Unavailability Assessment of Redundant Safety Instrumented Systems Subject to Process Demand

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

[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.

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

Abstract

The process industry has always been faced with the challenging task of determining the overall unavailability of safeguarding systems such as the Safety Instrumented Systems (SISs). This paper proposes an unavailability model for a redundant SIS using Markov chains. The proposed model incorporates process demands in conjunction with dangerous detected and undetected failures for the first time and evaluates their impacts on the unavailability quantification of SIS. The unavailability of the safety instrumented system is quantified by considering the Probability of Failure on Demand (PFD) for low demand systems. The safety performance of the system is also assessed using Hazardous Event Frequency (HEF) to measure the frequency of system entering a hazardous state that will lead to an accident. The accuracy of the proposed Markov model is verified for a case study of a chemical reactor protection system. It is demonstrated that the proposed approach provides a sufficiently robust result for all demand rates, demand durations, dangerous detected and undetected failure rates and associated repair rates for safety instrumented systems utilised in low demand mode of operation. The effectiveness of the proposed model offers a robust opportunity to conduct unavailability assessment of redundant SISs subject to process demands.

Keywords: Markov Chain; Unavailability Assessment, Safety Instrumented Systems; Hazardous Event Frequency; Process Demand.

1.0 Introduction

Independent Protection Layers (IPLs) are predominantly used to prevent hazardous events, and to mitigate their consequences to humans, the environment, and financial assets. IPLs can be implemented by physical barriers such as mechanical systems, instrumented protective functions or in the form of administrative procedures. An Electric, Electronic and Programmable Electronic System (E/E/PES) such as a Safety Instrumented System (SIS) is an independent layer of protection that provides a protective function by detecting hazardous events, performing the required safety action and maintaining the safe status of the system. The unavailability of a SIS is usually realised from overall hazard and risk analyses. Without suitable design, implementation and maintenance, the SIS may fail to provide the necessary risk reduction. In this context, IEC

61508 [1] standard is a guide for designing, validating and verifying the safety function realised by an E/E/PES throughout all phases of its lifecycle. The principles introduced in this generic standard, are also customised in application specific standards, such as IEC 61511 [2] for the process industry, IEC 62425 [3] for the railway industry, and ISO/DIS 26262 [4] for the automobile industry.

In accordance with IEC 61508 [1] the performance of a SIS shall be proven using a suitable technique. Although no particular model is recommended by the international standards, some of the options are cited in their appendices. The most commonly used techniques include Simplified Equation (SE) [1,5], Bayesian methods [6] Reliability Block Diagram (RBD) [7,8], Fault Tree Analysis (FTA) [9,10], Markov Analysis (MA) [11–13] and Petri Nets (PN) [14]; all of which can be used to analyse the reliability of SIS utilised in various modes of operations. These diverse techniques have their own advantages and limitations. Zhang et al. [15] demonstrated that the simplified equations given in the standard are over simplistic and are more suitable for practicing engineers. The reliability block diagrams represent a success oriented logic system structure and hence the analyst will focus on functions rather than failures, and may thereby fail to identify all the possible failure modes [16]. The fault tree analysis is straightforward to handle for the practitioners and generates approximations which sometimes provide non-conservative results as argued by Dutuit et al. [14].

Whilst the main benefit of Markov models is accuracy and flexibility according to the specific feature of each mode, establishing a Markov model of *k* out of *n* (*k*oo*n*) with a high value of *n*, can be time consuming and error prone [17–19]. Signoret et al. [20] employed Petri Nets to categorise safety instrumented systems. Although Petri Nets allow assessment of the SIS performance very finely taking into account several parameters, the models of safety instrumented system produced by Petri Nets can be challenging to use and the analyst should make substantial effort to obtain an understandable model to compute unavailability [20].

A comparison of reliability analysis techniques carried out by Rouvroye and Brombacher [21] concludes that Markov analysis covers most aspects for quantitative safety evaluation. Additionally, Innal [22] investigated the performance of different modelling approaches and observed that Markov methods are the most suitable approach due to their flexibility. Guo and

Yang [7] also highlighted that Markov analysis shows more flexibility and is the only technique that can describe dynamic transitions amongst different states of a system. A number of Markov models were evolved in recent years that combine the dynamic behaviour of safety instrumented systems and the impact of process demand inflicted on the SIS. A simple Markov model of SIS was first created by Bukowski [12] which included both dangerous detected and undetected failures in conjunction with the process demand. Jin et al. [23] further developed the preliminary model of Bukowski [12] and incorporated the repair rate of dangerous undetected failures for safety instrumented system in addition to inclusion of safe failure and repairs. In a separate attempt to extend the boundaries of Markov analysis for redundant systems, a Markov chain was generated by Liu et al. [24] for a redundant configuration, however, the dangerous detected failures were omitted to adopt the core characteristics of a specific safety system known as a pressure relief valve.

This paper aims to address this limitation by proposing a unique Markov chain to model the unavailability of redundant SIS subject to process demand which includes both dangerous detected and undetected failures. Therefore, this model is deemed as one step closer to analysing actual behaviour of the redundant configurations since dangerous detected failures influence unavailability and safety performance of the safety instrumented systems and cannot be omitted in generic SIS architectures. The model available in Jin et al. [23] is extended further by using Markov chains for their ability to model accurately and correctly a redundant safety instrumented system in low demand. The proposed model integrates the following parameters: diagnostic coverage, dangerous undetected failures, dangerous detected failures, repair rates, process demand and demand reset rate. The concurrent consideration of process demand and system failures (dangerous detected and dangerous undetected) offers a unique opportunity to analyse the SIS behaviour using an integrated model as opposed to verifying SIS architecture in isolation by exclusion of the process demand. In Section 2 we recall the principle of safety instrumented systems. Section 3 entails the mathematical preliminaries and consists of basic elements required for reliability modelling. Section 4 is devoted to the Markov models of simple and redundant safety instrumented systems followed by a numerical analysis presented in Section 5. Applications of the proposed models are discussed in Section 6 based on the results obtained, and concluding remarks are drawn at the end of this section.

2.0 Safety Instrumented Systems

2.1 Definition & Key Parameters

The primary objective of a SIS is to bring the system it supervises to a safe position i.e. in a situation where it protects people, environment and/or asset when the Equipment Under Control (EUC) deviates from its design intent into a hazardous situation and results in an unwanted consequence (e.g. loss of containment leading to explosion, fire, etc.). SISs are frequently utilised across process industry to prevent the occurrence of hazardous events or to mitigate the consequences of undesirable events. A SIS may execute one or multiple Safety Instrumented Functions (SIFs) to attain or maintain a safe state for the EUC (e.g. equipment, system etc.) the SIS is protecting against a specific process demand [8].

A SIS is a system consisting of any combination of sensors, logic solvers and final elements for the purpose of taking the supervised process to a safe state when predetermined design conditions are violated [13,25]. A SIS (or SIS subsystem) is recognised to have a *k*oo*n* configuration when *k* units of its *n* total units have to function to provide the required system function. Typical SIS configurations comprised of 1oo1, 1oo2, 1oo3, and 2oo3 [22]. In this article, only the two first configurations are considered, a 1oo1 system (i.e. a single unit) and a 1oo2 system. This demarcation is established because we believe that the main features of our new model will be illustrated by these simple systems. The Markov models of systems with more components will be complex and the main features of the approach will easily disappear in the technical calculations. Another reason for this delimitation is that the aforementioned systems have been thoroughly assessed with other approaches [1,26], therefore facilitating comparison.

2.2 Low Demand vs High Demand

Two separate modes of SIS operation comprised of low demand and high demand are outlined by IEC 61508 [1] based on two main criteria: (1) the frequency at which the SIS is expected to operate in response to demands, and (2) the anticipated time interval that a failure may remain hidden, taking cognisance of the proof test frequency. A SIS is in low demand mode of operation if the demand is less than or equal to 1 per year and in high demand mode in other situations [1,27]. The demand rate for a SIS may vary from continuous to very low (i.e. infrequent demands) and the duration of each demand may fluctuate from instantaneous up to a rather long period (e.g. hours). High demand systems are different from low demand systems, and the same analytical techniques can normally not be applied to all systems in various modes of operations. FTA and analysis based on RBD are generally not suitable for high demand systems when the duration of demands is significant. Several authors have indicated that Markov methods are best suited for analysing both high demand and low demand systems [24].

Despite the clear distinction between the high demand and the low demand mode of operation, there are still some underlying issues that cause confusion and problems in the quantification of SIS unavailability and safety performance [28]. As such, instead of drawing a clear boundary between low demand mode and high demand mode of operation, some authors suggest to incorporate the rate of demands into the analysis of safety instrumented systems [10,12,28].

2.3 Integrity Levels

IEC 61508 / 61511 [1,2] present the requirements of safety function and introduce a probabilistic approach for the quantitative assessment of the SIS unavailability. The instigation of probability into the evaluation of the integrity level necessitated the particular concept of average probability of failure on demand (PFD) for low demand mode of operations and probability of failure per hour (PFH) for high demand systems. Thus, the PFD is in fact the unavailability of the system that signifies its ability to react to hazards, i.e. the safety unavailability [27,29,30]. The quantification of this performance is determined by Safety Integrity Levels (SIL). The IEC 61508 standard [1] establishes 4 classifications of integrity levels based on the PFD and/or PFH. The definition of SIL classes can be seen in Table 1:

Table 1 – SIL Levels Definition

Integrity Level	Low Demand	High Demand
$1 \leq i \leq 4$	$PFD \in \left[10^{-(i+1)}, 10^{-i}\right]$	$PFH \in \left[10^{-(i+5)}, 10^{-(i+4)}\right]$

Furthermore, IEC 61508 [1] requires to estimate the PFD due to random hardware failures for the SIS main elements. The calculations for assessing the performance can consider a large number of parameters including but not limited to component failure rates, mean times to repair, diagnostic coverage, common cause failures and proof test intervals. The interpretation of PFD and PFH is questioned by various authors [10,12,28] and a common measure for use with both low demand and high demand mode is proposed [10,12]. Bukowski [12] calculates the probability of being in a state “of fail dangerous and process requires shutdown” based on a Markov model, while Misumi et al. [10] used FTA to develop analytical formulae for what they call the “hazardous event frequency”. These proposals are promising for the quantification of SIS unavailability in general, however further development is required to reflect all relevant modelling aspects. In this paper both the PFD and hazardous event frequency will be used as performance indicators of the safety instrumented systems.

3.0 Mathematical Preliminaries

3.1 Failure Modes

The SIS failure modes are categorised into two categories, safe failures and dangerous failures. Safe failures cause the system to fail safe, e.g. the component operates without demand [31]. The safe failures are divided into Safe Detected (SD) and Safe Undetected (SU) failures. Safe failures do not have any effect on the ability of the SIS to perform its functions and hence excluded from the SIS models in this paper. Dangerous failures prevent the SIS from performing its function, i.e. the component does not operate on demand. Similarly, the dangerous failures are divided into detected and undetected. The relevant failure modes are [31]:

- Dangerous Detected (DD): this is a dangerous failure mode, however the failure will be detected almost immediately.
- Dangerous Undetected (DU): this is also a dangerous failure mode that may occur during normal operation, however will not be revealed until a proof test (or functional test) is carried out or until a real demand for the system occurs.

Assuming that the λ_{DD} represents DD failure rate and λ_{DU} is the DU failure rate, the overall dangerous failure rate of a component λ_D is obtained from

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{1}$$

Although majority of the failures are detected via online diagnostic testing system, proof tests are normally performed at regular time intervals to reveal and rectify dangerous undetected failures prior to the occurrence of a demand. In order to model the unavailability of a safety instrumented system successfully, it is essential to recognise the nature of the failure modes and means of their detection. This would allow the development of appropriate strategies to ensure the required functionality, reliability and availability of safety instrumented functions as specified in IEC 61508 [1].

