# Effect of demand rate on evaluation of Spurious Trip Rate of a SIS

Thao Dang, Michael Schwarz, and Josef Börcsök

***Abstract*—**A spurious trip is one cause of an unexpected plant shutdown initiated by a safety-instrumented system (SIS). Therefore, spurious activation normally leads to lost production or low availability of the EUC. Some of the spurious activations can lead to a hazardous state and so the plant cost can be extremely increased. On these foundations the modeling of spurious activations in safety-instruments systems (SIS) has been studied for over ten years and in different industry branches, for example: nuclear industry, offshore-onshore industry, process industry, etc.…. In line with the important standard IEC 61508, SISs are generally classified into two types: low-demand systems and high-demand systems. This article focuses on the estimation of “spurious trip rate” (STR) and “mean time to failure spurious” ($MTTF_{Spurious}$) for these two different system modes. The research is based on block diagrams and the Markov model and is exemplified by two system configurations: 1oo1 and 1oo2.

***Keywords*—**demand rate, $MTTF_{Spurious}$, spurious trip rate, 1oo1, 1oo2.

## I. Introduction

Safety-instrumented systems (SISs) are widely used in the process industry to respond to hazardous events and unwanted events. If a hazardous situation occurs within an EUC (Equipment Under Control) and is detected, a demand is sent to the safety system with a rate $\lambda_{DE}$. This demand serves to activate the safety function to achieve the EUC in safe state (Fig. 1).

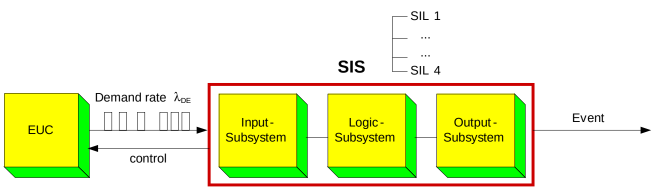


Fig. 1 EUC and SIS [14], [15]

The demand rate is not defined in standard IEC 61508 [1], but defined in the standard prEN ISO 13849-1 (2004) [17] as a frequency of demands for a safety-related action of a safety related part of a control system (SRP/CS).

N.T. Dang Pham was with Department Computer Architecture and System Programming University of Kassel, Germany.

Prof. Dr. Michael Schwarz is with Department Computer Architecture and System Programming, University of Kassel, Germany (e-mail: m.schwarz@uni-kassel.de)

Prof. Dr. habil. Josef Börsök is with Department Computer Architecture and System Programming, University of Kassel, Germany (e-mail: j.boersoek@uni-kassel.de).

According to the important standard IEC 61508 [1], SISs are classified into two types: low-demand systems and high-demand systems. A low-demand SIS has a frequency of demands not more than once per year and not more than twice the proof test frequency. Else, the SIS is considered as a high-demand system. However, there are no further discussions about the distinction between low- and high-demand systems. There is only a discussion about the difference of the reliability evaluation between systems: Probability of Failure on Demand (PFD) for low-demand systems and Probability of Failure per Hour (PFH) for high-demand systems.

The SIS can be regarded from one of two different perspectives: safety or availability. From the point of view of a safety perspective a SIS can be evaluated by some important safety parameters such as PFD, PFH, MTTF (Mean Time To Failure). And other parameters like STR, $MTTF_{Spurious}$, PFS (Probability of Failure Safe) are commonly calculated for a SIS with availability perspective. Whereas the safety integrity levels (SIL) are defined in the standard IEC 61508 [1] to provide a measure of how often a function fails to operate when required (Table 1), spurious trip levels (STL) are defined in [5], [6] to measure how often a function is carried out when not required (Table 2). The more financial damage the spurious trip can cause, the higher the STL of the safety function should be.

TABLE I
Safety Integrity Level [1]

| SIL | PFDavg | PFH |
|---|---|---|
| 1 | $\geq 10^{-2}$ to $<10^{-1}$ | $\geq 10^{-4}$ to $<10^{-5}$ |
| 2 | $\geq 10^{-3}$ to $<10^{-2}$ | $\geq 10^{-7}$ to $<10^{-6}$ |
| 3 | $\geq 10^{-4}$ to $<10^{-3}$ | $\geq 10^{-8}$ to $<10^{-7}$ |
| 4 | $\geq 10^{-5}$ to $<10^{-4}$ | $\geq 10^{-9}$ to $<10^{-8}$ |

TABLE II
Spurious Trip Level™ [5], [6]

| STL | Probability of Failure Safe Per Year | Spurious Trip Cost |
|---|---|---|
| X | $\geq 10^{-(x+1)}$ to $<10^{-x}$ | … |
| … | … | … |
| 5 | $\geq 10^{-6}$ to $<10^{-5}$ | 10M€ - 20M€ |
| 4 | $\geq 10^{-5}$ to $<10^{-4}$ | 5M€ - 10M€ |
| 3 | $\geq 10^{-4}$ to $<10^{-3}$ | 1M€ - 5M€ |
| 2 | $\geq 10^{-3}$ to $<10^{-2}$ | 500k€ - 1M€ |
| 1 | $\geq 10^{-2}$ to $<10^{-1}$ | 100k€ - 500k€ |

The SIS reliability is analyzed by different methods, like reliability block diagrams [2], Markov models [3], approximation formulas [8], Monte Carlo simulation [20], etc. Most of the references focus on low-demand systems and do not take high-demand systems into consideration as well as the borderline between two SIS types. Some authors suggest to incorporate the rate of demands into the analysis by using the Markov model [11], [8], [12]. However, H. Jin, M.A Lundteigen and M. Rausand [10] listed some criterion in the quantification of the SIS reliability performance (PFD and PFH) and presented modeling issues for this quantification for both demand modes. Issues like demand rate, demand duration make the difference between low-demand and high-demand systems. The borderline between theses system modes is discussed and shown by the quantification of SIS reliability with Markov modeling [10], [13]. But this borderline has not been considered for the evaluation of a SIS from an availability perspective. STR and $MTTF_{Spurious}$ have been commonly calculated for a low-demand system.

The main purpose of this article is to verify the difference between low-demand and high-demand systems for de-energized to trip application by using the block diagram and the Markov method for the STR and $MTTF_{Spurious}$ calculation. This paper is organized as follows: section 2 discusses the definition and causes as well as the characteristics of spurious activation. In section 3 the differences between low-demand and high-demand systems are described. In the next sections, section 4 and 5, the evaluation of spurious trip rate and $MTTF_{Spurious}$ of these system modes is studied for 1oo1 and 1oo2 systems. The analysis is based on block diagram and Markov model. In the section 6 the safety parameters like PFS, STR and $MTTF_{Spurious}$ of 1oo1- and 1oo2-architectures are calculated through an example. The results will be compared with results, which are derived from conventional methods. And finally, a discussion on the overall study is provided in Section 7.

## II. Spurious Trip

A spurious trip is one cause of an unexpected plant shutdown initiated by a safety-instrumented system. Namely, if a safety loop component fails to function, the safety instrumented system is prompted to shut down that part of the plant's operation. This is done because the failure of a particular safety loop can prevent the safety-instrumented system from functioning properly. It does not guarantee plant safety. Therefore, spurious activation normally leads to lost production or low availability of the EUC [9].

Industry data report that when a process unit experiences a high number of spurious alarms, the operators become ambivalent and are likely to respond slowly or not at all to a critical "real alarm" [7]. This means that spurious trip is not only expensive, but also in most cases can be considered as dangerous too. The standard IEC 61508 has no requirement related to spurious activations, while IEC 61511 requires that a maximum STR is specified, but the standard does not provide how the rate should be estimated [1], [4] and [9].

### A. Spurious Trip Rate

The spurious trip rate or also known as "false trip rate" is defined in [3]: "the term spurious trip rate (STR) refers to the rate at which a nuisance or spurious trip might occur in the SIS". The unit of STR is 1/h and describes how available a component or a system is. The availability is higher if the STR is smaller.

