failure of manual control itself can be due to operator's failure to respond OR failure of PAH. According to the PDS reliability data handbook [34] the frequency of a BPCS loop failure consists of 3 elements. These elements are failure of LT, $\lambda_{DU} = 0.6 \times 10^{-6}$ per hour, failure of a hardwire logic controller (analogue input, 1oo1 logic and digital output), $\lambda_{DU} = 0.1 \times 10^{-6}$ per hour, and failure of LCV, $\lambda_{DU} = 2.2 \times 10^{-6}$ per hour (frequently operated). The PFD value for the PAH failure is obtained 1.3×10^{-3} assuming that the PAH is operating in a clean medium with no potential for clogging of sensing line and considering test intervals of 8,760h. By modelling the failure mechanisms using CARA FAULT TREE (Figure 6), the process demand frequency is calculated as $\lambda_{DE} = 3.86 \times 10^{-8}$ per hour.

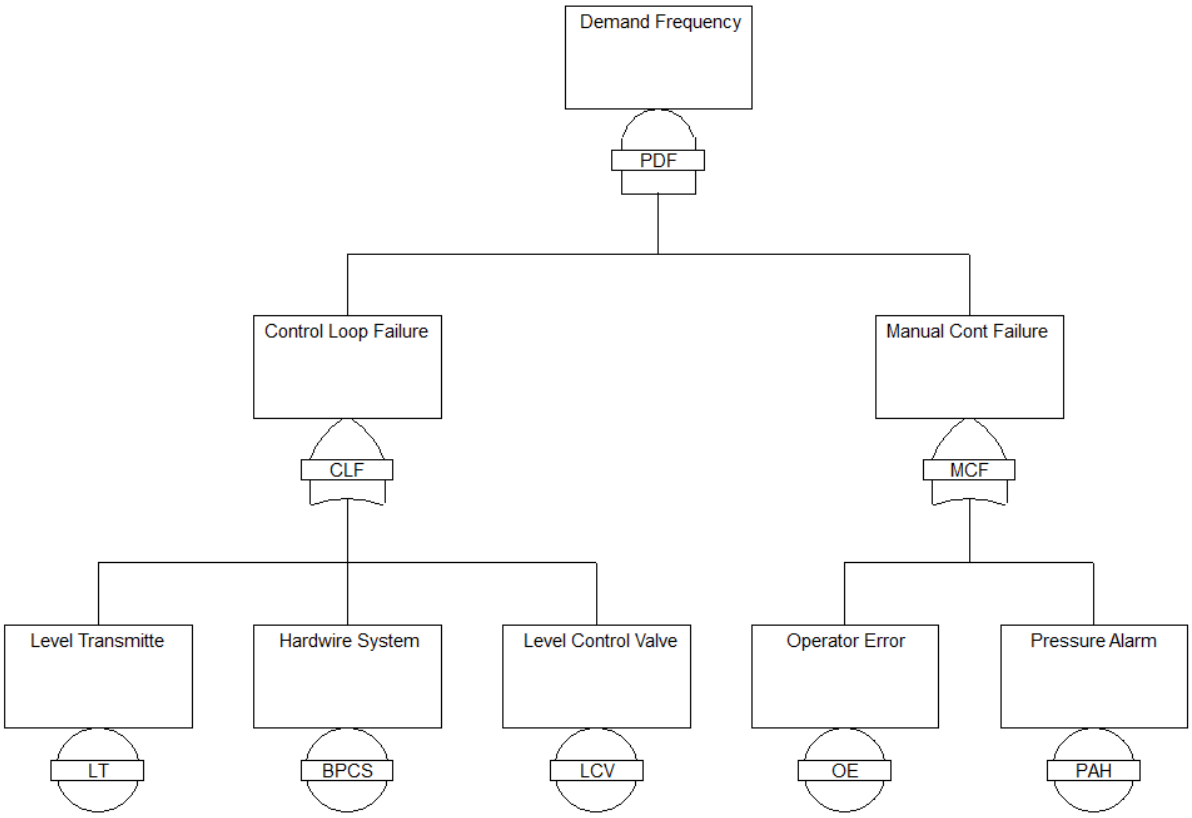

Figure 6 – Process Demand Frequency Fault Tree

6.3 Numerical analysis of 1oo1 system

The PDS handbook provides the following additional estimates for the failures rates: $\lambda_{DD} = 0$, $\lambda_D = \lambda_{DU} = 2.2 \times 10^{-6}$ per hour and $\lambda_S = 1.1 \times 10^{-6}$ per hour. In addition, we set $\mu_S = 1 \times 10^{-1}$ per hour, meaning that the mean repair time of a safe failure is 10h. The interval between proof tests is assumed to be one year or $\tau = 8{,}760$h. These estimates are uncertain and will obviously be strongly dependent on the particular maintenance arrangements. The restoration rate from hazardous event is also estimated as $\mu_T = 1 \times 10^{-3}$ per hour [16]. This means that the mean restoration time after a hazardous state (or accident) is set to 1000h. As we are addressing only repeatable and/or renewable hazardous event, this estimate is deemed as suitable however the extent of the damage dominates this value.