3.2 Diagnostic Coverage

Diagnostic testing is a feature that is sporadically lodged for programmable electronic components. A diagnostic test is able to reveal certain types of failures, such as run-time errors and signal transmission errors, without interrupting the equipment under control by fully operating the main functions of the component. The diagnostics of a pressure transmitter may reveal drifting in the signal conversion, without the pressure transmitter responding to a genuine high pressure signal. The diagnostic tests are performed usually with an interval between seconds and hours. For low demand SISs, this allows sufficient time to carry out repair activities and restore the component function prior to the next process demand. Therefore, diagnostic testing is a means to timely reveal dangerous failures, and thereby reduce the SIS unavailability; whether or not such a testing leads to side-effects is seldom evaluated [32]. IEC 61508 [1] defines the Diagnostic Coverage (DC) rate as the ratio between the failure rate of detected dangerous failures, λ_{DD}, and the total failure rate of the dangerous failure, λ_D [29]:

$$DC = \frac{\lambda_{DD}}{\lambda_D} = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \tag{2}$$

As such, the DC rate represents the effectiveness of the diagnostic test. The diagnostic testing can detect dangerous failure more or less immediately post occurrence of a failure, however only a fraction of dangerous failures can be usually detected. This fraction of dangerous failures is defined as DD failures, and the remaining failures that are only detected by proof testing are DU failures. Therefore, DC rate distinguishes the dangerous failures into detected and undetected, resulting in two distinct failure modes [33] as follows:

$$\lambda_{DD} = DC.\lambda_D \qquad \lambda_{DU} = (1 - DC).\lambda_D \tag{3}$$

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

$$\lambda_D = DC.\lambda_D + (1 - DC).\lambda_D \tag{4}$$

The effect of diagnostic testing should be carefully evaluated at design stage of SIS taking conscience the influencing parameters such as process demand frequency, diagnostic coverage rate, the diagnostic test interval and time required for completion of the repair activity.

3.3 Testing Strategies & Repair Rates

3.3.1 Proof Test

A SIS in low demand mode has the specificity to be periodically tested. The primary objective of the proof tests (also known as functional tests) is to detect latent failures and to ensure that the SIS meets the requirements and preserves its safety integrity level [34]. As such, the proof tests have a fundamental importance for the SIS since they facilitate retaining and improving the SIL without making design modifications [34]. When the latent failures are detected, the system can be restored to “as good as new” or as close as practical to this condition [1]. Although the necessity of proof testing for safety instrumented systems operating in high demand mode is not always evident [23], it is essential for low demand SISs to ensure that a dangerous undetected failure does not remain hidden for a long time. The proof test can be applied utilising various test strategies [35]. The proof test interval denoted by τ, is considered equal to the length of time after which a proof test of safety instrumented function is carried out.

3.3.2 1oo1 System

For the dangerous failures detected via online diagnostic testing, the equipment downtime is limited to the actual repair time, assuming the repair actions are commenced immediately after detection of the failure. Therefore, the repair rate of dangerous detected failures, μ_{DD}, can be obtained directly from the Mean Time To Repair (MTTR) as follows:

$$\mu_{DD} = \frac{1}{MTTR} \tag{5}$$

However, the equipment downtime due to dangerous undetected failures are not solely limited to the repair time as the failure is hidden and has not yet been revealed by an online diagnostic test. The undetected failures can be revealed either by solicitation of the equipment under control or by proof testing, assuming these tests are comprehensive and perfectly accurate (i.e. 100% detection rate) in detecting latent failures. The average downtime for undetected failures consists of two elements, unknown downtime and known downtime.

Unknown downtime: considering a Poisson process, if one and only one event occurs in the interval between 0 and τ, then the timing of when the event occurs is uniform between 0 and τ [36,37]. Since the undetected dangerous failure of SIS component is a sole event (i.e. DU failure cannot occur more than once during the proof test interval) and is assumed as a random variable following a Poisson process (i.e. $N(\tau) = 1$), the probability of failure occurring before time t ($t \leq \tau$) is obtained from:

$$P(T < t|N(\tau) = 1) = \frac{e^{-t\lambda_{DU}}\left(\frac{t\lambda_{DU}}{1!}\right) . e^{-\lambda_{DU}(\tau-t)}}{e^{-\tau\lambda_{DU}}\left(\frac{\tau\lambda_{DU}}{1!}\right)} = \frac{t}{\tau} \tag{6}$$

As such, the undetected dangerous failure time follows uniform distribution during its test interval between 0 and τ. The average downtime prior to detection of the failure is therefore equivalent to half of the test interval [8]:

$$t \sim U(0, \tau) \rightarrow E(t) = \int_0^\tau \frac{1}{\tau} t dt = {}^{\tau}\!/_{2} \tag{7}$$

Known downtime: once the failure is detected the equipment downtime due to repair is equivalent to MTTR assuming the remedial actions are initiated immediately after detection of the failure during proof testing. The time to perform a proof test is often negligible and therefore excluded from average downtime. The dangerous undetected repair rate, μ_{DU}, can be calculated as:

$$\mu_{DU} = \frac{1}{{}^{\tau}\!/_{2} + MTTR} \tag{8}$$

Of the two contributing elements to the downtime of undetected failures, the unknown part is generally governing the overall downtime of equipment. The failure modes and associated repairs for a 1oo1 SIS are illustrated in Figure 1. The approach undertaken in this paper to obtain the "unknown" downtime portion of DU repair rate (μ_{DU}), for a 1oo1 system, using the relationship between the Poisson process and Uniform distribution (Equation (6)) is exclusive and offers an alternative means in obtaining the average downtime for a 1oo1 system. The average downtimes computed in this paper are not the same as $\mathrm{PFD_{avg}}$ defined in IEC 61508 and 61511 but are deemed acceptable as they are more conservative than the $\mathrm{PFD_{avg}}$ that would be computed from the same Markov model.

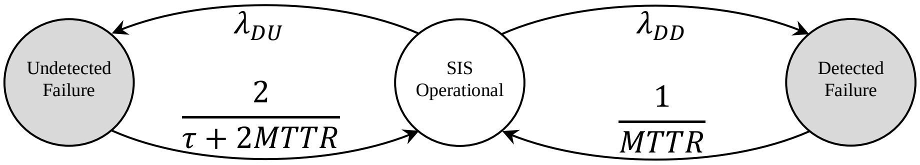

Figure 1 – Failure & Repair Rates of 1oo1 SIS

3.3.3 1oo2 System

The DD repair rate, μ_{DD}, for a 1oo2 configuration is identical to 1oo1 system and can be acquired from Equation (5) assuming availability of the diagnostic testing and instantaneous commencement of repair action. Similar to the 1oo1 architecture, undetected failures in 1oo2 system can be revealed upon discharge of a process demand or by performing a proof test, assuming precise 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 calculated by ${}^{\tau}/_{3} + MTTR,$ the DU repair rate, μ_{DU}, can be obtained from [38]:

$$\mu_{DU} = \frac{1}{MDT} = \frac{1}{{}^{\tau}/_{3} + MTTR} \tag{9}$$

The DD and DU repair rates are embedded within the unavailability model proposed in this paper in parametric form. The case study in section 5 however will take account of the repair rate values accordingly.

3.4 Demand Rate & Demand Duration

The process demands are assumed to occur according to a Homogeneous Poisson Process (HPP) with rate λ_{DE}, hence the time between two consecutive demands is exponentially distributed with parameter λ_{DE} [39]. The duration of each demand is also assumed to be exponentially distributed with rate, μ_{DE}. Therefore, the mean demand duration is $1/_{\mu_{DE}}$. It is further assumed that the SIS is "as good as new" after a successful response to a process demand. When a hazardous event occurs, we assume that the system is restored / renewed to the normal functional state. The renewal rate is also assumed to be exponentially distributed with rate μ_T.

3.5 Quantitative Evaluation

The performance evaluation of SIS must be obtained by quantitative methods as stipulated by the international standards IEC 61511 [2]. This evaluation is accomplished by the computation of the safety function unavailability on demand [14,29]. In this context, Markov chains are widely recognised as suitable modelling technique for calculating unavailability of SIS considering all possible events (failure, repair, etc) and associated parameters (detected and undetected etc). Markov chains offer an appropriate tool for modelling the dynamic behaviour of the SIS under study [13,24]. The Markov chains presented in this article follow homogeneous process meaning that transition probabilities of Markov chain are considered to be time independent. As such, the transitions associated with repairable systems are considered to be constant, i.e. components of the system fail at constant failure rate and restored at constant restoration rates [13,24]. This assumption is consistent with useful life of components i.e. maturity phase of bathtub curve.

3.6 Markov Chains

A Markov chain is a model that transits from state i to state j with a transition rate a_{ij} which depends only on the states i and j. Let transition rate matrix $\boldsymbol{A} = [a_{ij}]$ be $(r \times r)$ constructed from all transition rates a_{ij}, as:

$$\boldsymbol{A} = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & \cdots & a_{2r} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & \cdots & a_{rr} \end{bmatrix} \tag{10}$$

where the transition rates are obtained from the following equation assuming the transition probability from state i to j at time t is denoted by $p_{ij}(t)$:

$$a_{ij} = \frac{d}{dt} p_{ij}(t) = \lim_{\mathrm{t} \to 0} \frac{p_{ij}(t)}{t} \tag{11}$$

As $\boldsymbol{A}$ is a transition rate matrix, the sum of each row of $\boldsymbol{A}$ is equal to zero. This means that all transition rates a_{ij} are equal to or greater than zero and $a_{ii} = -\sum_{j=1}^{r} a_{ij}$, $i \neq j$ for $i = 1,2,\dots,r$. The Kolmogorov Forward Equations [8] give:

$$\boldsymbol{P}(t).\boldsymbol{A} = \acute{\boldsymbol{P}}(t) \tag{12}$$

where $\boldsymbol{P}(t) = [P_1(t),\dots,P_r(t)]$, $P_i(t)$ is the probability that the system is in state i at time t, and $\acute{\boldsymbol{P}}(t)$ is the time derivative of $\boldsymbol{P}(t)$. The probability of 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:

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

&

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

The steady state probability for state i, π_i, is the long-run probability that the system is in state i. It also signifies the mean proportion of time the system is in state i [23]. The vector $\boldsymbol{\Pi} = [\pi_1,\dots,\pi_r]$ represents the steady state probabilities and the fact that the sum of the steady state probabilities is always equal to 1.

$$\sum_{i=1}^{r} \pi_i = 1 \tag{15}$$

The following linear system of equations can be used for a homogeneous Markov chain to calculate the steady state probabilities [8]:

$$\boldsymbol{\Pi}.\boldsymbol{A} = 0 \tag{16}$$

In a Markov model, the frequency of entering a hazardous state can be obtained directly from the transition diagram. The system transits to the hazardous state 0 when a demand is inflicted on it whilst the SIS is failed dangerously either detected or undetected. The hazardous event frequency (HEF) is equal to the visit frequency to state 0, from any other possible states [8], as:

$$HEF = \sum_{i=1}^{r} a_{i0}\,\pi_i \tag{17}$$

In this article, we aim to investigate the unavailability of safety instrumented system where redundancy in components is included within the architectural design of the system. This takes into account the process demand rate and duration of demand for safety instrumented systems operating in low demand mode. The considered framework for unavailability assessment of redundant SIS subject to process demand using Markov chains is illustrated in Figure 2.