To estimate the STR, the oil and gas industry often use the formulas presented in [3] and [8]. When comparing these formulas, it becomes evident that there is no unique interpretation of the concept of spurious trip. Whereas the PDS method [8] defines a spurious trip as "a spurious activation of a single SIS element or of a SIF", ANSI/ISA-TR84.00.02-2002 [3] refers to a spurious trip as a "non-intended process shutdown". As a result, the concept of spurious trip is rather confusing and it is difficult to compare the STR in different applications [9]. STR formulas of some conventional methods are presented in the following table:

TABLE III
Spurious Trip Rate formulas of conventional method

| STL | ANSI/ISA TR84.00.02.2002 [3] | PDS-Method [8] | Machleidt & Litz [16] |
|---|---|---|---|
| 1oo1 | $STR=\lambda_S+\lambda_{DD}+\lambda_F^S$ | $STR=\lambda_{STU}$ | $STR=\lambda_{sp}=\lambda_S$ |
| 1oo2 | $STR=2(\lambda_S+\lambda_{DD})+\beta(\lambda_S+\lambda_{DD})+\lambda_F^S$ | $STR=2\cdot\lambda_{STU}$ | $STR=(2-\beta_{sp})\lambda_{sp}^{1oo2}$ $\lambda_{sp}^{1oo2}=\sqrt{\lambda_{sp1}\lambda_{sp2}}$ |
| 2oo2 | $STR=2\lambda_S(\lambda_S+\lambda_{DD})MTTR+\beta(\lambda_S+\lambda_{DD})+\lambda_F^S$ | $STR=\beta\cdot\lambda_{STU}$ | |
| 2oo3 | $STR=6\lambda_S(\lambda_S+\lambda_{DD})MTTR+\beta(\lambda_S+\lambda_{DD})+\lambda_F^S$ | $STR=C_{2oo3}\beta\lambda_{STU}$ | $STR=\beta_{sp}\lambda_{sp}^{2oo3}$ $\lambda_{sp}^{2oo3}=\sqrt{(\lambda_{sp1}\lambda_{sp2}}\sqrt{+\lambda_{sp1}\lambda_{sp3}}\sqrt{+\lambda_{sp2}\lambda_{sp3})}/\sqrt{3}$ |
| 2oo4 | $STR=12(\lambda_S+\lambda_{DD})^3 MTTR+\beta(\lambda_S+\lambda_{DD})+\lambda_F^S$ | $STR=C_{3oo4}\beta\lambda_{STU}$ | |

### B. Probability of Spurious Trip

Probability of Failure Spurious (PFS) is the probability of failure due to the spurious trip. The smaller this value, the more available the system is. For the evaluation and comparison of systems, the average $PFS_{avg}$ is calculated as followed:

$$PFS_{avg}(T)=\frac{1}{T}\int_0^T PFS(t)\cdot dt = \frac{1}{T}\int_0^T (1-R_{Spurious}(t))\cdot dt \tag{1}$$

with $R_{Spurious}(t)$ is calculated by the following equation:

$$R_{Spurious}(t) = e^{-\int_0^t STR(\tau)dt} \quad (2)$$

### C. Mean Time To Failure Spurious

Mean Time to Failure Spurious is abbreviated as $MTTF_{Spurious}$ and is the estimated time between spurious failures of a component or a system [3]. To estimate the $MTTF_{Spurious}$ value, ISA [3] introduces three methods: simplified equation, fault tree analysis and the Markov model. $MTTF_{Spurious}$ is proportional to the availability. This means that a component or a system is more available if the $MTTF_{Spurious}$ value is higher. The following equation presents the calculation of $MTTF_{Spurious}$ by simplified equation:

$$MTTF_{Spurious} = \int_0^\infty R_{Spurious}(t) \cdot dt \quad (3)$$

## III. Low Demand and High Demand System

A SIS has to achieve or maintain a safe state for the system the SIS is protecting with respect to a specific process demand. Safe state can be defined differently for each system. In some cases, the safe state is to maintain before the demand occurs, whereas in other cases, it means to stop the EUC. Typical low-demand systems are emergency shutdown systems (ESD), process shutdown systems (PSD) or airbag systems in automobiles. And the typical high-demand systems are railway signal systems, safety-related electrical control systems for machinery. One of the important aspects of SIS with low-demand is that the EUC remains in the safe state after the SIS has responded to a demand. And for a SIS with high-demand the EUC will be returned to the normal operating state after the demand [10]. For example, a railway signaling system is always ready to respond to a new request when the previous train has left the rail section [10].

Another difference between low-demand and high-demand systems is the functional testing. For a low-demand SIS, it is important to perform functional testing to detect DU-failure (dangerous undetected) but it is not always required for high-demand. Due to the fact that the demand rate is high it may not be possible to use functional testing to detect and repair DU-failures before the next demand. However, it is important to perform regular testing for high-demand systems to prevent the operating of SIS with reduced fault tolerance [10].

The diagnostic testing is an automatic self-test that is implemented in SIS to reveal failure without an interruption of the EUC and it is frequent. It can take place every few seconds, minutes or hours. This test should be carefully considered for the both systems. This means, for low-demand systems, there is usually enough time to repair and restore the function until the next demand appears. But for high-demand systems, the demand rate and the diagnostic test frequency may be the same [10].

The demand rate varies from low to high or continuous and the duration of each demand may vary from short to long period. So, the same equation can usually not be applied to all systems [13]. With the Markov method several authors have shown the best suited for analyzing safety systems. By using this method, it is possible to model different states with different failure modes of the components, different points in time, periods and test strategies. Therefore the authors in [10], [13] have used the Markov model to illustrate the borderline between low-demand and high-demand systems in a better way. The whole calculations of PFD and PFH are dependent on the demand rate and the demand duration. Based on this result and availability theory, a STR-, PFS- and $MTTF_{Spurious}$ calculation of the 1oo1- and 1oo2-architecture will be presented in low- and high-demand in this article.

## IV. Modelling of 1oo1-Architecture

If the system fails because of a spurious trip failure, the system will be in de-energized state. This means that the system is not available anymore. The characteristics of 1oo1-architecture will be presented in Fig. 2. The EUC enters a safe state without demand, when a safe failure respectively spurious trip failure occurs in the SIS.

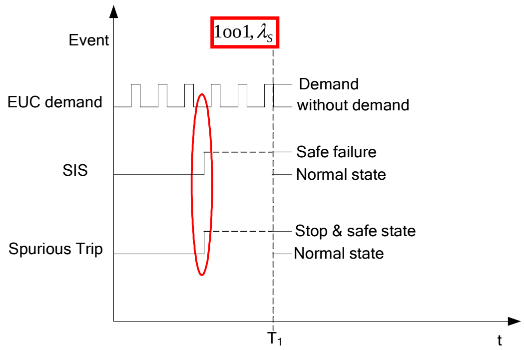


Fig. 2. EUC and SIS of 1oo1-architecture

### A. Block diagram

A block diagram of a SIS with 1oo1-architecture is illustrated in Fig. 3 with three elements: input, logic and output:

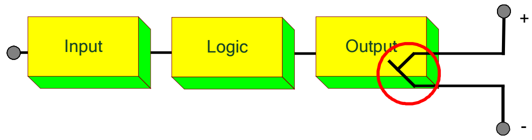


Fig. 3. Block diagram of 1oo1-architecture

A SIS with 1oo1-architecture fails spurious, when a safe failure in SIS or a false demand arises. Therefore, the spurious trip rate consists of not only the rate of safe failures $\lambda_S$ but also of the demand rate $\lambda_{DE}$. Let the factor $0 < \gamma < 1$ be the ratio of false demand to total demand of SIS in a considered time interval, the calculation of spurious trip rate for 1oo1 architecture is described in the following way:

$$STR_{1oo1} = \lambda_S + \gamma \cdot \lambda_{DE} \tag{4}$$

$PFS_{avg\_1oo1}$ can be calculated by using simplified equation:

$$\begin{aligned} PFS_{avg\_1oo1} &= \frac{1}{T}\int_0^T PFS_{1oo1}(t)\cdot dt \\ &= \frac{1}{T}\int_0^T (1 - R_{Spurious\_1oo1}(t))\cdot dt \end{aligned} \tag{5}$$

for 1oo1-architecture the reliability is estimated as follows:

$$R_{Spurious\_1oo1}(t) = 1 - e^{-STR_{1oo1}t} \tag{6}$$

Derived from equations (4), (5) and (6) the formula of $PFS_{avg}$ for 1oo1-architecture is described as:

$$\begin{aligned} \Rightarrow PFS_{avg\_1oo1}(T) &= \frac{1}{T}\int_0^T (1 - e^{-STR_{1oo1}\cdot t})\cdot dt \\ &\approx \frac{STR_{1oo1}\cdot T}{2} \\ &\approx \frac{(\lambda_S + \gamma\cdot\lambda_{DE})\cdot T}{2} \end{aligned} \tag{7}$$