The MTTR value is set at 8 hours, consistent with the IEC 61508 [1] default value. Using $\tau = 8{,}760$h and $MTTR = 8$h the repair rate of dangerous undetected is calculated as $\mu_{DU} = 2.28 \times 10^{-4}$ per hour, as per Equation (18). The process hazard rate and its duration are considered as $\lambda_{DE} = 3.86 \times 10^{-8}$ and $\mu_{DE} = 1 \times 10^{-4}$ per hour respectively. The state equations were solved for 1oo1 model by using MATLAB to obtain the HEF and PFD as a function of λ_{DE}. The PFD is calculated as 9.55×10^{-3} corresponding to the upper boundary of SIL 2 requirements for 1oo1 PRV. The integrity level can be reduced by an order of magnitude via incorporation of additional layer of protection e.g. trip function on liquid inflow on high level. While designing a system to implement the required function, it is proposed to aim and engineer the SIS's performance to lie in the middle of that IL range. The PFD for each SIS corresponding to its integrity level is identified in IEC 61508 [1]. The HEF is calculated as 1.19×10^{-9}, indicating a very low likelihood of hazardous event occurrence.

6.4 Numerical analysis of 1oo2 system

The 1oo2 PRV consists of 2 relief valves that can respond to a process demand upon imposition i.e. concurrent failure of the control loop and manual control. The configuration of considered 1oo2 PRV system is illustrated in Figure 7. During normal operations (i.e. no process demand) the PRVs remain in closed position as the vessel's pressure is lower than the set pressure of relief valves. The PRVs lift to release excessive liquid into the flare system only when process demand

occurs. The valves are independent and individually sized for full liquid release meaning that only one PRV is sufficient to respond to the overpressure scenario. Failure of one of the PRVs will not affect the availability of the pressure relief capability due to redundancy incorporated within the design and hence the system is operational as long as one PRV is functional. The system enters the hazardous situation only if both PRVs are in failed status and a process demand occurs.

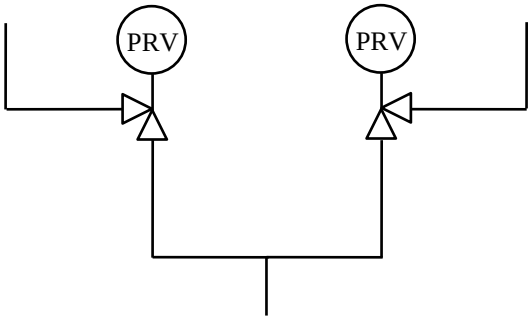

Figure 7 – 1oo2 PRV

As shown in Figure 7 the PRVs are connected to the vessel via a common header. For liquid services there is a possibility of blockage in the header which results in common cause failure of the PRVs. Other underlying factors leading to CCF include but not limited to incorrect selection of material for corrosive environment e.g. offshore, incorrect fabrication / installation methods, human error in maintenance / calibration / testing etc. In this paper the latter underlying factors of CCFs are studied in which the CCF can be rectified in two stages by repair of individual components in succession. Using $\tau = 8{,}760$h and $MTTR = 8$h the repair rate of dangerous undetected is calculated as $\mu_{DU} = 3.42 \times 10^{-4}$ per hour as per Equation (24). An approximate value for Beta factor $\beta_U = 0.1$ is also used in accordance with IEC 61508 [1] for final elements in the 1oo2 redundant architecture. The state equations were solved by MATLAB for 1oo2 model to obtain the PFD and HEF as a function of λ_{DE} using the failure and repair rates identical to the 1oo1 system.

The PFD for 1oo2 PRV is calculated as 7.13×10^{-4} which corresponds to the SIL 3 range indicating a more reliable system in comparison with a single PRV case. The redundant PRV system enters hazardous event with a frequency value of 2.98×10^{-11}, a lower probability when

compared to the 1oo1 system, resulting in improving safety performance of the system. This is also an advantage of utilising a redundant configuration as opposed to a single relief pressure protection system with no redundancy. These findings are consistent with the general philosophy that utilising a redundant architecture will enhance the reliability and safety performance of the system.