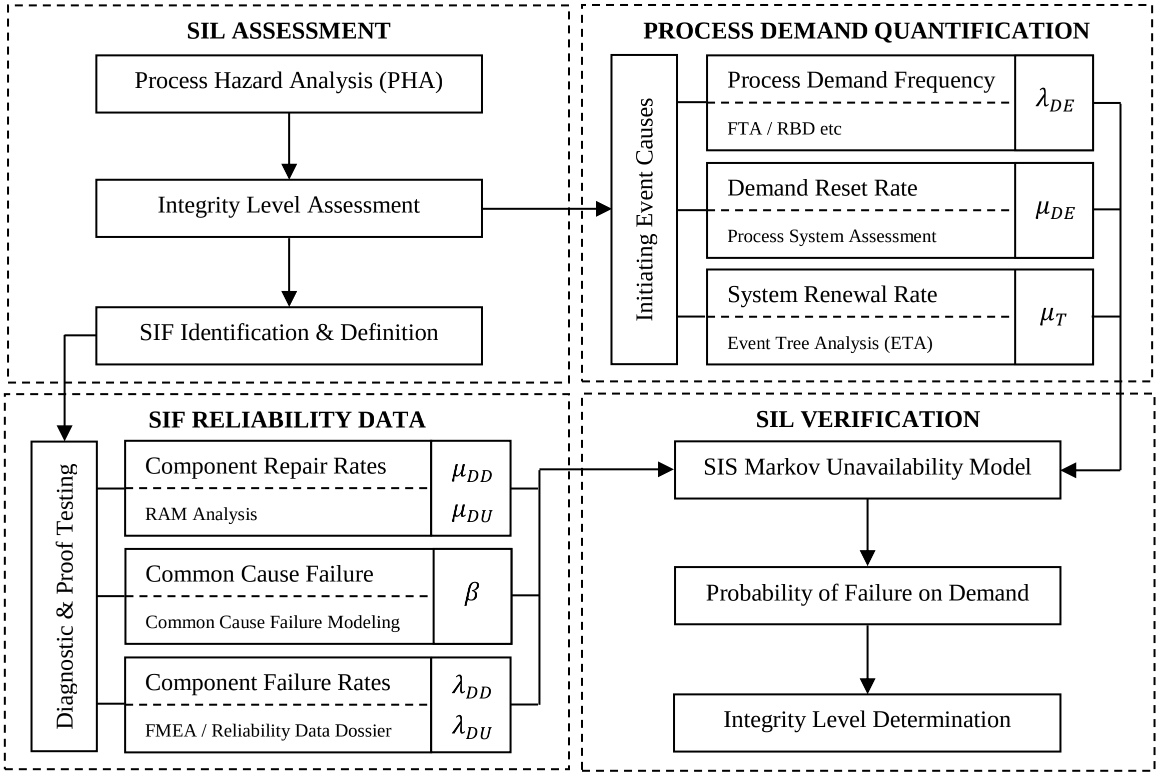
SIL ASSESSMENT
Process Hazard Analysis (PHA)
Integrity Level Assessment
SIF Identification & Definition
PROCESS DEMAND QUANTIFICATION
Initiating Event Causes
Process Demand Frequency
FTA / RBD etc
λ_{DE}
Demand Reset Rate
Process System Assessment
μ_{DE}
System Renewal Rate
Event Tree Analysis (ETA)
μ_T
SIF RELIABILITY DATA
Diagnostic & Proof Testing
Component Repair Rates
RAM Analysis
μ_{DD}
μ_{DU}
Common Cause Failure
Common Cause Failure Modeling
β
Component Failure Rates
FMEA / Reliability Data Dossier
λ_{DD}
λ_{DU}
SIL VERIFICATION
SIS Markov Unavailability Model
Probability of Failure on Demand
Integrity Level Determination

Figure 2 – Framework for Unavailability Assessment for Redundant SIS Subject to Process Demand

3.7 Modelling Considerations

3.7.1 Assumptions

The underlying assumptions of the SIS models developed in this paper are as follows:

- The times to failure (dangerous detected / undetected) are exponentially distributed (all failure rates are constant in time).
- Failures occur independently and their severities are constant over time.

- The time between demands is exponentially distributed (the process demand rate is constant).
- The process demand duration and restoration time from hazardous state are exponentially distributed.
- Proof tests are comprehensive (100% accurate) and carried out periodically in line with test intervals of the system.
- A single maintenance team is available on site.
- The system is studied over one test interval only.
- The system can be considered “as good as new” post repair or a proof test.

3.7.2 Transition Rates

In order to develop state transition diagram it is essential to define a set of transition rates representing the physical status of the system. 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 a reset from the DU occurs per hour
- μ_{DD} DD repair rate - the frequency that an active repair of DD 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

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

3.7.3 Proof Test Coverage & Common Cause Failures

The model presented in this paper excludes two variables, consisting of Proof Test Coverage (PTC) and Common Cause Failures (CCFs). We discuss in this section the justification and potential implications of their incorporation within the Markov model.

The impact of proof test coverage (also known as imperfect proof test) was discarded in various publications including studies based on Markovian technique (e.g. Jin et al. [23], Liu et al. [24], Zhang et al. [38] etc.) and those that implemented non-Markovian methodology (e.g. Wang et al. [16] etc.) on the basis of 100% detection rate during proof tests. This is also evident in the IEC 61508 approach where the formulas do not include the effects of non-perfect proof-testing [19]. Similarly, the assessment of proof test coverage was not explored further in this paper considering that proof tests are assumed as comprehensive (100% accurate) and carried out periodically in line with test intervals of the system. However, where the proof tests are not perfect (i.e. not 100% accurate) or when proof tests can be 100% accurate but are not completely executed, then the PTC ratio shall be considered in accordance with the latest edition of IEC 61511 (2016). This implies the identification of the DU failures which, inherently, can never be detected by proof tests. Inclusion of PTC within the unavailability model may potentially lead to significant change in the structure of the Markov chain. Nevertheless, one shall analyse the model's behaviour more accurately prior to incorporation of PTC as an additional variable. The proposed unavailability model in this paper however provides a platform to include the PTC in the next phase of its development.

A query may arise as once proof test coverage is included in the state diagram, the assumption of constant repair rates no longer applies for all states. Thus, without the assumption of constant repair rates, unavailability cannot be determined by considering steady state equations because without constant repair rates a steady state does not occur and therefore the model needs to be solved numerically. A separate study conducted by Bukowski [40] to evaluate the impact of non-exponential repair times (non-constant repair rates) on the steady state probabilities in Markov models concludes that exponential repair-time densities can be used in Markov models and will generate the same results as more complicated non-exponential repair-time densities. As such, the assumption of constant repair rates (regardless of whether the actual repair rates are exponentially distributed or not) used in the proposed Markov chain is justifiable and the unavailability model proposed in this paper provides a reasonably accurate result. This is also valid when incorporation of proof test coverage variable results in alteration of repair rate density functions.

The CCF is similarly excluded from the proposed Markov model. However, in order to include CCFs, the rate of independent (ID) failures shall be segregated from the total failure rate, such that $(1-\beta_U)\lambda_{DU}$ / $(1-\beta_D)\lambda_{DD}$ (where β_U and β_D represent CCF factors for DU and DD failures respectively) is used instead of λ_{DU} / λ_{DD} for independent DU / DD failures. Subsequently, CCF rates ($\beta_U\lambda_{DU}$ / $\beta_D\lambda_{DD}$) leading to subsystem unavailability are required to be clearly identified for redundant subsystems. Furthermore, a repair strategy for the Markov model shall be established to identify whether a single stage repair policy would be feasible or multiple stage repair strategy of CCF can be used instead. On this basis, incorporation of CCF into the proposed Markov model would merit a standalone study where the impact of CCF factor can be studied in detail and behaviour of the model can be examined thoroughly. Consequently, evaluation of CCF was excluded in the scope of this paper and it may be a topic for future work.

The effect of proof test coverage and CCF remain as one of the areas for further improvement of the proposed model since it was primarily developed to investigate the combined effect of process demand and SIS failure modes only. Noting the limitations embedded within the other SIL verification methodologies (e.g. FTA, RBD, Simplified Equations etc), specific attention is needed in this area to introduce these variables into the Markov chains to enhance their applicability and precision in assessing the SIS PFD value.

4.0 Markov Models for SIS

In this section two reliability models for 1oo1 and 1oo2 safety instrumented systems are developed using Markov chains. We start by analysing a simple 1oo1 SIS by re-constructing the state transition diagram, and then introduce a new reliability model for a 1oo2 redundant SIS.

4.1 1oo1 SIS Markov Model

A Markov model for a simple safety instrumented system of 1oo1 architecture was originally presented by Jin et al. [23]. The system's situation consists of the combined characteristics 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 manifestation. In this case the SIS has not failed due to DU or DD failure and has not been spuriously activated. SIS is defined as "functioning" state when it is responding to a process demand.

Table 2 – States of 1oo1 SIS

System State	Property	Demand State
0	Hazardous	On Demand
1	DU Failure	No Demand
2	Functional	On Demand
3	DD Failure	No Demand
4	Functional	No Demand

The possible states of the system are listed in Table 2 and the Markov transition diagram is shown in Figure 3 where the nodes correspond to the system states and arrows represent system transition from one state to another.

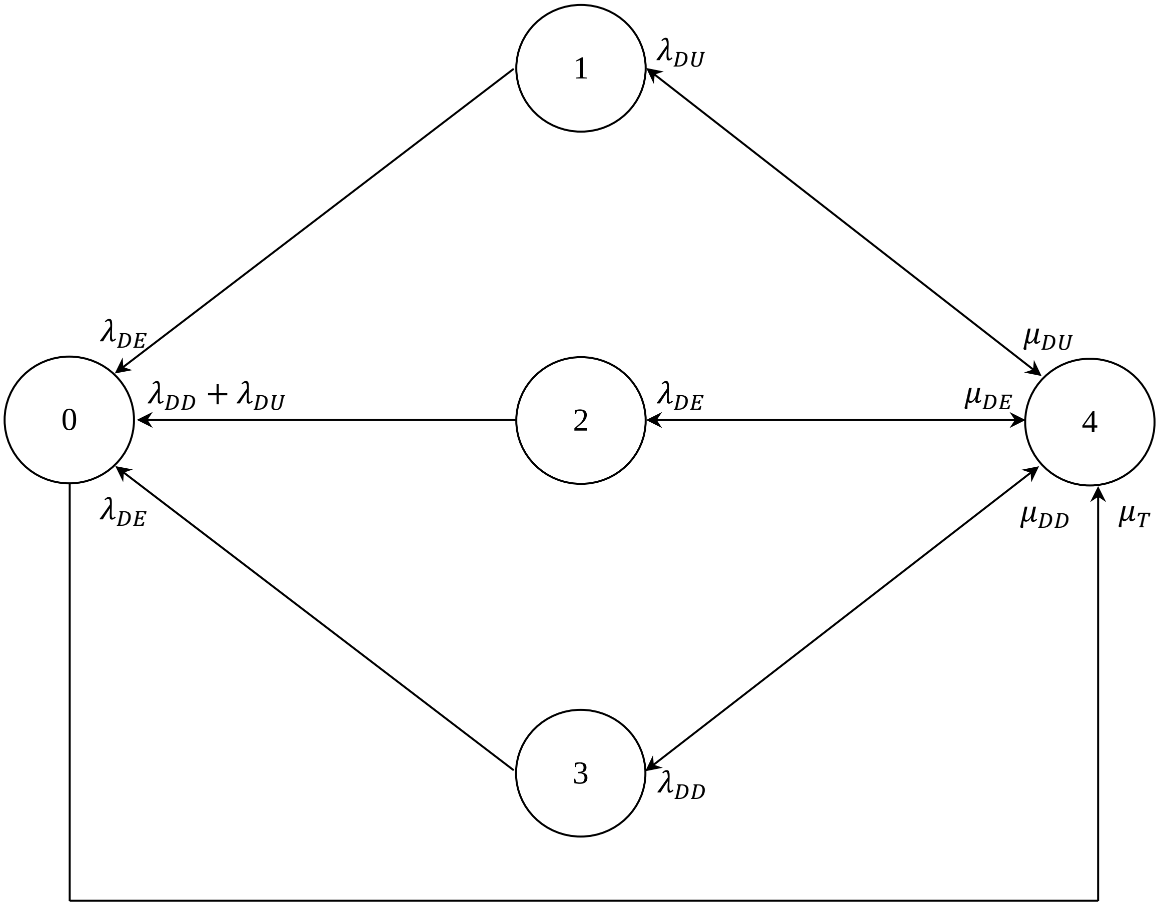

Figure 3 – State Transition Diagram for a 1oo1 SIS

State 4 denotes the initial and normal operating state in the transition diagram, where the SIS is available but there is no demand for activation of the SIS. The system transits to state 1 or 3 from state 4, if SIS endures a DU or DD failure while there is no process demand on the SIS.