$MTTF_{Spurious\_1oo1}$ can be calculated by:

$$\begin{aligned} MTTF_{Spurious\_1oo1} &= \int_0^\infty R_{Spurious\_1oo1}(t)\cdot dt \\ &= \int_0^\infty e^{-STR_{1oo1}\cdot t} \\ &= \frac{1}{\lambda_S + \gamma\cdot\lambda_{DE}} \end{aligned} \tag{8}$$

### *B. Markov model*

By the use of simplified equations the effect of demand rate and demand duration cannot be shown precisely. For this reason Markov model will be used. It is better to model different states with different failure mode of the components. Fig. 4 presents 8 states of the Markov model of a 1oo1-architecture. State Z0 represents the failure free state and the system is operating correctly. From this state, seven other states can be reached:

--State Z1 presents the safe state (de-energized state) or spurious trip state. This state can be left with a transition rate $\mu_R = 1/\tau_{Repair}$, with $\tau_{Repair}$ which is the time the system requires for repair and startup.

--State Z2 has got a safe detected failure and will reach the safe state with the transition rate $\lambda_{DE}$ when a demand occurs or with the transition rate $\mu_0 = 1/\tau_{Test}$, with $\tau_{Test}$ which is the test time interval.

--State Z3 has got a safe undetected failure. With the transition rate $\mu_{LT} = 1/\tau_{LT}$ (with $\tau_{LT}$ which is the lifetime) the system is able to reach the failure free state. And with the transition rate $\lambda_{DE}$ the system can reach the safe state.

--State Z4 has got a dangerous detected failure. If a demand occurs, the system can reach the dangerous state Z6 with the transition rate $\lambda_{DE}$. And with the transition rate $\mu_0 = 1/\tau_{Test}$ the system can reach the safe state.

--State Z5 represents the dangerous undetected state. This state can change into state Z0 at the end of its lifetime and subsequently replaced or repaired with a transition rate $\mu_{LT} = 1/\tau_{LT}$. If the system is at this state and a demand occurs, the system can reach the dangerous state Z6 with the transition rate $\lambda_{DE}$.

--State Z6 is the hazardous state, where the safety function fails and the system cannot reach the safe state.

--State Z7 presents the demand state, where the activation of the safety function is requested.

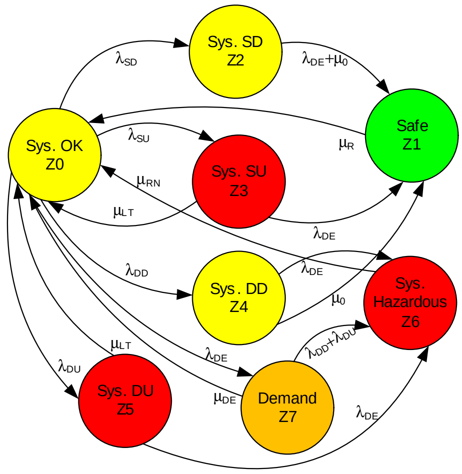


Fig. 4. Markov model of 1oo1-architecture

The transition matrix is described in the following way:

$$P = \begin{bmatrix} 1-A_0 & 0 & \lambda_{SD} & \lambda_{SU} & \lambda_{DD} & \lambda_{DU} & 0 & \lambda_{DE} \\ \mu_R & 1-\mu_R & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_{DE}+\mu_0 & 1-A_2 & 0 & 0 & 0 & 0 & 0 \\ \mu_{LT} & \lambda_{DE} & 0 & 1-A_3 & 0 & 0 & 0 & 0 \\ 0 & \mu_0 & 0 & 0 & 1-A_4 & 0 & \lambda_{DE} & 0 \\ \mu_{LT} & 0 & 0 & 0 & 0 & 1-A_5 & \lambda_{DE} & 0 \\ \mu_{RN} & 0 & 0 & 0 & 0 & 0 & 1-\mu_{RN} & 0 \\ \mu_{DE} & 0 & 0 & 0 & 0 & 0 & \lambda_{DD}+\lambda_{DU} & 1-A_7 \end{bmatrix}$$

with:

$$A_0 = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU} + \lambda_{DE} \tag{9}$$

$$A_2 = A_4 = \lambda_{DE} + \mu_0 \tag{10}$$

$$A_3 = A_5 = \lambda_{DE} + \mu_{LT} \tag{11}$$

The steady-state equation corresponding to the Markov model in Fig. 4 can be obtained:

$$
\begin{aligned}
&\mu_R P_1 = (\lambda_{DE} + \mu_0)P_2 + \lambda_{DE} P_3 + \mu_0 P_4 \\
&(\lambda_{DE} + \mu_0)P_2 = \lambda_{SD} P_0 \\
&(\lambda_{DE} + \mu_{LT})P_3 = \lambda_{SU} P_0 \\
&(\lambda_{DE} + \mu_0)P_4 = \lambda_{DD} P_0 \\
&(\lambda_{DE} + \mu_{LT})P_5 = \lambda_{DU} P_0 \\
&\mu_{RN} P_6 = \lambda_{DE}(P_4 + P_5) + (\lambda_{DD} + \lambda_{DU})P_7 \\
&(\lambda_{DD} + \lambda_{DU} + \mu_{DE})P_7 = \lambda_{DE} P_0 \\
&P_0 + P_1 + P_2 + P_3 + P_4 + P_5 + P_6 + P_7 = 1
\end{aligned} \tag{12}
$$

Solving this equation system results in:

$$
\begin{aligned}
A = &\frac{\lambda_{SD}}{\lambda_{DE} + \mu_0} + \frac{\lambda_{SD}}{\mu_R} + \left(\frac{\lambda_{DE}}{\mu_R} + 1\right)\frac{\lambda_{SU}}{\lambda_{DE} + \mu_{LT}} \\
&+ \left(\frac{\mu_0}{\mu_R} + 1 + \frac{\lambda_{DE}}{\mu_{RN}}\right)\frac{\lambda_{DD}}{\lambda_{DE} + \mu_0} \\
&+ \frac{\lambda_{DU}}{\mu_{LT} + \lambda_{DE}}\left(1 + \frac{\lambda_{DE}}{\mu_{RN}}\right) + \left(1 + \frac{\lambda_D}{\mu_{RN}}\right)\frac{\lambda_{DE}}{\mu_{DE} + \lambda_D}
\end{aligned} \tag{13}
$$

$$P_0 = \frac{1}{A} \tag{14}$$

$$P_1 = \frac{(\lambda_{DE} + \mu_0)P_2 + \lambda_{DE} P_3 + \mu_0 P_4}{\mu_8} \tag{15}$$

$$P_2 = \frac{\lambda_{SD} P_0}{\mu_{21}} = \frac{\lambda_{SD} P_0}{\lambda_{DE} + \mu_0} \tag{16}$$

$$P_3 = \frac{\lambda_{SU} P_0}{\mu_{31}} = \frac{\lambda_{SU} P_0}{\lambda_{DE} + \mu_{LT}} \tag{17}$$

$$P_4 = \frac{\lambda_{DD} P_0}{\lambda_{DE} + \mu_{41}} = \frac{\lambda_{DD} P_0}{\lambda_{DE} + \mu_0} \tag{18}$$

$$P_5 = \frac{\lambda_{DU} P_0}{\lambda_{DE} + \mu_{LT}} \tag{19}$$

$$P_6 = \frac{\lambda_{DE}\left[\frac{\lambda_{DD} P_0}{\lambda_{DE} + \mu_0} + \frac{\lambda_{DU} P_0}{\mu_{LT} + \lambda_{DE}}\right] + \lambda_D \frac{\lambda_{DE} P_0}{\mu_{DE} + \lambda_D}}{\mu_{RN}} \tag{20}$$

$$P_7 = \frac{\lambda_{DE} P_0}{\lambda_{DD} + \lambda_{DU} + \mu_{DE}} = \frac{\lambda_{DE} P_0}{\mu_{DE} + \lambda_D} \tag{21}$$