A query may arise whether utilising a PRV in conjunction with a rupture disk could also provide a suitable level of redundancy with lower capital expenditure. Although rupture disks are more cost efficient in comparison with additional redundant PRV, they have their own limitations. Rupture disks may only be replaced after activation and cannot be maintained, tested, calibrated and recertified (in contrast to PRVs) during their lifetime when in operation. Furthermore, spurious activation of a rupture disk may result in relatively significant commercial loss including immediate production loss, and loss of revenue due to shutdown period for replacement of the rupture disk. On the other hand spurious activation of a PRV in a 1oo2 configuration will result in production loss only, since PRVs can be isolated and reset accordingly with no requirement for production shutdown. Various parameters shall be taken into account for selection of a suitable device including but not limited to capital and operational expenditure, maintenance requirements, reliability, design conditions etc. However, this was beyond the scope of this paper and as such was not explored further. On this basis an assumption was made that a 1oo1 simple PRV system can be replaced with the 1oo2 PRV configurations in the same industrial application to enhance reliability.

6.5 Sensitivity Analysis

6.5.1 PFD and HEF Comparison for 1oo1 vs 1oo2 Systems

An analysis is conducted in this section to compare the reliability of 1oo1 system versus 1oo2 system. The models were developed in MATLAB with the parameter values outlined in Sections 6.2 and 6.3 taking into account variation in CCF rate (β_U) between 0.01 and 0.2 as per the IEC 61508 recommended range for redundant systems. The system performance indicators (PFD & HEF) are utilised in this analysis to compare the performance of two models and the results are presented in Figure 8 & Figure 9. The PFD of 1oo2 system is an order of magnitude lower than

1oo1 system as illustrated in Figure 8 indicating a significant improvement in reliability of the system. The PFD for 1oo2 PRV system increases as β_U acquires higher values, however the increase in PFD is negligible in the region of 10^{-3}.

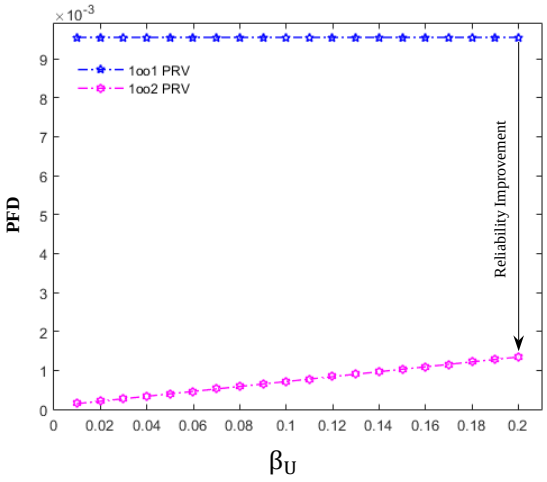

Figure 8 – PFD comparison of 1oo1 vs 1oo2 PRV system with varying β_U value

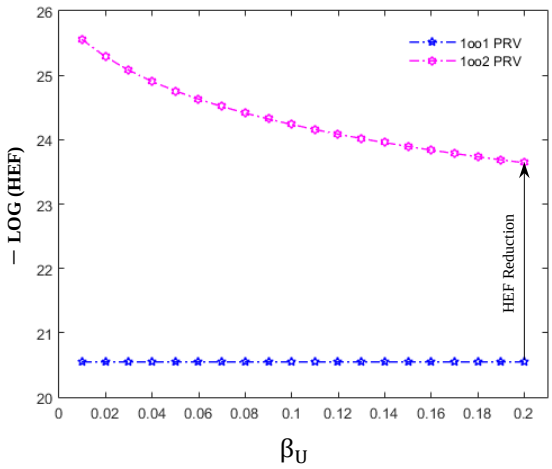

Figure 9 – HEF comparison of 1oo1 PRV vs 1oo2 PRV system with varying β_U value

The trends of HEF for both systems are shown in Figure 9. It can be observed that whilst the frequency of hazardous event for 1oo1 system is constant against the variation in β_U values, the frequency for 1oo2 increases due to increase in the CCF factor. Comparing the two HEFs clearly illustrates a significant reduction in the frequency of system entering the hazardous states. Despite an increase in HEF for 1oo2 system as the β_U factor obtains higher values, the HEF is substantially lower than the 1oo1 system. It shall be noted that the HEF comparison is illustrated in a negative logarithmic scale and hence reduction in HEF results in acquisition of higher values on y-axis. The abovementioned observations for PFD and HEF are consistent with the overall expectations for 1oo1 system versus 1oo2 redundant structures as it is generally accepted that any increase in redundancy will result in enhancing system reliability and reducing exposure of the process system to hazardous event.

6.5.2 The effect of λ_{DE} and μ_{DE} on the reliability of 1oo2 System

We now study the effect of varying the process system parameters including the demand rate, λ_{DE}, and demand duration, μ_{DE} against change in β_U. The effect of varying λ_{DE} on the PFD and

HEF are evaluated for β_U in the range of 0.01 - 0.2. The assessment was conducted for demand rates equal to 10^{-9}, 10^{-5}, 10^{-4}, 10^{-3} and 10^{-2} respectively. In order to illustrate the visit frequency to hazardous event we use $-\log_{10}$ scale on the y-axis. As seen in Figure 10 and Figure 11 the HEF and PFD are functions of λ_{DE} for the specified β_U values.