Imposition of a process demand at either of these two states will result in occurrence of the hazardous event. State 2 represents the functioning state where the SIS is responding to a process demand. The system enters hazardous state 0 from state 2 when either of DU or DD failure occurs whilst the SIS is responding to a process demand in functional status. State 0 (hazardous state) represents a state where the SIS sustains a failure (DU or DD) and there is a demand for activation of the SIS.

Repair of a DU failure in state 1 or DD failure in state 3 will lead to system transition to the fully functioning state by the corresponding repair rate (μ_{DU} or μ_{DD}). A restoration action is initiated when system enters the hazardous state (state 0) and the system is started up again in a "as good as new condition" in state 4 when the restoration is completed. The mean time required to restore the system from state 0 to state 4 is considered to be ${}^{1}\!/_{\mu_T}$. It shall be noted that the relevance of this assumption may vary for some applications as start up after a hazardous event may not be practical. In a worst credible event scenario, the entire system may be demolished due to a consequence of the hazardous event. The steady state equations [8] corresponding to the state transition diagram in Figure 3 are as follows:

$$\begin{aligned}
\mu_T P_0 &= \lambda_{DE}(P_1 + P_3) + (\lambda_{DD} + \lambda_{DU})P_2 \\
\mu_{DE} P_2 &= \lambda_{DE} P_4 - (\lambda_{DD} + \lambda_{DU})P_2 \\
\mu_{DU} P_1 &= \lambda_{DU} P_4 - \lambda_{DE} P_1 \\
\mu_{DD} P_3 &= \lambda_{DD} P_4 - \lambda_{DE} P_3
\end{aligned} \tag{18}$$

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

$$P_0 + P_1 + P_2 + P_3 + P_4 = 1 \tag{19}$$

The 1oo1 SIS will not be able to respond to a process demand when it is in state 1 or 3, hence the PFD of the safety system is given by:

$$PFD = P_1 + P_3 \tag{20}$$

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:

$$HEF = \lambda_{DE}(P_1 + P_3) + (\lambda_{DD} + \lambda_{DU})P_2 \tag{21}$$

4.2 1oo2 SIS Markov Model

Another common configuration for safety instrumented systems is 1oo2, where the protection function is available if at least one of the two components is operational. The redundancy improves availability of the system, however may bring common cause failures which occur when two or more components fail simultaneously due to a common stressor. In this article CCF is not considered to focus on unavailability model. Using the 1oo1 system as a platform, we intend to introduce a new Markov chain for a 1oo2 redundant SIS by inclusion of both DD and DU failures for the first time as well as incorporating process demand within the unavailability model. The general underlying assumptions listed in section 3.7.1 are all valid for 1oo2 SIS model. The possible states of the system are outlined in Table 3 and the Markov transition diagram is illustrated in Figure 4:

Table 3 – States of a 1oo2 SIS

System State	Property	Demand State
0	Hazardous	On Demand
1	2 DD	No Demand
2	2 DU	No Demand
3	1 Functional, 1 DD	On Demand
4	1 Functional, 1 DU	On Demand
5	1 DD, 1 DU	No Demand
6	1 Functional, 1 DD	No Demand
7	1 Functional, 1 DU	No Demand
8	2 Functional	On Demand
9	2 Functional	No Demand

In a 1oo2 redundant system, single failure does not impact system ability to respond to a process demand and hence has no impact on its availability. In this case SIS is still defined as in “functioning” state. Taking this into cognisance we describe the structure of the Markov chain for a 1oo2 safety instrumented system developed in this paper. 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 instrumented system. Consistent with the 1oo1 system, safe failures are excluded for modelling purpose since the probability of failure on demand is characterised by dangerous failures only. The system transitions due to dangerous failures, λ_{DU}

and λ_{DD}, and associated repairs, μ_{DU} and μ_{DD}, are intact. 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 the simple architecture and in the same industrial application to reduce unavailability.

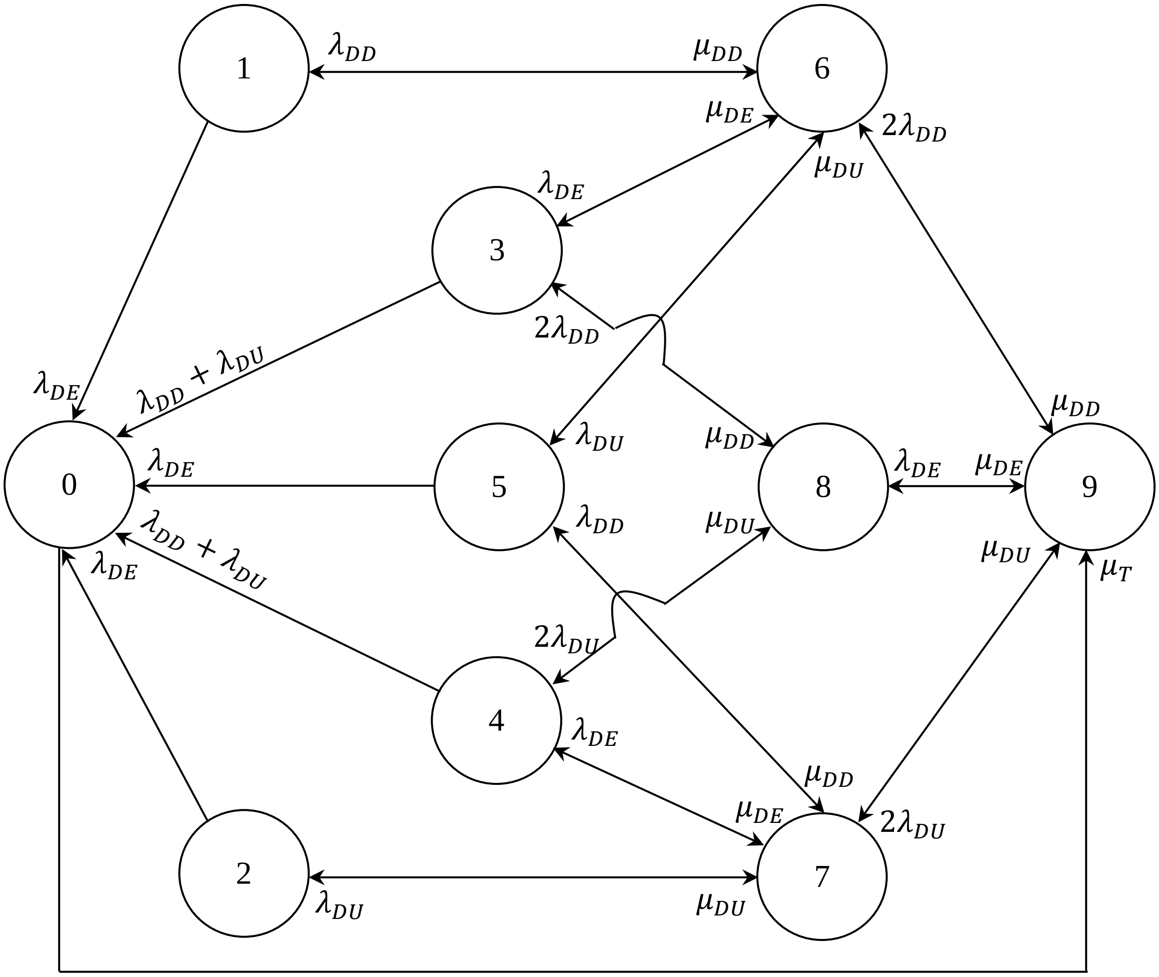

Figure 4 – State Transition Diagram for a 1oo2 SIS

Starting with system in fully functional status and no process demand (i.e. state 9), the SIS fails dangerously (detected) while there is no process demand and transits from state 9 to state 6 with failure rate $2\lambda_{DD}$. This is a minimum of 2 independent DD failures associated with the system components and it can be interpreted as the system transiting to state 6 when one of the two redundant components has a DD failure. The system transits back to the fully functional state 9 with repair rate, μ_{DD}, where repair of the failed component takes place. State 7 is similar to state 6, but the SIS has a DU rather than a DD failure. In the proposed model, the dangerous undetected failures can only be repaired during proof testing. The deterministic nature of the DU repair rate is reflected in Equations (8) and (9) and embedded within the Markov model. Noting the conclusion of the study conducted by Bukowski [40], the assumption of constant repair rates is justifiable.

From state 6 or 7 the system transits into state 3 or 4 when a process demand is levied on the system. In state 3 and 4, the SIS is responding to a process demand with only one component functioning since the other component is in failed status. The safety system alternates between states 3 and 6 (or, 4 and 7) depending on manifestation of a process demand or removal of the demand when it ends. Failure of the remaining component whilst the system is in state 3 or 4, results in system entering the hazardous state. Regardless of whether the dangerous failure of the remaining component is detected or undetected (DD or DU), the hazardous event occurs with the first failure. In state 8, the SIS 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 9. DD or DU failure of any of the components whilst the system is responding to a process demand in state 8, will lead to the system transition from state 8 to states 3 or 4, depending on whether the dangerous failure is detected or unknown until next proof test interval. If another dangerous failure arises either detected or undetected when one of the components is already failed in states 6 or 7, the system will move to one of the nodes 1, 2 or 5. Upon identification of the failed component and its repair in any of these states with μ_{DU} or μ_{DD} repair rate, the system transits to the previous states, 6 and 7 respectively. It is necessary to highlight that there is no process demand enforced on the system in any of the states 1 - 2 and 5 - 7.

The system enters hazardous state 0 from state 1 or 2 when a process demand occurs with λ_{DE} rate whilst both components are in failed states either due to two consecutive DD failures (9-6-1), two DU failures (9-7-2), or a combination of DD and DU failures (9-6-5 or 9-7-5). Alternatively the hazardous state 0 is reached from state 3 or 4 where system is responding to a process demand with the only remaining functional component (9-6-3, 9-8-3, 9-7-4 and 9-8-4) and it fails dangerously, either detected or undetected, resulting in removal of the protection layer and exposure to a hazardous event.