The $PFS_{1oo1}$ value is the sum of the probabilities P1 and γ·P7:

$$PFS_{1oo1} = P_1 + \gamma \cdot P_7 \tag{22}$$

The spurious trip rate of 1oo1-system will be given by the following equation:

$$
\begin{aligned}
PFS_{1oo1} &= 1 - R_{Spurious\_1oo1}(t) \\
&= 1 - e^{-STR_{1oo1} \cdot t} \\
\Rightarrow STR_{1oo1} &= -\frac{\ln(1 - PFS_{1oo1})}{t}
\end{aligned} \tag{23}
$$

And the Mean Time To Failure Spurious is calculated as follows:

$$
\begin{aligned}
MTTF_{Spurious\_1oo1} &= \int_0^\infty R_{Spurious\_1oo1}(t) \cdot dt \\
&= \int_0^\infty e^{-STR_{1oo1} \cdot t} \\
&= \frac{1}{STR_{1oo1}} \\
&= \frac{-t}{\ln(1 - PFS_{1oo1})}
\end{aligned} \tag{24}
$$

## V. Modeling of 1oo2-Architecture

A safety system with 1oo2-architecture will bring EUC in de-energized state, if a safe failure or common cause failure respectively spurious trip failure occurs in the SIS. The characteristics of 1oo2-architecture are presented in Fig. 5, if random failure occurs and in Fig. 6, if common cause failure occurs. A random failure is a "failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware" [1], [18]. And a common cause failure occurs, when a random failure leads to a failure of several components [1], [18].

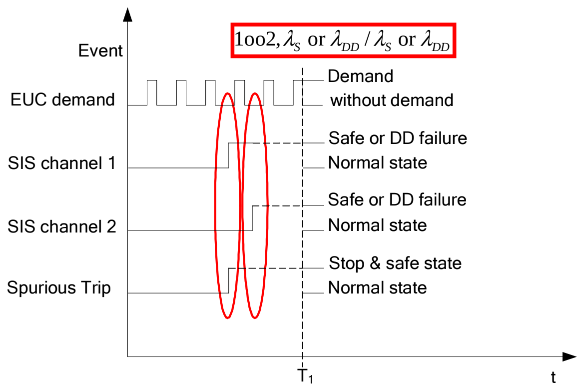


Fig. 5 EUC and SIS of 1oo2-architecture (random failure) [14]

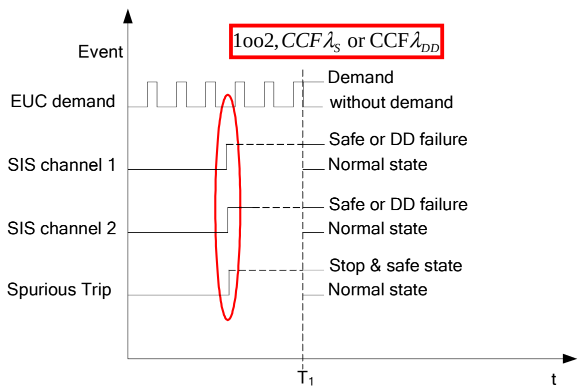


Fig. 5 EUC and SIS of 1oo2-architecture (common cause failure) [14]

### *A. Block diagram*

A block diagram of a SIS with 1oo2-architecture is illustrated in Fig. 7 with two channel, which consist of three elements: input, logic and output.

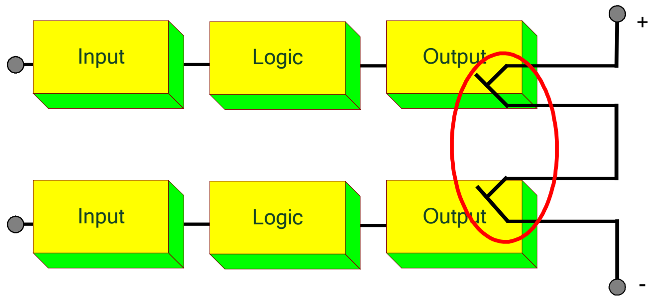


Fig. 7 Block diagram of 1oo2-architecture

A SIS with 1oo2-architecture fails spurious, when one of the following cases in SIS arises: a safe failure or a dangerous detected failure or a common cause failure; or a false demand arises. Therefore, the spurious trip rate consists of not only the rate of safe failures $\lambda_S$, $\lambda_{DD}$ but also of the demand rate $\lambda_{DE}$. Let the factor $0 < \gamma < 1$ be the ratio of false demand to total demand of SIS in a considered time interval, the calculation of spurious trip rate for 1oo2 architecture is described in the following way:

$$\begin{aligned} STR_{1oo2} &= 2\cdot[(1-\beta_D)\cdot\lambda_{SD} + (1-\beta)\cdot\lambda_{SU}] \\ &\quad + \beta\cdot\lambda_{SU} + \beta_D\cdot\lambda_{SD} + \gamma\cdot\lambda_{DE} \end{aligned} \tag{25}$$

$PFS_{avg\_1oo2}$ can be calculated by using simplified equation:

$$\begin{aligned} PFS_{avg\_1oo2}(T) &= \frac{1}{T}\int_0^T PFS_{1oo2}(t) \\ &= \frac{1}{T}\int_0^T (1 - R_{Spurious\_Trip\_1oo2})\cdot dt \\ &= 1 + \frac{2}{T}\cdot\frac{e^{-STR_{1oo2}\cdot T} - 1}{STR_{1oo2}} - \frac{e^{-2\cdot STR_{1oo2}\cdot T} - 1}{2\cdot T\cdot STR_{1oo2}} \end{aligned} \tag{26}$$

with the development of MacLaurin series:

$$\begin{aligned} e^{-STR_{1oo2}\cdot T} &= 1 - STR_{1oo2}\cdot T + \frac{STR_{1oo2}{}^2\cdot T^2}{2!} \\ &\quad - \frac{STR_{1oo2}{}^3\cdot T^3}{3!} + R_4 \end{aligned} \tag{27}$$

$$\begin{aligned} e^{-2\cdot STR_{1oo2}\cdot T} &= 1 - 2\cdot STR_{1oo2}\cdot T + \frac{(2\cdot STR_{1oo2})^2\cdot T^2}{2!} \\ &\quad - \frac{(2\cdot STR_{1oo2})^3\cdot T^3}{3!} + R_4 \end{aligned} \tag{28}$$

The remaining term R4 converges for T = 0 to the value 0 and can be neglected:

$$\lim_{T\to 0} R_4 = 0 \tag{29}$$

Derived from equations (25), (26), (27), (28) and (29) the formula of $PFS_{avg}$ for 1oo2-architecture is described as:

$$\Rightarrow PFS_{avg\_1oo2}(T) = \frac{STR_{1oo2}{}^2\cdot T^2}{3} \tag{30}$$

$MTTF_{Spurious\_1oo2}$ can be calculated by:

$$\begin{aligned} MTTF_{Spurious\_1oo2} &= \int_0^\infty R_{Spurious\_1oo2}(t)\cdot dt \\ &= \frac{3}{2\cdot STR_{1oo2}} \end{aligned} \tag{31}$$

### *B. Markov model*

Fig. 8 presents 22 states of the Markov model of a 1oo2-architecture. State Z0 represents the failure free state and the system is operating correctly. From this state, 21 other states can be reached.