Increase in process demand means shifting from low demand mode of operations to high demand mode where safety system has to respond more frequently to demands from the process system. Although the model developed in this paper is solely focused on low demand mode of operation, the increase in process demand is studied in this section to analyse the behaviour of the system in those scenarios. From Figure 10 the PFD ascends as the CCF rises for various λ_{DE}, however for more frequent process demands, the PFD rises with lower slope and hence loses sensitivity gradually to any increase in β_U.

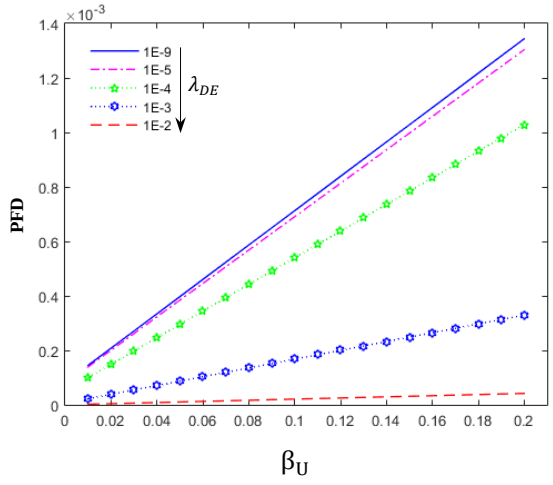

Figure 10 – PFD verses β_U with varying demand rates for a 1oo2 PRV system

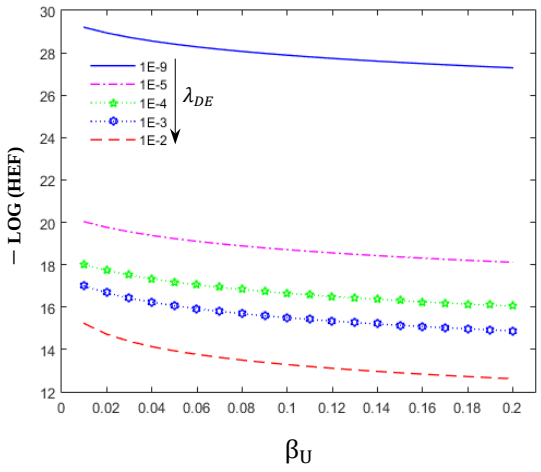

Figure 11 – HEF verses β_U with varying demand rates for a 1oo2 PRV system

The variation in PFD values can be explained by reviewing the system state diagram in Figure 4. As the PFD is equivalent to the probability of system at state 1, any variation in PFD value means increase or decrease in the probability of system being in this state. When the demand frequency increases, the system will spend a higher proportion of time in states 2, 3 and 4 and less in state 1, resulting in reducing the probability of system transition to state 1 and the PFD value. The frequency of entering the hazardous state increases when the demand rate increases for a 1oo2 system as shown in Figure 11. This was predicted since the system is responding more

often to process demand and component failures during this period will affect the system capabilities. The curves for the different demand rates have a similar form, but increase with different rates as the CCF rate increases. The outcome of this sensitivity investigation is consistent with the observations of Liu et al. [16] for the selected values of λ_{DE} in a 1oo2 PRV system as the PFD decreases with demand rate. Moreover, the HEF for 1oo2 PRV system exhibits a similar trend to the observations recorded by Liu et al. [16] as the frequency of entering the hazardous state increases when the demand rate increases for a low demand system.

The effect of varying μ_{DE} on the PFD and HEF is also evaluated for β_U in the similar range of 0.01 - 0.2. The assessment was conducted for demand duration, μ_{DE}, equal to 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2} and 10^{-1} respectively. No disparity in the PFD trend for various demand durations is illustrated in Figure 12 although an increase in PFD value is observed whilst the CCF rate is on the rise. This sensitivity analysis shows that the model is more sensitive to change in CCF rate as opposed to the duration of the demand. The PFD increases more than 7 times from the initial β_U value of 0.01 indicating that the 1oo2 system is susceptible to increase in CCF rate as anticipated.