Similar to the 1oo1 system, 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 reinstated to “as good as new condition” in state 9. This is only achievable where the hazardous event is either repeatable or renewable as outlined by Youshiamura [41]. It is necessary to highlight that the abovementioned scenarios involve dangerous system failures only and do not entail CCF failures. Furthermore, it is assumed that only one component can be repaired at a time since only one maintenance team is available onsite. The primary property of any Markov process also known as Markov property is that the future status of the system depends on the current status of the system only and is independent of its past circumstances. This property is embedded within the Markov chain developed for the 1oo2 SIS as a memoryless system. Additionally, the system fulfils the secondary feature of Markov process recognised as stationary property in which the transition probabilities from one state to another state remain constant with time. As such, the steady state probabilities ($P_i, i = 0, \ldots, 9$) can be derived from the transition rate matrix. The steady state equations corresponding to the Markov transition diagram are as follows:

$$\begin{aligned}
&\mu_{DD}(P_6 - P_1) - (\mu_{DU}P_5 + \mu_{DE}P_3) = \lambda_{DD}(2P_9 - P_6) - (\lambda_{DE} + \lambda_{DU})P_6 \\
&\mu_{DU}(P_7 - P_2) - (\mu_{DD}P_5 + \mu_{DE}P_4) = \lambda_{DU}(2P_9 - P_7) - (\lambda_{DE} + \lambda_{DD})P_7 \\
&\mu_{DE}P_8 - (\mu_{DD}P_3 + \mu_{DU}P_4) = \lambda_{DE}P_9 - 2(\lambda_{DD} + \lambda_{DU})P_8 \\
&(\mu_{DE} + \mu_{DD})P_3 = 2\lambda_{DD}P_8 + \lambda_{DE}P_6 - (\lambda_{DD} + \lambda_{DU})P_3 \\
&(\mu_{DE} + \mu_{DU})P_4 = 2\lambda_{DU}P_8 + \lambda_{DE}P_7 - (\lambda_{DD} + \lambda_{DU})P_4 \\
&\mu_T P_0 = \lambda_{DE}(P_1 + P_2 + P_5) + (\lambda_{DD} + \lambda_{DU})(P_3 + P_4) \\
&(\mu_{DD} + \mu_{DU})P_5 = \lambda_{DU}P_6 + \lambda_{DD}P_7 - \lambda_{DE}P_5 \\
&\mu_{DU}P_2 = \lambda_{DU}P_7 - \lambda_{DE}P_2 \\
&\mu_{DD}P_1 = \lambda_{DD}P_6 - \lambda_{DE}P_1
\end{aligned} \tag{22}$$

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

$$\sum_{i=0}^{9} P_i = 1 \tag{23}$$

The 1oo2 SIS will not be able to respond to a process demand when it is in states 1, 2 or 5, therefore the PFD of the safety system is equivalent to:

$$PFD = P_1 + P_2 + P_5 \tag{24}$$

The frequency (per hour) of entering into the hazardous state from all possible states is:

$$HEF = \lambda_{DE}(P_1 + P_2 + P_5) + (\lambda_{DD} + \lambda_{DU})(P_3 + P_4) \tag{25}$$

A comparison between the Markov chains for 1oo1 and 1oo2 SIS configurations reveals that the number of nodes (corresponding to the number of steady state equations) has increased from 5 to 10 which results in a significant increase in the dimension of the transition rate matrix and subsequently computational effort required to solve the model. This highlights once more the difficulty associated with handling 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 [23].

5.0 Case Study

The Chemical Reactor Protection System (CRPS) shown in Figure 5 has been studied in [33,35] and is used for illustration of the newly developed model in this paper. The proposed Markov chain is applied to the protection system for calculating its unavailability against high temperature and/or high pressure produced within the chemical reactor and the frequency at which the system enters hazardous conditions. The reactor is a pressurised container deigned to process volatile hydrocarbon multiphase fluid which segregates gas and liquid products post completion of an exothermic reaction. This system is predominantly used in downstream process facilities such as refineries.

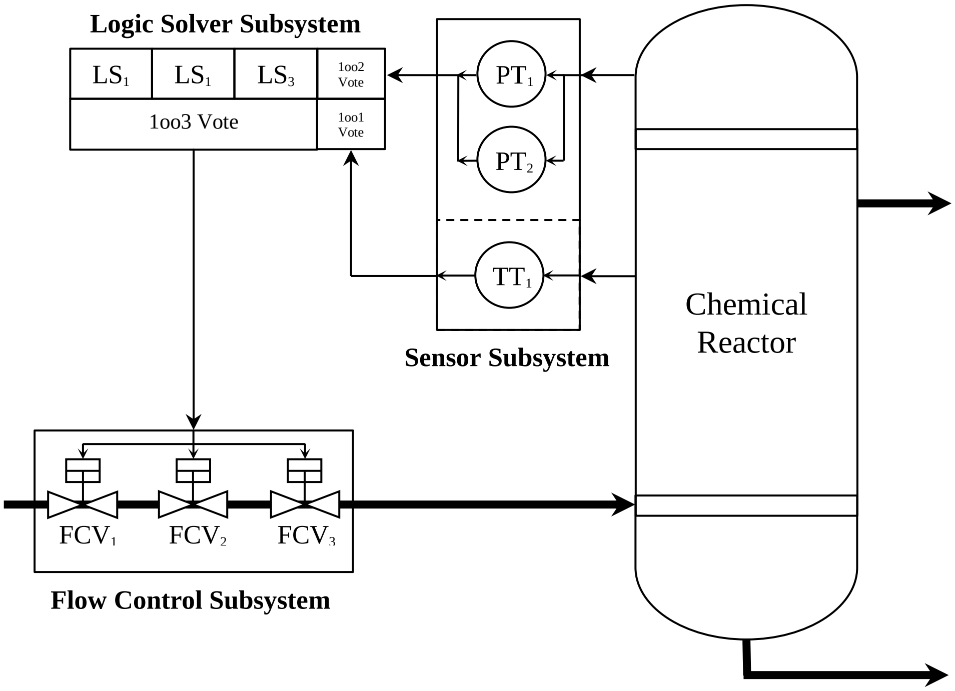

Figure 5 – CRPS Process Flow Diagram

5.1 High Integrity Pressure & Temperature Protection System

The protection system implemented to the chemical reactor consists of three distinct elements: sensor subsystem including pressure and temperature transmitters, logic solver subsystem and flow control subsystem. Upon detection of either high pressure or high temperature within the vessel, the final element shuts down the supply in order to prevent a runaway reaction [35]. Each subsystem is designed with sufficient level of redundancy encompassed within their configuration. The studied pressure and temperature safety system is composed of the following subsystems:

- The field instrumentation comprises of two independent sets of transmitters: Temperature Transmitter (TT) and Pressure Transmitter (PT); configured in 1oo1 and 1oo2 architectures respectively.
- The Logic Solver (LS) subsystem which is a programmable unit located in the control room and structured in 1oo3 redundant architecture.
- The Flow Control (FC) subsystem structured in 1oo3 architecture made up of three Flow Control Valves (FCVs) and their associated actuators.

5.2 Hazardous Event

Where pressure or temperature within the reactor exceeds the defined design envelop, the SIS shuts down the incoming flow and maintains the safe status of the equipment under control. The reactor is neither connected to the flare system nor provided with an atmospheric release. As such, the high integrity SIS is the last and only layer of protection safeguarding the reactor against extreme pressure and/or temperature. Failure of the SIS will lead to rupture of the reactor and subsequent loss of containment.

It is assumed that loss of containment will be contained within a dedicated dike and subsequently drained via the plant’s closed drain system. Both dike and drain system are suitably designed to accommodate full release of reactor containment. The drain system directs the excess fluids into a separate container and as such eliminates personnel exposure to toxic / flammable fumes and also minimises environmental damage so far as reasonably practicable. Furthermore, the existing plant fire and gas detection system is deemed as sufficient in detecting the gas cloud resulting from the loss of containment and to initiate a high level executive action to shutdown the plant and isolate all energy feeds which could act as potential ignition sources. Therefore, fire and explosion are discounted from the potential range of consequences and the ramification of the hazardous event is limited to minor to moderate asset damage only with no safety and environmental impact perceived. Noting the aforementioned, the hazardous event for this case is considered as repeatable or renewable [41] only.

5.3 Process Demand

Process demand on the SIS will be triggered by uncontrolled liquid level resulting in pressure spike within the reactor. Alternatively, process demand is generated due to excessive pressure and/or temperature, released as a result of exothermic chemical reaction within the vessel. The underlying cause for the later could be due to change in composition of the upstream fluid.

5.4 Calculation of System Unavailability

5.4.1 Overall Model

The reliability block diagram of the CRPS is illustrated in Figure 6. In order to compute the system unavailability, the proof test interval associated with test frequency of the SIS is required to be established. Some applications require the use of different test intervals of each subsystem of the CRPS, however in this study we assume that all subsystems are tested independently of each other at the their own proof test interval of τ_i. Thus, the complexity of the SIS does not increase as each subsystem can be studied independently.

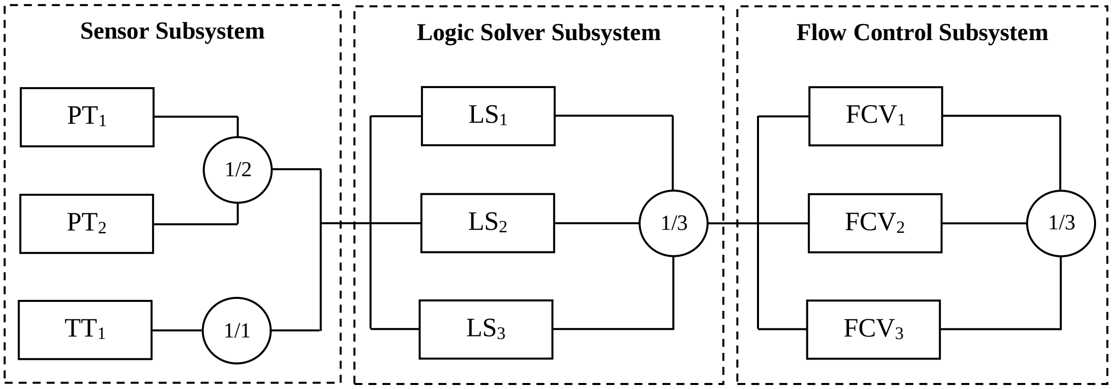

Figure 6 – CRPS Reliability Block Diagram

The unavailability of SIS individual subsystems for the CRPS was calculated as follows:

- The 1oo1 temperature transmitter and 1oo2 pressure transmitter sensor subsystems were analysed using the proposed unavailability models presented in this paper;
- The 1oo3 logic solver and 1oo3 flow control subsystems were solved using the simplified formula from IEC 61508.

The overall system unavailability can be calculated by the combination of probability of failure on demand of all the three subsystems providing the safety function. It is expressed by the following expression:

$$PFD_{CRPS} = (PFD_{TT}.PFD_{PT}) + PFD_{LS} + PFD_{FC} \tag{26}$$

The PDS handbook [42] provides the following estimates for individual components of the CRPS (topside equipment):

Table 4 – CRPS Reliability Data

Parameters	**Unit**	PT_i	TT_i	LS_i	FC_i
λ_{DU}	$\times 10^{-6}/h$	0.3	0.3	0.8	3.5
DC	$-$	0.6	0.6	0.9	0.2
$MTTR$	h	8	8	8	8
τ	h	8,760	8,760	17,520	17,520

It is assumed that the logic solver subsystem is a control logic unit programmable safety system which consists of an analogue input, a single processing unit (CPU) / logic and a digital output configuration. The failure rates associated with the flow control valves are related to shutdown service only (i.e. normally not operated). The failures rates of the actuators, pilot / solenoid valve etc are excluded from this analysis. The $MTTR$ value for all SIS components is set at 8 hours, consistent with the IEC 61508 [1] recommended value. In addition, it is assumed that various independent upstream and downstream protection layers are incorporated within the design of the process system leading to a low frequency of process upset which may generate demand on SIS. Where a demand is inflicted on the SIS, it is expected to be a short duration given the nature of system operability. Thus, the process demand rate and its duration are considered as $\lambda_{DE} = 1 \times 10^{-5}$ and $\mu_{DE} = 1 \times 10^{-4}$ per hour respectively. The restoration rate from hazardous event is also projected as $\mu_T = 1 \times 10^{-3}$ per hour [24] which is equivalent to 1000h mean restoration time after a hazardous event. This estimate is deemed appropriate as we are addressing repeatable and/or renewable hazardous event only, although the severity of the consequence dominates this value.