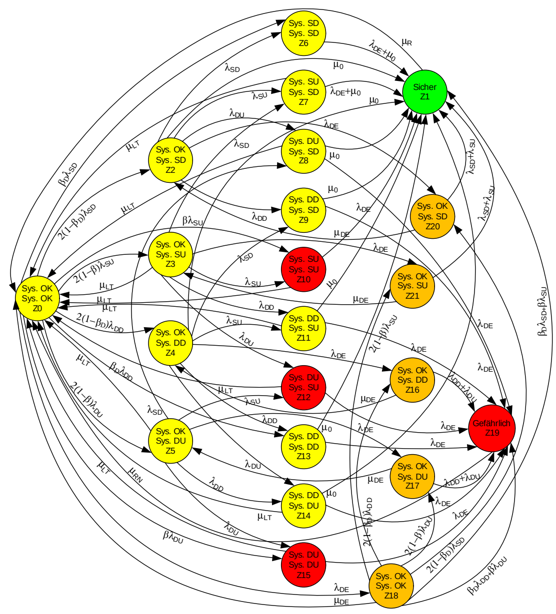

Fig. 8 Block diagram of 1oo2-architecture

The transition matrix is described in the following way:

$$P = \begin{bmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \end{bmatrix} \tag{32}$$

with:

$$P_{11}=\begin{bmatrix}1-A_0dt & 0 & 2(1-\beta_D)\lambda_{SD}dt & 2(1-\beta)\lambda_{SU}dt & 2(1-\beta_D)\lambda_{DD}dt & 2(1-\beta)\lambda_{DU}dt\\ \mu_R dt & 1-A_1dt & 0 & 0 & 0 & 0\\ 0 & 0 & 1-A_2dt & 0 & 0 & 0\\ \mu_{LT}dt & 0 & 0 & 1-A_3dt & 0 & 0\\ 0 & 0 & 0 & 0 & 1-A_4dt & 0\\ \mu_{LT}dt & 0 & 0 & 0 & 0 & 1-A_5dt\\ 0 & (\lambda_{DE}+\mu_0)dt & 0 & 0 & 0 & 0\\ \mu_{LT}dt & (\lambda_{DE}+\mu_0)dt & 0 & 0 & 0 & 0\\ \mu_{LT}dt & \mu_0dt & 0 & 0 & 0 & 0\\ 0 & \mu_0dt & 0 & 0 & 0 & 0\\ \mu_{LT}dt & \lambda_{DE} & 0 & 0 & 0 & 0\end{bmatrix}$$

$$P_{12}=\begin{bmatrix}\beta_D\lambda_{SD}dt & 0 & 0 & 0 & \beta\lambda_{SU}dt & 0 & 0 & \beta_D\lambda_{DD}dt\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ \lambda_{SD}dt & \lambda_{SU}dt & \lambda_{DU}dt & \lambda_{DD}dt & 0 & 0 & 0 & 0\\ 0 & \lambda_{SD}dt & 0 & 0 & \lambda_{SU}dt & \lambda_{DD}dt & \lambda_{DU}dt & 0\\ 0 & 0 & 0 & \lambda_{SD}dt & 0 & \lambda_{SU}dt & 0 & \lambda_{DD}dt\\ 0 & 0 & \lambda_{SD}dt & 0 & 0 & 0 & \lambda_{SU}dt & 0\\ 1-A_6dt & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1-A_7dt & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1-A_8dt & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1-A_9dt & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1-A_{10}dt & 0 & 0 & 0\end{bmatrix}$$

$$P_{13}=\begin{bmatrix}0 & \beta\lambda_{SU}dt & 0 & 0 & \lambda_{DE}dt & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{DE}dt & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{DE}dt\\ \lambda_{DU}dt & 0 & \lambda_{DE}dt & 0 & 0 & 0 & 0 & 0\\ \lambda_{DD}dt & \lambda_{DU}dt & 0 & \lambda_{DE}dt & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & \lambda_{DE}dt & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & \lambda_{DE}dt & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$$

$$P_{21}=\begin{bmatrix}\mu_{LT}dt & \mu_0dt & 0 & 0 & 0 & 0\\ \mu_{LT}dt & 0 & 0 & 0 & 0 & 0\\ 0 & \mu_0 & 0 & 0 & 0 & 0\\ \mu_{LT}dt & \mu_0 & 0 & 0 & 0 & 0\\ \mu_{LT}dt & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \mu_{DE}dt & 0\\ 0 & 0 & 0 & 0 & 0 & \mu_{DE}dt\\ \mu_{DE}dt & (\beta_D\lambda_{SD}+\beta\lambda_{SU})dt & 0 & 0 & 0 & 0\\ \mu_{RN}dt & 0 & 0 & 0 & 0 & 0\\ 0 & (\lambda_{SD}+\lambda_{SU})dt & \mu_{DE}dt & 0 & 0 & 0\\ 0 & (\lambda_{SD}+\lambda_{SU})dt & 0 & \mu_{DE}dt & 0 & 0\end{bmatrix}$$

$$P_{22}=\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 1-A_{11}dt & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1-A_{12}dt & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-A_{13}dt\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$$

$$P_{23}=\begin{bmatrix}0 & 0 & 0 & 0 & 0 & \lambda_{DE} & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & \lambda_{DE} & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & \lambda_{DE} & 0 & 0\\ 1-A_{14}dt & 0 & 0 & 0 & 0 & \lambda_{DE} & 0 & 0\\ 0 & 1-A_{15}dt & 0 & 0 & 0 & \lambda_{DE} & 0 & 0\\ 0 & 0 & 1-A_{16}dt & 0 & 0 & \lambda_{DD}+\lambda_{DU} & 0 & 0\\ 0 & 0 & 0 & 1-A_{17}dt & 0 & \lambda_{DD}+\lambda_{DU} & 0 & 0\\ 0 & 0 & 2(1-\beta_D)\lambda_{DD} & 2(1-\beta)\lambda_{DU} & 1-A_{18}dt & \beta_D\lambda_{DD}+\beta\lambda_{DU} & 2(1-\beta_D)\lambda_{SD} & 2(1-\beta)\lambda_{SU}\\ 0 & 0 & 0 & 0 & 0 & 1-\mu_{RN}dt & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1-A_{20}dt & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-A_{21}dt\end{bmatrix}$$

$$\begin{aligned}A_0 &= 2(1-\beta_D)\lambda_{SD}+2(1-\beta)\lambda_{SU}+2(1-\beta_D)\lambda_{DD}\\ &\quad +2(1-\beta)\lambda_{DU}+\beta_D\lambda_{SD}+\beta\lambda_{SU}+\beta_D\lambda_{DD}+\beta\lambda_{DU}+\lambda_{DE}\\ A_2 &= A_4 = \lambda_{DE}+\lambda_{SD}+\lambda_{SU}+\lambda_{DU}+\lambda_{DD}\\ A_3 &= A_5 = \mu_{LT}+\lambda_{SD}+\lambda_{SU}+\lambda_{DU}+\lambda_{DD}+\lambda_{DE}\\ A_6 &= A_9 = A_{13} = \mu_0+\lambda_{DE}\\ A_7 &= A_8 = A_{11} = A_{14} = \mu_{LT}+\mu_0+\lambda_{DE}\\ A_{10} &= A_{12} = A_{15} = \mu_{LT}+\lambda_{DE}\\ A_{16} &= A_{17} = \mu_{DE}+\lambda_{DD}+\lambda_{DU}\\ A_{18} &= \mu_{DE}+2(1-\beta_D)\lambda_{DD}+2(1-\beta)\lambda_{DU}+\beta_D\lambda_{DD}+\beta\lambda_{DU}\\ &\quad +2(1-\beta_D)\lambda_{SD}+2(1-\beta)\lambda_{SU}+\beta_D\lambda_{SD}+\beta\lambda_{SU}\\ A_{20} &= A_{21} = \lambda_{SD}+\lambda_{SU}+\mu_{DE}\end{aligned}$$