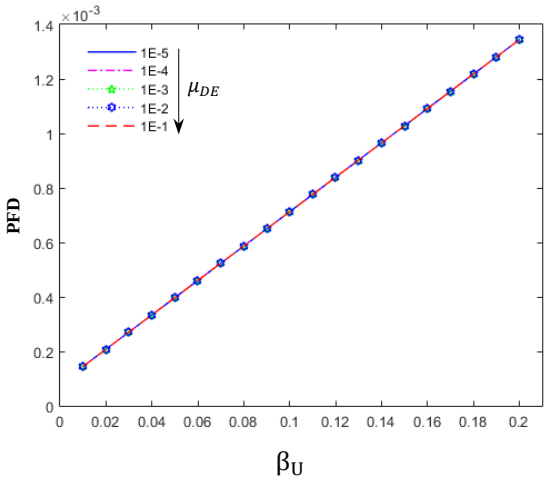

Figure 12 – PFD verses β_U with varying demand durations for a 1oo2 PRV system

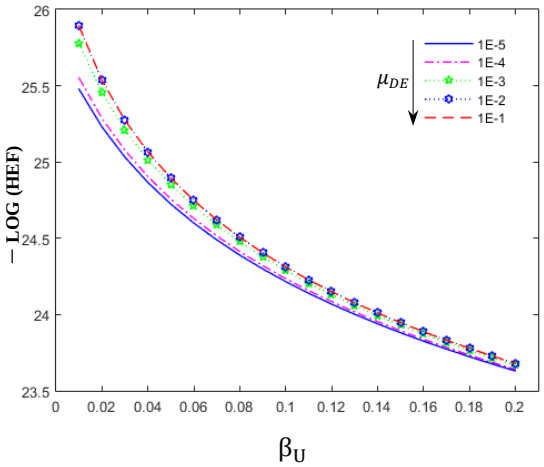

Figure 13 – HEF verses β_U with varying demand durations for a 1oo2 PRV system

For the system under study the demand duration will last for a short duration since the flare system is provided with a level control system that shuts down the process system upon detection of high level alarm in the flare knock out drum, therefore, 10^{-4} is a suitable representative. The

system visits the hazardous states more frequently as demonstrated in Figure 13 when β_U increases. No significant change in system behaviour is identified for various μ_{DE} values. In this assessment all other parameters including demand rate are considered to be constant. The result of the sensitivity analysis for selected values of μ_{DE} is in line with the findings of Liu et al. in [16] for a 1oo2 PRV system, in which the PFD is identified as independent of the demand duration and HEF increases with the demand duration for systems operating in low demand mode.

6.5.3 The Effect of λ_{DU} and μ_{DU} on the reliability of 1oo2 System

For completion of the sensitivity analysis the effect of varying the component failure rates, λ_{DU}, and repair rates, μ_{DU} against changes in β_U are also studied in this paper. Similar to the process system demand sensitivity analysis, the effect of varying λ_{DU} on the PFD and HEF is evaluated for β_U in the range of 0.01 - 0.2. The assessment was carried out for failure rates equal to 10^{-7}, 10^{-5}, 10^{-4}, 10^{-3} and 10^{-2} respectively. Where the component failure rate increases, the system will be less available to respond to process demand and this is reflected in Figure 14. A gradual increase in PFD can be witnessed when λ_{DU} is varying between 10^{-7} and 10^{-4} with a substantial rapid rise to around 1 when λ_{DU} is equivalent to 10^{-2}.

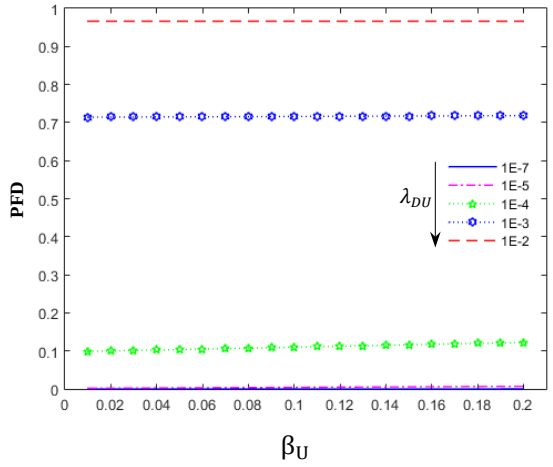

Figure 14 – PFD verses β_U with different failure rates for a 1oo2 PRV system

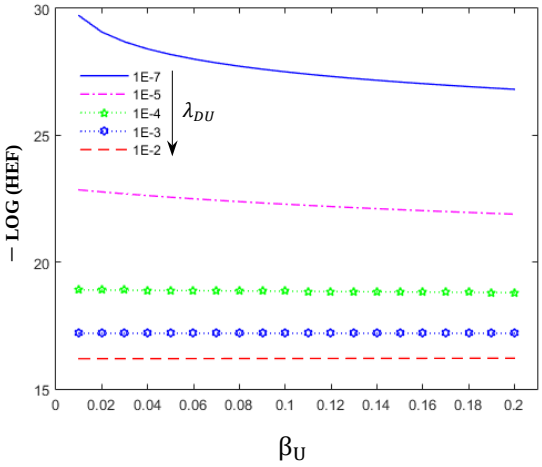

Figure 15 – HEF verses β_U with different failure Rates for a 1oo2 PRV system

This behaviour is also observed in the system entering hazardous scenario in Figure 15. As shown the exposure to hazardous event increases since the system components fail more frequently, impacting system availability to respond to process demand. It is also noted that increase in CCF rate will influence the HEF for a component failure rate of 10^{-7}, however remains constant for higher values of λ_{DU}. This is due to the dominant impact of component failure rates that neutralise any change in β_U values.