5.4.2 Analysis of Sensor Subsystem

The sensor subsystem consists of two independent initiators, temperature transmitter and pressure transmitter. The temperature transmitter subsystem is a 1oo1 system and as such can be analysed using the Markov chain presented in Figure 3. The interval between proof tests for the TT subsystem 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. Using $\tau = 8{,}760$h and $MTTR = 8$h, the repair rate of dangerous undetected for temperature transmitter is calculated as $\mu_{DU} = 2.28 \times 10^{-4}$ per hour, as per Equation (8). The pressure transmitter subsystem is a 1oo2 redundant system and can be analysed using the Markov chain presented in Figure 4. Similarly, the repair rate of dangerous undetected for pressure transmitter is calculated as $\mu_{DU} = 3.42 \times 10^{-4}$ per hour, as per Equation (9). The state equations were solved using MATLAB for both temperature and pressure transmitter subsystems corresponding to 1oo1 and 1oo2 models presented in this paper. Since the reliability data sets are identical for both subsystems, the results are comparable. The calculated PFD and HEF values are outlined in Table 5:

Table 5 – Analysis of Sensor Subsystem

Performance Indicator	1oo1 SIS	1oo2 SIS
PFD	1.15×10^{-3}	1.36×10^{-6}
HEF	7.46×10^{-8}	1.25×10^{-10}

The PFD for 1oo2 SIS is lower than 1oo1 by 3 orders of magnitude indicating a considerably more available system in comparison with a simple SIS. The redundant SIS enters hazardous event with a lower frequency when compared to the simple system, resulting in significant enhancement in safety performance of the system. This is also an advantage of utilising a redundant configuration as opposed to a single transmitter system with no redundancy. These outcomes are in line with the general philosophy that utilising a redundant architecture will reduce the unavailability and improve the safety performance of the system.

There is a distinction between the sensor subsystem and the other two elements of the SIS (i.e. logic solver and flow control subsystems) in Figure 5. In the case study conducted in this paper the process demand imposition only occurs on the sensors due to rise in pressure / temperature as a result of exothermic chemical reaction. Whereas the SIS logic solver and flow control subsystems in this case only facilitate the discharge of the safety function if the operation conditions exceed design envelops. As such, the Markov model presented in this paper was only applied to the sensor subsystems due to direct impact of the process demand.

5.4.3 Analysis of Protection System

The unavailability of 1oo3 logic solver and flow control subsystems can be calculated in accordance with IEC 61508 [1]. Since there is no direct process demand imposition on the logic solver and flow control subsystems, the IEC 61508 simplified formula is deemed as sufficient in providing a reasonably accurate approximation for the PFD values of these elements. Taking into account that the common cause failure is discarded in this study and assuming that any diagnostic testing would only report the faults identified and will not change the output states or the voting logic, the average probability of failure on demand for the 1oo3 architecture provided by the IEC 61508 standard can be simplified as follows:

$$PFD_{LS/FC} = 6(\lambda_{DD} + \lambda_{DU})^3 \prod_{n=2}^{4} \left[\frac{\lambda_{DD}}{\lambda_D} MTTR + \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{n} + MRT\right)\right] \tag{27}$$

The Mean Repair Time (MRT) is presumed identical to the MTTR considering that the repair is commenced instantaneously upon detection and the delay time associated with logistics is annulled. In this case if $\lambda_D MTTR \ll 0.1$, one can justify that $(\lambda_{DU}\tau)^3/4$ is a good approximation [43] to the value of PFD for the logic solver and flow control subsystems. Considering that the Markov model assumes 100% detection rate during proof tests, the elimination of proof test coverage and consequently use of approximate formula is justified and in line with the requirements of international standards IEC 61508.

The overall unavailability of the protection system is calculated as 5.83×10^{-5} corresponding to safety integrity level 4. It shall be noted that the sensor subsystems form minimal portion of system unavailability in comparison with final elements of the protection system as presented in Figure 7 for the CRPS subsystems. This is predominantly due to the technological variation between detection of process abnormality versus mechanical completion of an executive action i.e. closure of the flow control valves. Therefore, where changing in test frequency of the components is deemed feasible, the final elements shall be given a higher priority.

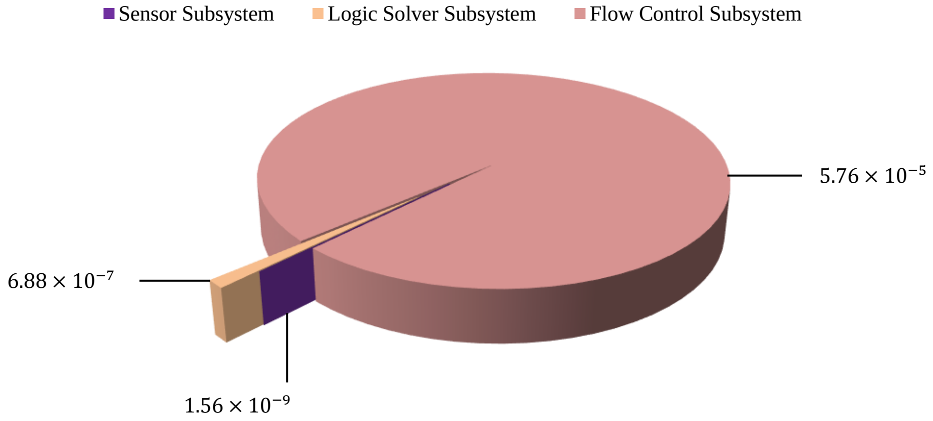

Figure 7 – Comparative Unavailability of Chemical Reaction Protection Subsystems

Exclusion of proof test coverage where perfect detection rate during the proof test is not achievable for the sensor subsystem may give slightly optimistic result but not prevailing in determination of overall system unavailability noting that the large portion of the system unavailability is dominated by final elements. Therefore, the impact of the PTC is negligible for the sensor subsystem and will not lead to unsafe results.

5.4.4 Impact of Proof Test Interval on Unavailability

The optimisation of proof test interval during SIS lifecycle is always a stimulating topic for functional safety engineers. Whilst the reduced proof text intervals will generally result in reduction of SIS unavailability, the expenditure associated with conducting the proof tests including labour, equipment and cost of shutdown will be determining factors. As such, a balance between expenditure and maintaining system integrity is required to be established. The behaviour of proposed 1oo1 and 1oo2 SIS models against various proof test intervals, τ, are shown in Figure 8 and Figure 9. The proof test intervals used for illustration purpose cover shorter periods consisting of 1, 2, 3, 6 and 12 month intervals as well as longer durations including 1.5, 2, 3, 5 and 10 years. It is observed that the unavailability of both 1oo1 and 1oo2 systems elevates gradually alongside the proof test duration, although the increase in 1oo2 system unavailability is steeper. The unavailability of redundant configuration is substantially lower than the simple structure, reflecting the prominence of redundancy.

In order to illustrate the visit frequency to hazardous event we use -$\log_{10}$ scale on the y-axis, hence any increase in HEF, results in acquisition of lower values. Although the frequency of 1oo1 system entering hazardous state is relatively constant throughout the 10 test intervals as shown in Figure 9, increase in hazardous event frequency for 1oo2 system is clearly visible in the same range. Nevertheless, the hazardous event frequency for a redundant 1oo2 configuration remains extensively lower than a simple 1oo1 system.

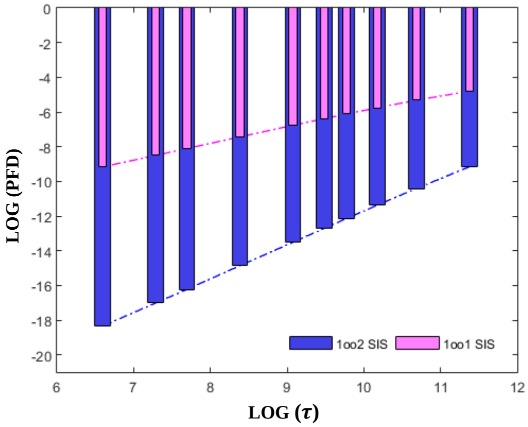

Figure 8 – PFD comparison of 1oo1 vs 1oo2 SIS with varying τ value

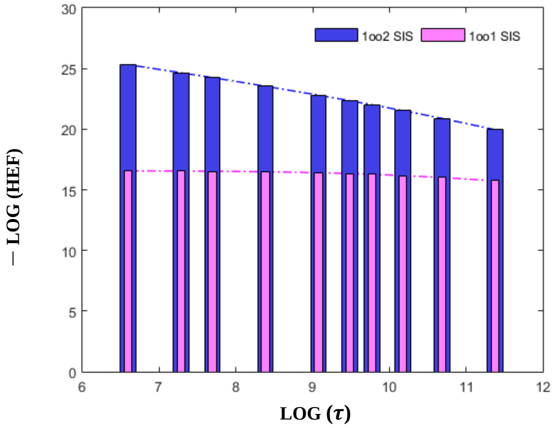

Figure 9 – HEF comparison of 1oo1 vs 1oo2 SIS with varying τ value

The minimum SIS proof test interval may not be achievable as other influencing elements play a significant role in determination of the optimum test interval. This is despite the augment of unavailability and hazardous event frequency resulting in deterioration of the system performance. The above illustration indicates that the proposed 1oo2 SIS model is in line with the anticipated trend in comparison with 1oo1 simple system.

5.5 Sensitivity Examination of 1oo2 SIS

5.5.1 The effect of λ_{DE} and μ_{DE}

We now examine the effect of varying process system parameters including the demand rate and demand duration. First we study the effect of varying the demand rate, λ_{DE}. As such the demand duration, μ_{DE}, is considered as a constant in this step. The effect of varying λ_{DE} on the PFD and HEF are evaluated for demand durations equal to 10^{-6}, 10^{-5}, 10^{-4}, 10^{-3} and 10^{-2} respectively. In order to illustrate the probability of failure on demand and visit frequency to hazardous state in a common figure we use logarithmic scale on both the x-axis and y-axis. The PFD and HEF are functions of λ_{DE} for the specified duration of demands as seen in Figure 10 and Figure 11 respectively.

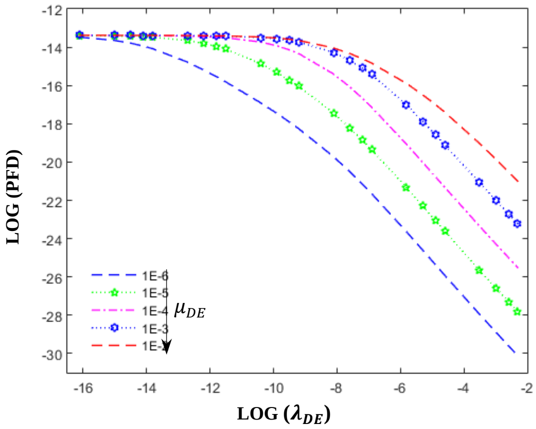

Figure 10 – PFD verses λ_{DE} with varying demand durations for a 1oo2 SIS system

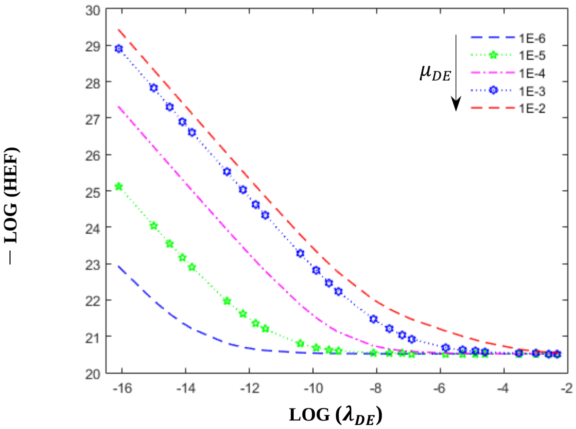

Figure 11 – HEF verses λ_{DE} with varying demand durations for a 1oo2 SIS system

Increase in process demand means shifting from low demand mode of operations to high demand mode where safety instrumented system has to respond more frequently to demands from the process system. Although the model proposed in this paper is solely focused on low demand mode of operation, the increase in process demand is evaluated to analyse behaviour of the system in those scenarios. From Figure 10 the PFD descends as the demand rate rises for various μ_{DE}. It is however observed that the change in PFD value is not apparent for less frequent process demand rates across the selected range of demand durations. This behaviour can be justified considering that when the demand frequency increases, the system will respond to the process demand more frequently. Therefore, the SIS function is discharged regularly resulting in revealing DU failures. Hence, the system unavailability due to undetected dangerous failure will reduce, leading to a reduction in PFD value. The frequency of visiting the hazardous state increases whilst λ_{DE} obtains higher values for a 1oo2 SIS as per Figure 11. This is due to dominant impact of λ_{DE} in Equation (25) that dictates an increase in HEF despite reduction of PFD.