The steady-state equation corresponding to the Markov model in Fig. 8 can be obtained:

$$\begin{aligned}&\mu_R P_1 = \mu_0(P_2+P_4+P_8+P_9+P_{11}+P_{13}+P_{14})\\ &\qquad +(\lambda_{DE}+\mu_0)(P_6+P_7)+\lambda_{DE}P_{10}+(\beta_D\lambda_{SD}+\beta\lambda_{SU})P_{18}\\ &\qquad +(\lambda_{SD}+\lambda_{SU})(P_{20}+P_{21})\\ &(\lambda+\lambda_{DE}+\mu_0)P_2 = 2(1-\beta_D)\lambda_{SD}P_0+\mu_{DE}P_{20}\\ &(\lambda+\lambda_{DE}+\mu_{LT})P_3 = 2(1-\beta)\lambda_{SU}P_0+\mu_{DE}P_{21}\\ &(\lambda+\lambda_{DE}+\mu_0)P_4 = 2(1-\beta_D)\lambda_{DD}P_0+\mu_{DE}P_{16}\\ &(\lambda+\lambda_{DE}+\mu_{Lt})P_5 = 2(1-\beta)\lambda_{DU}P_0+\mu_{DE}P_{17}\\ &(\lambda_{DE}+\mu_0)P_6 = \beta_D\lambda_{SD}P_0+\lambda_{SD}P_2\\ &(\mu_{LT}+\lambda_{DE}+\mu_0)P_7 = \lambda_{SU}P_2+\lambda_{SD}P_3\\ &(\mu_{LT}+\lambda_{DE}+\mu_0)P_8 = \lambda_{DU}P_2+\lambda_{SD}P_5\\ &(\lambda_{DE}+\mu_0)P_9 = \lambda_{DD}P_2+\lambda_{SD}P_4\\ &(\mu_{LT}+\lambda_{DE})P_{10} = \beta\lambda_{SU}P_0+\lambda_{SU}P_3\\ &(\mu_{LT}+\lambda_{DE}+\mu_0)P_{11} = \lambda_{DD}P_3+\lambda_{SU}P_4\\ &(\mu_{LT}+\lambda_{DE})P_{12} = \lambda_{DU}P_3+\lambda_{SU}P_5\\ &(\lambda_{DE}+\mu_0)P_{13} = \beta_D\lambda_{DD}P_0+\lambda_{DD}P_4\\ &(\mu_{LT}+\lambda_{DE}+\mu_0)P_{14} = \lambda_{DU}P_4+\lambda_{DD}P_5\\ &(\mu_{LT}+\lambda_{DE})P_{15} = \beta\lambda_{DU}P_0+\lambda_{DU}P_5\\ &(\mu_{DE}+\lambda_{DD}+\lambda_{DU})P_{16} = \lambda_{DE}P_4+2(1-\beta_D)\lambda_{DD}P_{18}\\ &(\mu_{DE}+\lambda_{DD}+\lambda_{DU})P_{17} = \lambda_{DE}P_5+2(1-\beta)\lambda_{DU}P_{18}\\ &\lambda_{DE}P_0 = [\mu_{DE}+(2-\beta_D)\lambda_{DD}+(2-\beta)\lambda_{DU}+(2-\beta_D)\lambda_{SD}]P_{18}\\ &\qquad +(2-\beta)\lambda_{DU}P_{18}\end{aligned}$$

$$\mu_{RN} P_{19} = \lambda_{DE}(P_8 + P_9 + P_{11} + P_{12} + P_{13} + P_{14} + P_{15}) + \lambda_D (P_{16} + P_{17}) + (\beta_D \lambda_{DD} + \beta \lambda_{DU}) P_{18}$$
$$(\lambda_{SD} + \lambda_{SU} + \mu_{DE}) P_{20} = \lambda_{DE} P_2 + 2(1-\beta_D)\lambda_{SD} P_{18}$$
$$(\lambda_{SD} + \lambda_{SU} + \mu_{DE}) P_{21} = \lambda_{DE} P_3 + 2(1-\beta)\lambda_{SU} P_{18}$$
$$\sum_{i=0}^{21} P_i = 1$$

Solving this equation system results in:

$$P_0 = \frac{1}{D_0} \quad (33)$$
$$P_2 = \frac{\lambda_{SD} P_0}{\lambda_{DE} + \mu_0} \quad (34)$$
$$P_3 = \frac{\lambda_{SU} P_0}{\lambda_{DE} + \mu_{LT}} \quad (35)$$
$$P_4 = \frac{\lambda_{DD} P_0}{\lambda_{DE} + \mu_0} \quad (36)$$
$$P_5 = \frac{\lambda_{DU} P_0}{\lambda_{DE} + \mu_{LT}} \quad (37)$$
$$P_6 = \frac{\lambda_{DE}\left[\frac{\lambda_{DD} P_0}{\lambda_{DE} + \mu_0} + \frac{\lambda_{DU} P_0}{\mu_{LT} + \lambda_{DE}}\right] + \lambda_D \frac{\lambda_{DE} P_0}{\mu_{DE} + \lambda_D}}{\mu_{RN}} \quad (38)$$
$$P_8 = \frac{\lambda_{SU} P_2 + \lambda_{SD} P_5}{\mu_{LT} + \lambda_{DE} + \mu_0} \quad (39)$$
$$P_9 = \frac{\lambda_{DD} P_2 + \lambda_{SD} P_4}{\lambda_{DE} + \mu_0} \quad (40)$$
$$P_{10} = \frac{\beta \lambda_{DU} P_0 + \lambda_{SU} P_3}{\lambda_{DE} + \mu_{LT}} \quad (41)$$
$$P_{11} = \frac{\lambda_{DD} P_3 + \lambda_{SU} P_4}{\mu_{LT} + \lambda_{DE} + \mu_0} \quad (42)$$
$$P_{12} = \frac{\lambda_{DU} P_3 + \lambda_{SU} P_5}{\lambda_{DE} + \mu_{LT}} \quad (43)$$
$$P_{13} = \frac{\beta_D \lambda_{DD} P_0 + \lambda_{DD} P_4}{\lambda_{DE} + \mu_0} \quad (44)$$
$$P_{14} = \frac{\lambda_{DU} P_4 + \lambda_{DD} P_5}{\lambda_{DE} + \mu_{LT} + \mu_0} \quad (45)$$
$$P_{15} = \frac{\beta \lambda_{DU} P_0 + \lambda_{DU} P_5}{\lambda_{DE} + \mu_{LT}} \quad (46)$$
$$P_{16} = D_{16} P_0 \quad (47)$$
$$P_{17} = D_{17} P_0 \quad (48)$$
$$P_{18} = D_{18} P_0 \quad (49)$$
$$P_{19} = D_{19} P_0 \quad (50)$$
$$P_{20} = D_{20} P_0 \quad (51)$$
$$P_{21} = D_{21} P_0 \quad (52)$$

with:

$$D_0 = 1 + \left(\frac{\mu_0}{\mu_R} + 1\right)(D_2 + D_4 + D_{22}) + (\lambda_{DE} + \mu_0 + 1) D_{23} + (\lambda_{DE} + 1)\frac{(\beta + D_3)\lambda_{SU}}{\lambda_{DE} + \mu_{LT}} + (\beta_D \lambda_{SD} + \beta \lambda_{SU} + 1) D_{18} + (\lambda_S + 1)(D_{20} + D_{21}) + D_3 + D_5 + D_{16} + D_{17} + D_{19} + \frac{\lambda_{DU}(D_3 + \beta) + (\lambda_{SU} + \lambda_{DU}) D_5}{\lambda_{DE} + \mu_{LT}} \quad (53)$$

$$D_1 = \frac{1}{\mu_R}\Big[\mu_0 (D_2 + D_4 + D_{22}) + (\lambda_{DE} + \mu_0) D_{23} + \frac{(\beta + D_3)\lambda_{SU}\lambda_{DE}}{\lambda_{DE} + \mu_{LT}} + (\beta_D \lambda_{SD} + \beta \lambda_{SU}) D_{18} + \lambda_S (D_{20} + D_{21})\Big] \quad (54)$$

$$D_2 = \frac{2(1-\beta_D)\lambda_{SD}\left(1 + \frac{\mu_{DE} D_{18}}{\lambda_S + \mu_{DE}}\right)}{\lambda + \lambda_{DE} + \mu_0 - \frac{\lambda_{DE}\mu_{DE}}{\lambda_S + \mu_{DE}}} \quad (55)$$