The effect of varying μ_{DU} on the PFD and HEF is also reviewed for β_U in the range of 0.01 - 0.2 for repair rates equal to 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2} and 10^{-1} respectively. Increase in repair rate is deemed as an improvement in system performance since higher repair rate leads to enhanced system availability and Figure 16 demonstrates this effect. It can be seen that the PFD decreases when repair rate increases. The decrease in PFD is significant when μ_{DU} increases from 10^{-5} to 10^{-4} and minimal change is observed for repair rates between 10^{-3} to 10^{-1}. The impact of β_U is realised for $\mu_{DU} = 10^{-5}$ but weakens for other values of μ_{DU}. The HEF figures obtained for different μ_{DU} values shown in Figure 17 is an emphasis of the abovementioned fact. Due to the enhanced repair rate, the system is less exposed to hazardous scenario hence reduction in HEF can be seen in this figure. Contrary to failure rate figure, the impact of β_U is more obvious as μ_{DU} increases whilst no notable change in HEF between 10^{-2} and 10^{-1} is identified.

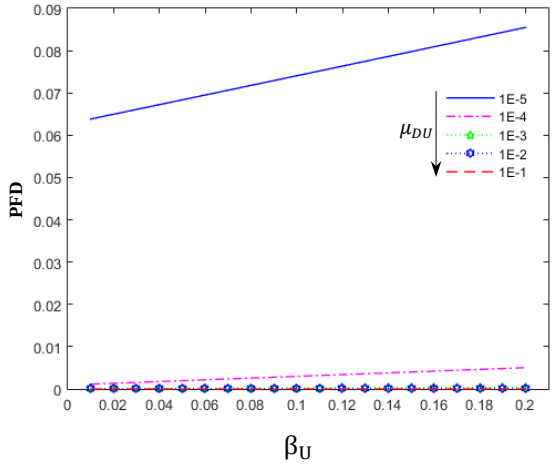

Figure 16 – PFD verses β_U with different repair rates for a 1oo2 PRV system

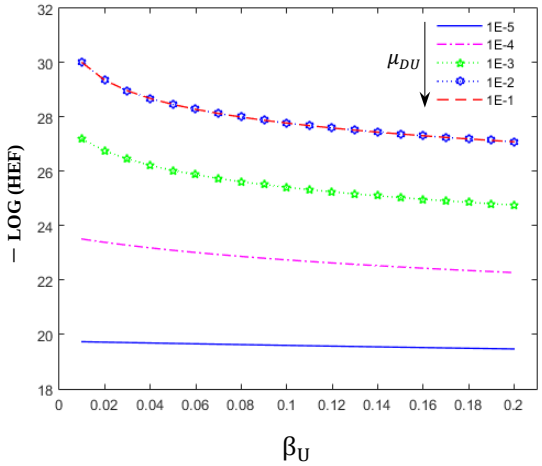

Figure 17 – HEF verses β_U with different repair rates for a 1oo2 PRV system

7.0 Conclusions

This paper has presented a new reliability model for a redundant safety system using Markov analysis approach. The main objective of this article was to develop a new model for a 1oo2 safety system for low demand mode of operation based on an established simple 1oo1 configuration. This model incorporates process demand imposed on the safety system in conjunction with CCF and established system failure modes such as dangerous undetected failure rate. The model is predominantly applicable to those safety systems without automatic diagnostics where the component dangerous detected failure mode is annulled. Two reliability measures have been utilised namely the Probability of Failure on Demand (PFD) and the Hazardous Event Frequency (HEF) to measure the reliability and safety performance of the model.

The model presented in this paper is an improvement to the Markov model previously outlined by Liu et al. [16] by incorporation of CCF however, this model assumes no single stage repair of CCFs. In the case where two components are in failed status due to CCF, the repair can only be carried out for individual components in two stages in succession. Although this assumption limits the application of the model proposed in this paper, it is considered as the normal modelling practice for repair of failed components in the industry.

The validity of the model introduced in this research was examined in a case study of pressure protection system for a pressure vessel containing flammable liquid hydrocarbon. A comparison of 1oo1 vs 1oo2 architecture demonstrates an improvement of the system performance due to the introduction of a redundant element within the safety system. This means that utilisation of a redundant architecture not only improves reliability of the system but also improves the safety performance of the system, resulting in lower frequency of system entering hazardous event. The behaviour of the 1oo2 safety system was further assessed by performing sensitivity analysis against CCF rate for various process parameters including demand rate and demand duration as well as component failure rate and repair rate. The results also indicate deterioration in reliability and safety performance of the system due to increase in CCF rate as was expected for redundant structures.