To study the influence of demand duration, the demand rate, λ_{DE}, is considered to be constant. Calculations are performed for five different values of demand rates including 10^{-7}, 10^{-6}, 10^{-5}, 10^{-4} and 10^{-3}. The results of these calculations are illustrated in Figure 12 and Figure 13 representing the effect of varying demand rates on the PFD and HEF in turn. The unavailability increases as the demand duration reduces according to the result shown in Figure 12. This might be predicted by the following argument: as the demand duration reduces (demand reset rate rises), the system devotes lower portion of time in responding to the process demand in states 3, 4, and 8 in Figure 4, hence resulting in higher possibility of system conveyancing to the remaining system states including 1, 2 and 5. This leads to higher system unavailability considering that the PFD for 1oo2 SIS is defined as per Equation (24). As the demand duration reduces, the HEF descends in Figure 13 indicating improvement in SIS safety performance for all λ_{DE} values. The frequency of system entering hazardous event shows minute sensitivity to changes in demand duration for more frequent demand rates.

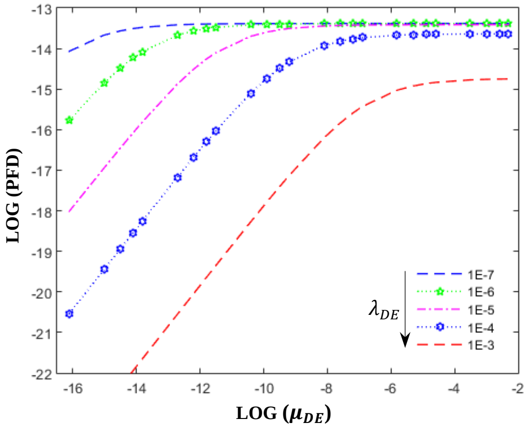

Figure 12 – PFD verses μ_{DE} with varying demand rates for a 1oo2 SIS system

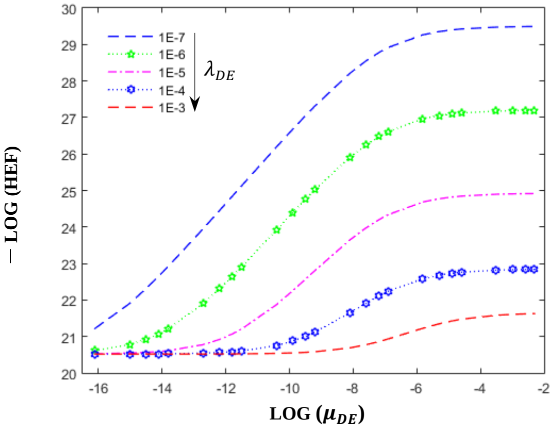

Figure 13 – HEF verses μ_{DE} with varying demand rates for a 1oo2 SIS system

The outcome of this sensitivity investigation is consistent with the observations of Liu et al. [24] for the effect of λ_{DE} and μ_{DE} on a 1oo2 Pressure Relive Valve (PRV) system in which both the PFD and HEF exhibit a similar trend.

5.5.2 The effect of λ_{DU} and μ_{DU}

To explore the impact of DU failure rate, λ_{DU}, on PFD and HEF, we assume μ_{DU} as a constant and repeat the analysis when DU repair rate equals to 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2} and 10^{-1}. Where the component failure rate increases, the system will be less available to respond to process demand and this is obvious in Figure 14. The PFD for the selected range of μ_{DU} ascend sharply and congregate at 100% unavailability as the DU failure rate gains higher values. 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, reducing system availability to respond to process demand. The HEF curves converge and remain constant for higher DU failure frequencies across the designated values for μ_{DU}.

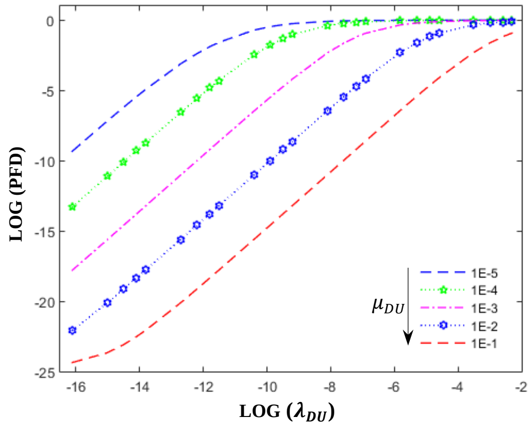

Figure 14 – PFD verses λ_{DU} with varying DU repair rates for a 1oo2 SIS system

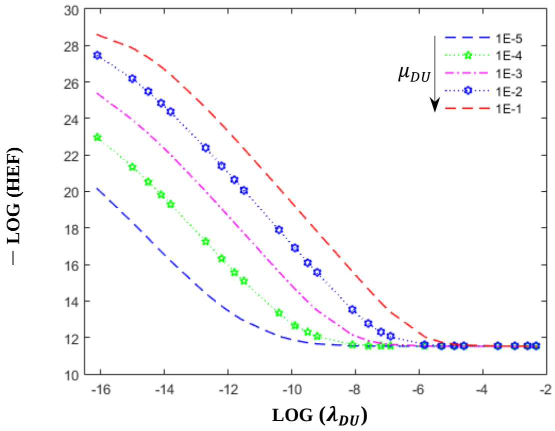

Figure 15 – HEF verses λ_{DU} with varying DU repair rates for a 1oo2 SIS system

The behaviour of the 1oo2 redundant system with regards to the effect of DU failure rate, λ_{DU}, is compatible with 1oo1 simple system. Using the principle of IEC 61508 [1] for a low demand system, the PFD and the visit frequency of 1oo1 SIS should be equal to the standard low demand formulae when the mean duration of the demands is smaller than the test interval. These values are approximately [1,24]:

$$PFD \approx {}^{1}/_{2}\,(\tau.\lambda_{DU}) \quad \text{and} \qquad HEF \approx PFD.\lambda_{DE} \tag{28}$$

According to the Equation (28) any adjustment in DU failure rate will directly result in increase or decrease in unavailability of SIS and subsequently in visit frequency. This pattern is consistent with the observation made in Figure 14 and Figure 15 as interpreted above which display similar pattern of behaviour in 1oo1 and 1oo2 systems.

In order to interrogate the effect of DU repair rate, μ_{DU}, on SIS performance indicators, we consider λ_{DU} to be a constant. The sensitivity examination was conducted for a diverse range of λ_{DU} consisting of 10^{-7}, 10^{-6}, 10^{-5}, 10^{-4} and 10^{-3} consecutively. Increase in repair rate is deemed as an improvement in system performance since higher repair rate leads to reduced system unavailability and Figure 16 proves this effect. It can be seen that the PFD decreases as DU repair rate increases. The PFD improvement is more evident for lower values of DU failure rates at 10^{-7} and 10^{-6} but limited disparity is witnessed when λ_{DU} is fluctuating between 10^{-5} and 10^{-3}. The HEF curves generated in Figure 17 against μ_{DU} for varying DD failure rates show a similar pattern which is an emphasis on this model behaviour. Due to the enhanced repair rate, the system is less exposed to hazardous event therefore reduction in HEF can be realised for almost all values of DU failure rate in this figure. Although there is no notable change in system visiting the hazardous event for DU failure rate equivalent to 10^{-3} against variation in DU repair rate.

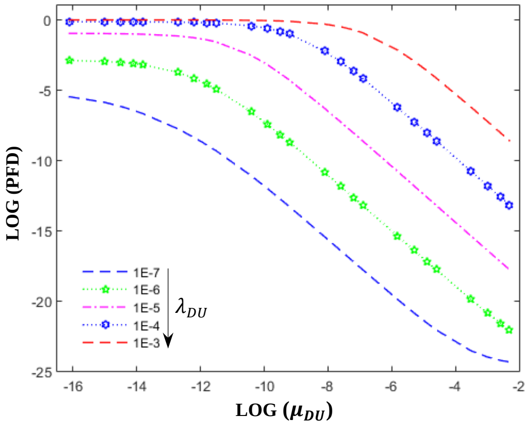

Figure 16 – PFD verses μ_{DU} with varying DU failure rates for a 1oo2 SIS system

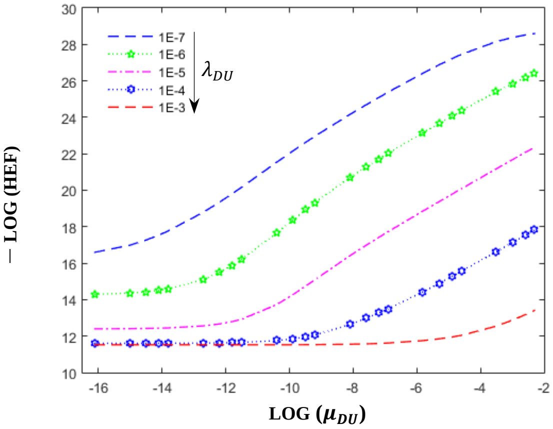

Figure 17 – HEF verses μ_{DU} with varying DU failure rates for a 1oo2 SIS system

Review of Figure 14 – Figure 17 shows the worst SIS performance as the combination of high DU failure rate and low DU repair rate which results in substantial unavailability of the high integrity pressure and temperature protection system and frequent visits to hazardous state. When designing a SIS this combination shall be avoided, otherwise the effectiveness of SIS as an independent layer of protection will be compromised.

5.5.3 The effect of λ_{DD} and μ_{DD}

For completion of the sensitivity analysis the effect of varying the component DD failure rates, λ_{DD}, and DD repair rates, μ_{DD} are also studied in this paper. We first examine the effect of varying DD failure rate by considering μ_{DD} as a constant. The analysis were carried out for μ_{DD} equal to $^1/_{10}$, $^1/_8$, $^1/_6$, $^1/_4$ and $^1/_2$. The system unavailability is constant for lower values of DD failure rate across the range of μ_{DD} and deteriorates sharply whilst the DD failure rate acquires higher values as shown in Figure 18. No considerable change between various values of DD repair rate is observed as λ_{DD} attains higher frequencies. The system visit frequency to hazardous event is demonstrated in Figure 19. The concurrent increase in HEF and DD failure rate is perceived in this figure although no notable change in HEF across the designated range of μ_{DD} is identified.