$$D_3 = \frac{2(1-\beta)\lambda_{SU}\left(1 + \frac{\mu_{DE} D_{18}}{\lambda_S + \mu_{DE}}\right)}{\lambda + \lambda_{DE} + \mu_{LT} - \frac{\lambda_{DE}\mu_{DE}}{\lambda_S + \mu_{DE}}} \quad (56)$$

$$D_4 = \frac{2(1-\beta_D)\lambda_{DD}\left(1 + \frac{\mu_{DE} D_{18}}{\lambda_D + \mu_{DE}}\right)}{\lambda + \lambda_{DE} + \mu_0 - \frac{\lambda_{DE}\mu_{DE}}{\lambda_D + \mu_{DE}}} \quad (57)$$

$$D_5 = \frac{2(1-\beta)\lambda_{DU}\left(1 + \frac{\mu_{DE} D_{18}}{\lambda_D + \mu_{DE}}\right)}{\lambda + \lambda_{DE} + \mu_{LT} - \frac{\lambda_{DE}\mu_{DE}}{\lambda_D + \mu_{DE}}} \quad (58)$$

$$D_{16} = \frac{\lambda_{DE} D_4 + 2(1-\beta_D)\lambda_{DD} D_{18}}{\lambda_D + \mu_{DE}} \quad (59)$$

$$D_{17} = \frac{\lambda_{DE} D_5 + 2(1-\beta)\lambda_{DU} D_{18}}{\lambda_D + \mu_{DE}} \quad (60)$$

$$D_{18} = \frac{\lambda_{DE}}{\mu_{DE} + (2-\beta_D)(\lambda_{SD} + \lambda_{DD}) + (2-\beta)(\lambda_{SU} + \lambda_{DU})} \quad (61)$$

$$D_{19} = \frac{\lambda_{DE}\left[D_{22} + \frac{(D_3 + \beta)\lambda_{DU} + (\lambda_{SU} + \lambda_{DU}) D_5}{\lambda_{DE} + \mu_{LT}}\right]}{\mu_{RN}} + \frac{\lambda_D (D_{16} + D_{17}) + (\beta_D \lambda_{DD} + \beta \lambda_{DU}) D_{18}}{\mu_{RN}} \quad (62)$$

$$D_{20} = \frac{\lambda_{DE} D_2 + 2(1-\beta_D)\lambda_{SD} D_{18}}{\lambda_S + \mu_{DE}} \quad (63)$$

$$D_{21} = \frac{\lambda_{DE} D_3 + 2(1-\beta)\lambda_{SU} D_{18}}{\lambda_S + \mu_{DE}} \quad (64)$$

$$D_{22} = \frac{\lambda_{DU} D_2 + \lambda_{DD} D_3 + (\lambda_{SU} + \lambda_{DU}) D_4}{\lambda_{DE} + \mu_0 + \mu_{LT}} + \frac{(\lambda_{SD} + \lambda_{DD}) D_5}{\lambda_{DE} + \mu_0 + \mu_{LT}} + \frac{(D_2 + \beta_D)\lambda_{DD} + (\lambda_{SD} + \lambda_{DD}) D_4}{\lambda_{DE} + \mu_0} \tag{65}$$

$$D_{23} = \frac{(D_2 + \beta_D)\lambda_{SD}}{\lambda_{DE} + \mu_0} + \frac{D_2 \lambda_{SU} + D_3 \lambda_{SD}}{\lambda_{DE} + \mu_0 + \mu_{LT}} \tag{66}$$

The $PFS_{1oo2}$ value is the sum of the probabilities P1 and $\gamma\cdot(P18+P20+P21)$:

$$PFS_{1oo2} = P_1 + \gamma(P_{18} + P_{20} + P_{21}) \tag{67}$$

The spurious trip rate of 1oo2-system will be given by the following equation:

$$PFS_{1oo2} = 1 - R_{Spurious\_1oo2}(t) \tag{68}$$

with:

$$\begin{aligned} R_{Spurious\_1oo2} &= \sum_{i=0}^{1} \binom{2}{i} R_{Spurious}^{2-i} \cdot (1 - R_{Spurious})^i \\ &= 2 \cdot R_{Spurious} - R_{Spurious}^2 \\ &= 2 \cdot e^{-STR_{1oo2} \cdot t} - e^{-2 \cdot STR_{1oo2} \cdot t} \end{aligned} \tag{69}$$

Let be $\gamma = e^{-STR_{1oo2} t}$, so the spurious trip rate of 1oo2-system will be given by the following equation:

$$y^2 + 2y - 1 + PFS_{1oo2} = 0 \tag{70}$$

There are two solutions for this equation, but only the positive value is accepted:

$$STR_{1oo2} = -\frac{\ln y}{t} = -\frac{\ln(-1 + \sqrt{2 - PFS_{1oo2}})}{t} \tag{71}$$

And the Mean Time To Failure Spurious is calculated as follows:

$$\begin{aligned} MTTF_{Spurious\_Trip\_1oo2} &= \int_0^{\infty} R_{Spurious\_Trip\_1oo2}(t) \cdot dt \\ &= \frac{3}{-2 \dfrac{\ln(-1 + \sqrt{2 - PFS}}{t}} \end{aligned} \tag{72}$$

## VI. EXAMPLE

The following parameters will be used as an example for an estimation of the parameters of spurious trip failure:

$$MTTR = 8h \Rightarrow \mu_R = \frac{1}{MTTR} = \frac{1}{8}$$
$$S = 0,5$$
$$DC = 0,9$$
$$\tau_{Test} = 24h \Rightarrow \mu_0 = \frac{1}{\tau_{Test}} = \frac{1}{24}$$
$$\beta_D = 0,01$$
$$\beta = 0,02$$
$$\lambda_B = 5 \cdot 10^{-6}$$
$$T = 8760h$$
$$\lambda_{DE} = \begin{bmatrix} 10^{-8} & 10^{-6} & 10^{-4} & 10^{-2} \end{bmatrix}$$
$$\mu_{DE} = \begin{bmatrix} 10^{-4} & 10^{-3} & 10^{-2} & 10^{-1} \end{bmatrix}$$
$$\mu_{RN} = 10^{-6}$$
$$\gamma = 0,01$$

### A. 1oo1-architecture

The following Figures (Fig. 9, Fig. 10 and Fig. 11) show the functions of $PFS_{1oo1}$, $STR_{1oo1}$ and $MTTF_{Spurious\_1oo1}$ in dependence on demand rate, which are deviated from Markov model in this work. At first, the effect of varying demand rate on the $PFS_{1oo1}$ (Fig. 9) is examined. The $PFS_{1oo1}$ function will increase, when the demand rate or demand duration increases. The $PFS_{1oo1}$-value will reach STL 4 when the demand rate is low and reach STL 2 when demand rate is high.

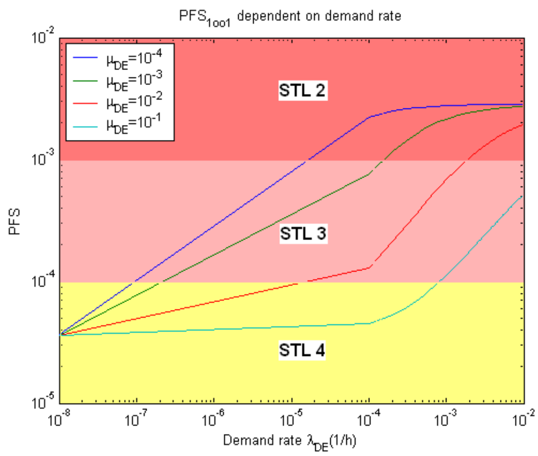


Fig. 9 PFS with different demand rate of 1oo1-architecture

Fig. 10 describes the function of $STR_{1oo1}$ which depends on the demand rate. Like the $PFS_{1oo1}$ function, the $STR_{1oo1}$ function will decrease when the demand rate or demand duration decrease. With a low demand rate the function of $STR_{1oo1}$ decreases slightly, but with a high demand rate the difference of $STR_{1oo1}$ is shown explicitly.