The proposed model in this paper can be applied to all safety systems that have similar features to PRVs such as deluge valves, fire damper (including solenoid valve), circuit breaker and relay, where the safety systems have no automatic diagnostic capability [34] and hence the SIS structure is reduced to a single element only. It is also worth highlighting that the diagnostic capability for some of the other final elements is very low although not annulled (e.g. DC rate for control valves in shutdown service only and blowdown valves is equivalent to 20%). This means that detection of dangerous failures occurs sporadically for these valves and λ_{DU} is almost equivalent to λ_D. Hence, an opportunity arises to investigate whether the model developed in this paper can be utilised to provide an estimation (with some inaccuracy) of the reliability and safety performance for this group of safety systems as opposed to constructing a more complex Markov chain by introduction of DD failure rate to this model. This may lead to expansion in application of the model to larger scale, although, this was beyond the scope of this paper.

The 1oo2 PRV model developed in this paper is based on various underlying assumptions, in specific the assumptions made with regards to restoration of the system from the hazardous state to the "as good as new" state. The relevance of this assumption may vary and for some applications it may not at all be possible to start up again after a hazardous state. In a worst case scenario, the whole system (or plant) may be destroyed as a consequence of the hazardous state. However, the restoration rate is an essential element of the Markov model since it eliminates absorbing state and enables calculation of the steady state probabilities. In some cases however, this is neither applicable, nor a realistic assumption. The detailed analysis of a multi-component system (e.g. 1oo3, 2oo3 etc) will be more complex from a computational point of view, and the main features of the analysis may easily disappear in the computational details, but this has not been pursued any further and may be a topic for further work.

Acknowledgment

Sriramula's work within the Lloyd's Register Foundation Centre for Safety and Reliability Engineering at the University of Aberdeen is supported by Lloyd's Register Foundation. The Foundation helps to protect life and property by supporting engineering-related education, public engagement and the application of re-search.

Notations

P_i	steady state probability for state i
τ	proof test interval
$p_{ij}(t)$	system transition probability from state i to state j
q_{ij}	transition rate from state i to state j
β	total common cause failure factor
β_D	detected common cause failure factor
β_U	undetected common cause failure factor
λ	component failure rate
λ_{DE}	process demand rate
λ_D	dangerous failure rate
λ_{DD}	dangerous detected failure rate
λ_{DU}	dangerous undetected failure rate
λ_S	safe failure rate
λ_{SD}	safe detected failure rate
λ_{SU}	safe undetected failure rate
λ^C	common cause failure rate
λ^I	independent failure rate
λ^I_{DD}	dangerous detected independent failure rate
λ^C_{DD}	dangerous detected common cause failure rate
λ^I_{DU}	dangerous undetected independent failure rate
λ^C_{DU}	dangerous undetected common cause failure rate
λ^I_{SD}	safe detected independent failure rate
λ^C_{SD}	safe detected common cause failure rate
λ^I_{SU}	safe undetected independent failure rate
λ^C_{SU}	safe undetected common cause failure rate
λ^T	total failure rate
μ	component repair rate
μ_{DD}	dangerous detected repair rate

μ_{DE}	demand reset rate
μ_{DU}	dangerous undetected repair rate
μ_S	safe repair rate
μ_T	renewal rate
π_i	steady state probability of system in state i
DC	diagnostic coverage rate
$P(t)$	transition matrix at time t
$P_i(t)$	probability of system in state i at time t
Q	transition rate matrix
r	states of stochastic process

References

[1] IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-related systems, parts 1–7. Geneva: International Electrotechnical Commission; 2010.

[2] IEC 61511, Functional safety: safety instrumented systems for the process industry sector, parts 1–3. Geneva: International Electrotechnical Commission; 2003.

[3] Oliveira LF, Abramovitch RN. Extension of ISA TR84.00.02 PFD equations to KooN architectures. Reliab Eng Syst Saf 2010;95(7):707–15.

[4] Guo H, Yang X. A simple reliability block diagram method for safety integrity verification. Reliab Eng Syst Saf 2007;92(9):1267–73.

[5] Rausand M, Høyland A. System reliability theory: models, statistical methods, and applications. 2nd ed. New Jersey: Wiley; 2004.

[6] Summers AE. Viewpoint on ISA TR84.0.02 – simplified methods and fault tree analysis. ISA Trans 2000;39(2):125–31.

[7] Misumi Y, Sato Y. Estimation of average hazardous-event-frequency for allocation of safety-integrity levels. Reliab Eng Syst Saf 1999;66(2):135–44.

[8] Bukowski JV, Goble WM. Using Markov models for safety analysis of programmable electronic systems. ISA Trans 1995;34(2):193–8.

[9] Bukowski JV. Incorporating process demand into models for assessment of safety system performance. In: Proceedings of RAMS'06 Symposium, Alexandria, VI, USA: 2006, p.

577–81.

[10] Langeron Y, Barros A, Grall A, Bérenguer C. Combination of safety integrity levels (SILs): A study of IEC 61508 merging rules. J Loss Prev Process Ind 2008;21(4):437–49.