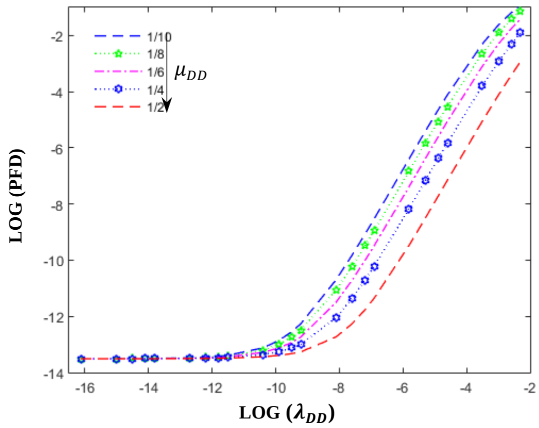

Figure 18 – PFD verses λ_{DD} with varying DD repair rates for a 1oo2 SIS system

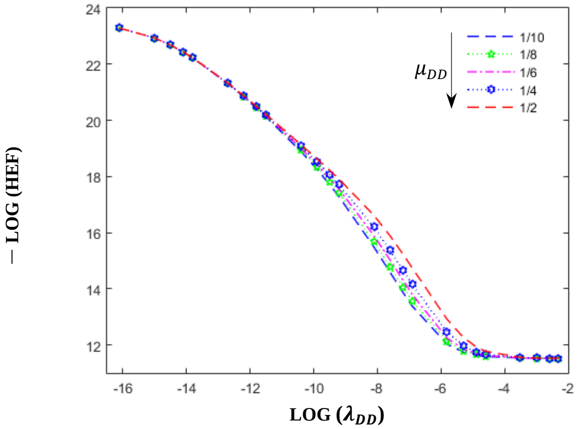

Figure 19 – HEF verses λ_{DD} with varying DD repair rates for a 1oo2 SIS system

In order to review the impact of varying DD repair rate, μ_{DD}, we assume that DD failure rate, λ_{DD}, is a constant. The assessment was completed for λ_{DD} values of 10^{-7}, 10^{-6}, 10^{-5}, 10^{-4} and 10^{-3}. Similar to the μ_{DU} inclination, increase in DD repair rate will result in enhancement of system availability and reduction in PFD as shown in Figure 20, though this reduction is not largely distinguished. The PFD curves overlap for λ_{DD} alternating between 10^{-7} – 10^{-5} which illustrates that the system is independent of variation in DD repair rates for lower DD failure frequencies. A substantial rapid rise in unavailability is however recognised when λ_{DU} is equivalent to 10^{-3} where PFD reduces as the DD repair rate rises. This feature is also mirrored in the system entering the hazardous event in Figure 21 where higher HEF is produced by greater values of λ_{DD}. The HEF shows negligible variation against change in μ_{DD} for lower values of DD failure rate but demonstrates a reduction in the system visit frequency to hazardous state for higher λ_{DD}. The behaviour of system PFD and HEF versus DD failure rates, λ_{DD}, and its repair rate, μ_{DD}, is in line with the overall expectation of SIS performance for 1oo2 redundant configurations.

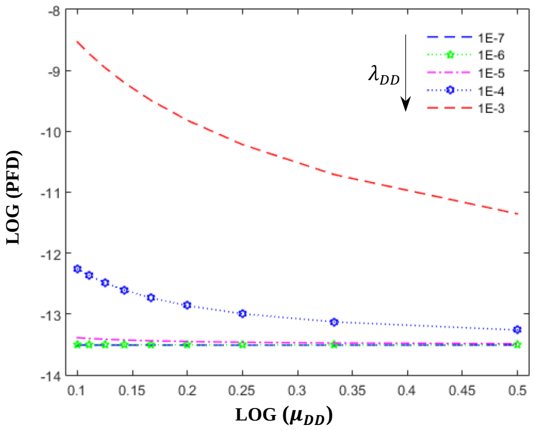

Figure 20 – PFD verses μ_{DD} with varying DD failure rates for a 1oo2 SIS system

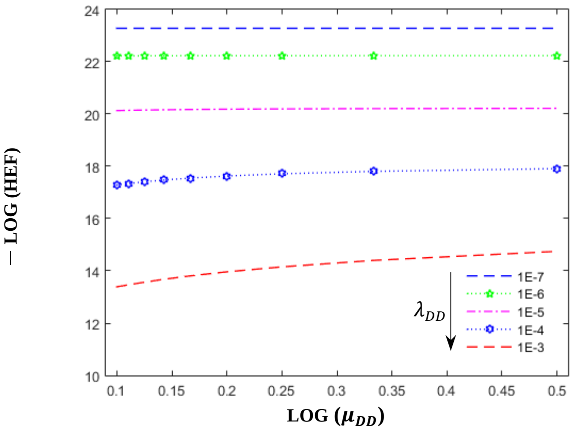

Figure 21 – HEF verses μ_{DD} with varying DD failure rates for a 1oo2 SIS system

6.0 Conclusions

This paper has presented a new unavailability model for a redundant safety instrumented system using Markov chains approach. The main objective of this article was to develop a new model for a 1oo2 SIS in low demand mode of operation based on an established simple 1oo1 simple system. This model incorporates process demand inflicted on the SIS in conjunction with established system failure modes such as dangerous detected and undetected failure rates. Two measures have been utilised namely the probability of failure on demand and the hazardous event frequency to measure the unavailability and safety performance of the model. The present paper focusses on comparing architectures, noting that proof test coverage and common cause failures are omitted, and leading to optimistic results. This may not be sufficient to satisfy the IEC requirements for PFD calculation whilst remaining compliant. Although this assumption limits the application of the proposed model, it is considered as a step forward towards the unavailability modelling of safety instrumented systems subject to process demand using Markov chains. The simultaneous consideration of SIS primary failure modes (dangerous detected and dangerous undetected) and process demand (demand rate and demand duration) is the main advantage of Markov modelling as this is not achievable by traditional reliability tools such as RBD and FTA. Hence, the utilisation of Markov model to its full advantage is implemented in the proposed model.

The validity of the model introduced in this research was examined in a case study of protection system for a pressurised chemical reactor containing volatile hydrocarbon multiphase fluid. A comparison of 1oo1 vs 1oo2 configuration for sensor subsystem demonstrates an improvement of the system performance due to the introduction of a redundant element within the safety instrumented system. This verifies that utilisation of a redundant architecture not only reduces unavailability but also improves the safety performance of the system, resulting in lower frequency of system visiting hazardous state. The behaviour of the 1oo2 SIS was further examined by performing sensitivity analysis against various model parameters including demand rate and demand duration as well as component failure rates (DD and DU) and the associated repair rates. The results confirm that the model behaviour against variation in parameters is consistent with the overall expectation of SIS performance for a redundant 1oo2 configuration.

It is to be noted that the assumption about system restoring from the hazardous state to the “as good as new” state, was made to calculate 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 dissolve in the computational details, but this has not been pursued any further and may be a topic for further work. At the same time, it would be of great interest to study the effects of common cause failure in a 1oo2 safety instrumented system which is subject to process demand as well as inaccuracy of the proof test where deemed practical. These are also new topics for further research.

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

τ	proof test interval
$p_{ij}(t)$	system transition probability from state i to state j
a_{ij}	transition rate from state i to state j
A	transition rate matrix
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
μ	component repair rate
μ_{DD}	dangerous detected repair rate
μ_{DE}	demand reset rate
μ_{DU}	dangerous undetected repair rate
μ_T	renewal rate
π_i	steady state probability of system in state i
Π	steady state probabilities matrix
DC	diagnostic coverage rate
$P(t)$	transition matrix at time t
$P_i(t)$	probability of system in state i at time t
$\acute{P}_i(t)$	time derivative probability of system in state i at time t
r	states of stochastic process
β_D	detected common cause failure factor

β_U undetected common cause failure factor

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] IEC 62425, Railway applications – communication, signalling and processing systems – safety related electronic systems for signalling. Geneva: International Electrotechnical Commission; 2007.

[4] ISO/DIS 26262, Road vehicles – functional safety, Parts 1 – 10. Geneva: International Organization for Standardisation; 2009.

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

[6] Yun G, Rogers WJ, Mannan MS. Risk assessment of LNG importation terminals using the Bayesian-LOPA methodology. J Loss Prev Process Ind 2009;22:91–6.

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

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

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

[10] 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.

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

[12] Bukowski JV. Incorporating process demand into models for assessment of safety system

performance. Proc. RAMS’06 Symp., Alexandria, VI, USA: 2006, p. 577–81.

[13] 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.

[14] 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.

[15] Zhang Y, Dai J, Zhu D. Calculation of the Probability of Failure on Demand of Redundant Systems Using Markov Model. Inf Technol J 2013;12:5477–81.

[16] Wang Y, Rausand M. Reliability analysis of safety-instrumented systems operated in high-demand mode. J Loss Prev Process Ind 2014;32:254–64.

[17] Chen Y. Reliability analysis of a fire alarm system. Procedia Eng., vol. 24, 2011, p. 731–6.

[18] Guo H, Yang X. Automatic creation of Markov models for reliability assessment of safety instrumented systems. Reliab Eng Syst Saf 2008;93:829–37.

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

[20] Signoret JP, Dutuit Y, Cacheux PJ, Folleau C, Collas S, Thomas P. Make your Petri nets understandable: Reliability block diagrams driven Petri nets. Reliab Eng Syst Saf 2013;113:61–75.

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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] Hauge S, Hokstad P, Langseth H, Hauge S, Onshus T. Reliability prediction method for safety instrumented systems. Trondheim: SINTEF; 2010.

[27] Bukowski JV. Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems. IEEE Trans Reliab 2001;50:321–9.

[28] Innal F, Dutuit Y, Rauzy A, Signoret J-P. New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. Proc Inst Mech Eng Part O J Risk Reliab 2010;224:75–86.

[29] 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;66:145–8.

[30] Torres-Echeverría AC, Martorell S, Thompson HA. Multi-objective optimization of design and testing of safety instrumented systems with MooN voting architectures using a genetic algorithm. Reliab Eng Syst Saf 2012;106:45–60.

[31] Smith DJ. Reliability, maintainability and risk. 7th ed. Oxford: Butterworth-Heinemann; 2001.

[32] Jin H, Lundteigen M a., Rausand M. Uncertainty assessment of reliability estimates for safety-instrumented systems. Proc Inst Mech Eng Part O J Risk Reliab 2012;226(6):646–55.

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

[34] Mechri W, Simon C, BenOthman K, Benrejeb M. Uncertainty evaluation of Safety Instrumented Systems by using Markov chains. Proc. 18th Int. Fed. Autom. Control World Congr., Milano, Italy: 2011, p. 7719–24.

[35] Torres-Echeverría AC, Martorell S, Thompson HA. Modelling and optimization of proof testing policies for safety instrumented systems. Reliab Eng Syst Saf 2009;94:838–54.

[36] Todinov M. Reliability and risk models: Setting reliability requirements: Second edition. Chichester, UK: John Wiley & Sons, Ltd; 2015.

[37] Beichelt FE, Fatti LP. Stochastic Processes and Their Applications. CRC Press, Taylor & Francis Group; 2001.

[38] 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.

[39] Mechri W, Simon C, Bicking F, Ben Othman K. Fuzzy multiphase Markov chains to handle uncertainties in safety systems performance assessment. J Loss Prev Process Ind 2013;26:594–604.

[40] Bukowski J V. Using Markov Models to Compute Probability of Failed Dangerous When Repair Times Are Not Exponentially Distributed. Proc. Annu. Reliab. Maintainab. Symp., Newport Beach, CA, USA: 2006, p. 273–7.

[41] 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 – 386.

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

[43] Bukowski J V. A comparison of techniques for computing PFD average. Proc. Annu. Reliab. Maintainab. Symp., Alexandria, VA, USA: 2005, p. 590–5.