[11] Dutuit Y, Innal F, Rauzy A, Signoret JP. Probabilistic assessments in relationship with safety integrity levels by using Fault Trees. Reliab Eng Syst Saf 2008;93(12):1867–76.

[12] Rouvroye JL, Brombacher AC. New quantitative safety standards: Different techniques, different results? Reliab Eng Syst Saf 1999;66(2):121–5.

[13] Jin H, Lundteigen MA, Rausand M. Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation. Reliab Eng Syst Saf 2011;96(3):365–73.

[14] Innal F. Contribution to modelling safety instrumented systems and to assessing their performance critical analysis of IEC 61508 standard. Ph.D. thesis, University of Bordeaux, 2008.

[15] Yoshimura I, Sato Y. Safety achieved by the safe failure fraction (SFF) in IEC 61508. IEEE Trans Reliab 2008;57(4):662–9.

[16] Liu YL, Rausand M. Reliability assessment of safety instrumented systems subject to different demand modes. J Loss Prev Process Ind 2011;24(1):49–56.

[17] Yoshimura I, Sato Y. Estimation of calendar-time- and process-operative- time-hazardous-event rates for the assessment of fatal risk. Int J Performability Eng 2009;5(4):377–86.

[18] CCPS, Layer of protection analysis; simplified process risk assessment. New York: American Institute of Chemical Engineers; 2001.

[19] Smith DJ. Reliability, maintainability and risk. 6th ed. Oxford: Butterworth-Heinemann; 2001.

[20] Goble WM, Brombacher AC. Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems. Reliab Eng Syst Saf 1999;66(2):145–8.

[21] Mechri W, Simon C, BenOthman K. Switching Markov chains for a holistic modeling of SIS unavailability. Reliab Eng Syst Saf 2015;133:212–22.

[22] Hokstad P, Rausand M. Common cause failure modelling: status and trends. In: Misra KB, editor. Handbook of Performability Engineering, London: Springer; 2008, p. 621–40.

[23] Lundteigen MA, Rausand M. Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. J Loss Prev Process Ind 2007;20(3):218–29.

[24] Mechri W, Simon C, BenOthman K, Benrejeb M. Uncertainty evaluation of Safety Instrumented Systems by using Markov chains. In: Proceedings of the 18th International Federation of Automatic Control (IFAC) World Congress, Milano, Italy: 2011, p. 7719–24.

[25] Jin H, Lundteigen MA, Rausand M. New PFH-formulas for k-out-of-n:F-systems. Reliab Eng Syst Saf 2013;111:112–8.

[26] Mechri W, Simon C, BenOthman K. Uncertainty analysis of common cause failure in safety instrumented systems. In: Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 225(4), 2011, p. 450–60.

[27] Fleming K. A reliability model for common mode failures in redundant safety systems. In: Proceedings of the 6th Annual Pittsburgh Conference on Modelling and Simulation, Pittsburgh, PA, USA: 1974, p. 579–81.

[28] Hauge S, Hokstad P, Langseth H, Hauge S, Onshus T. Reliability prediction method for safety instrumented systems. Trondheim: SINTEF; 2006.

[29] Barros A, Grall A, Vasseur D. Estimation of common cause failure parameters with periodic tests. Nucl Eng Des 2009;239(4):761–8.

[30] Vaurio JK. Consistent mapping of common cause failure rates and alpha factors. Reliab Eng Syst Saf 2007;92(5):628–45.

[31] Humphreys RA. Assigning numerical value to the beta factor for common cause evaluation. In: Proceedings of Reliability '87, Altrincham, UK: 1987.

[32] Johnston BD. A structured procedure for dependent failure analysis (DFA). Reliab Eng Syst Saf 1987;19(2):125–36.

[33] Rahimi M, Rausand M. Monitoring human and organizational factors influencing common-cause failures of safety-instrumented system during the operational phase. Reliab Eng Syst Saf 2013;120:10–7.

[34] Hauge S, Langseth H, Onshus T. Reliability data for dafety instrumented systems. Trondheim: SINTEF; 2010.

[35] Liu YL, Rausand M, Jin H. Modelling and reliability assessment of a 3-channel safety-

instrumented system. In: Proceedings of the 19th IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Hong Kong, China: 2012, p. 2098–102.

[36] Zhang T, Long W, Sato Y. Availability of systems with self-diagnostic components – Applying Markov model to IEC 61508-6. Reliab Eng Syst Saf 2003;80(2):133–41.

[37] Stavrianidis P, Bhimavarapu K. Safety instrumented functions and safety integrity levels (SIL). ISA Trans 1998;37(4):337–51.

[38] Williams JC. HEART – A proposed method for assessing and reducing human error. In: Proceedings of the 9th Advances in Reliability Technology Symposium, Bradford, UK: 1986.