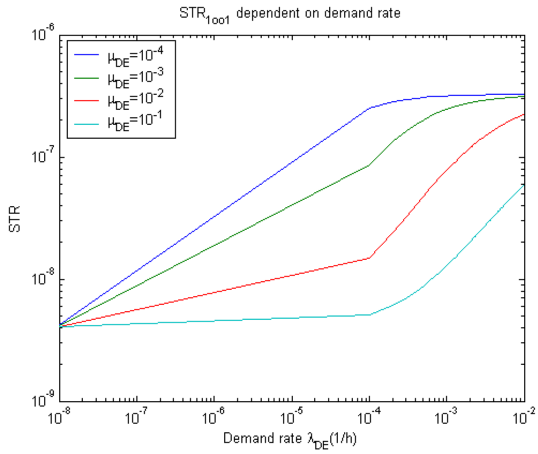


Fig.10 STR with different demand rate of 1oo1-architecture

The $MTTF_{Spurious\_1oo1}$ function is shown in the Fig. 11. While the $PFS_{1oo1}$ function and the $STR_{1oo1}$ function are proportional to demand rate and demand duration, the $MTTF_{Spurious\_1oo1}$ function is inversely proportional to the demand rate and demand duration.

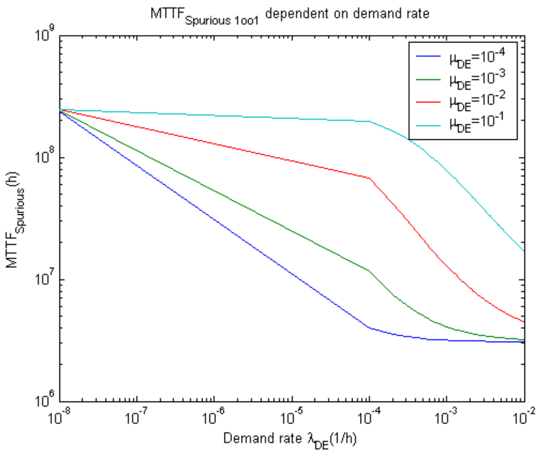


Fig. 11 $MTTF_{Spurious}$ with different demand rate of 1oo1-architecture

Fig. 12 shows the function of $STR_{1oo1}$ in dependence on diagnostic coverage factor DC with different methods. The function of $STR_{1oo1}$ by method of Machleidt & Litz [16] is like the function of $STR_{1oo1}$ but using the reliability block diagram method, which is deviated from this work. $STR_{1oo1}$ function by ANSI/ISA TR84.00.02-2002 [3] is another set of functions.

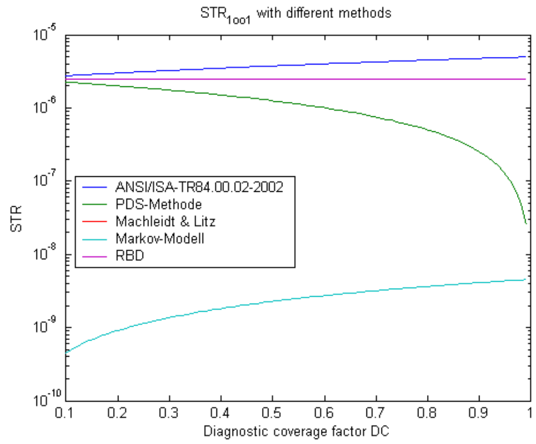


Fig. 12 STR with different methods of 1oo1-architecture

### *B. 1oo2-architecture*

The effect of varying demand rate on the $PFS_{1oo2}$ is displayed in Fig. 13. The $PFS_{1oo2}$ function will increase, when the demand rate or demand duration increases. The $PFS_{1oo2}$-value will reach STL 4 when the demand rate and the demand duration are low , and reach the higher level when demand rate or demand duration is high.

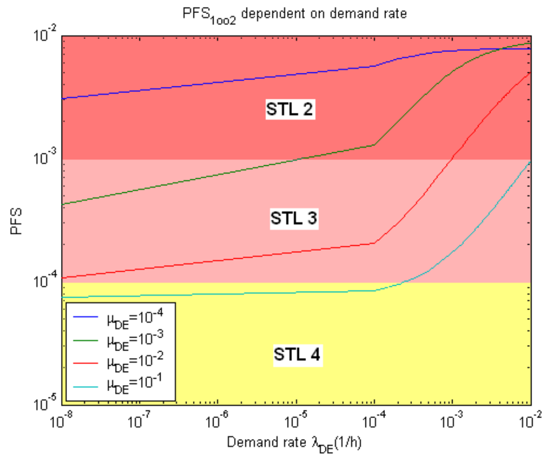


Fig. 13 PFS with different rate of 1oo2-architecture

Fig. 14 describes the function of $STR_{1oo2}$ which depends on the demand rate. Like the $PFS_{1oo2}$ function, the $STR_{1oo2}$ function will decrease when the demand rate or demand duration decrease. With a low demand rate the function of $STR_{1oo2}$ is strictly monotonically decreasing, but not strictly decreasing with a high demand rate, and the x-value of the saddle point is 1/8760 ≈ $1{,}14.10^{-4}$.

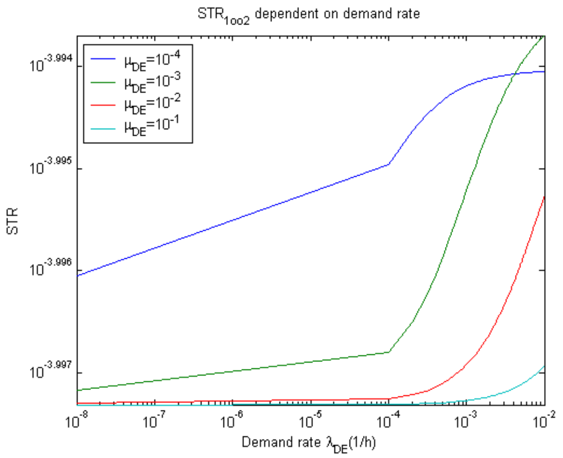


Fig. 14 STR with different demand rate of 1oo2-architecture

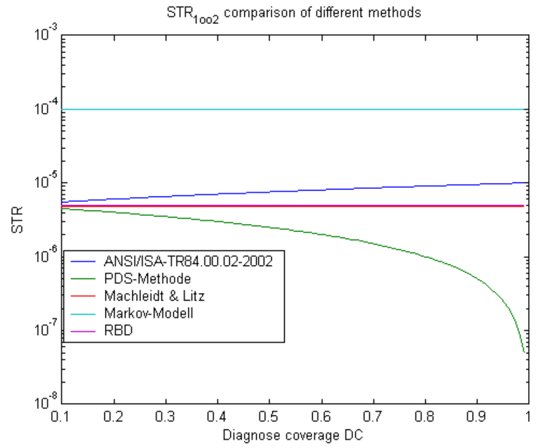


Fig. 16 STR with different methods of 1oo2-architecture (1)

The $MTTF_{Spurious\_1oo2}$ function is shown in Fig. 15. $MTTF_{Spurious\_1oo2}$ value increases when the demand rate or demand duration decreases. The $MTTF_{Spurious\_1oo2}$ function is strictly monotonically increasing if the demand rate is low, but not strictly increasing if the demand rate is high. Like the $PFS_{1oo2}$ -, $STR_{1oo2}$ -curve the x-value of the saddle point of the $MTTF_{Spurious\_1oo2}$ curve is $1{,}14.10^{-4}$.

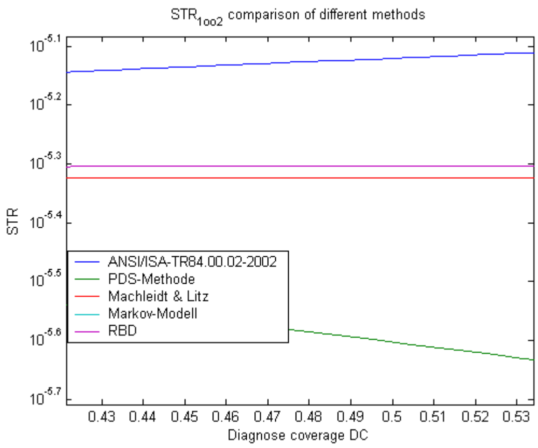


Fig. 17 STR with different methods of 1oo2-architecture (2)

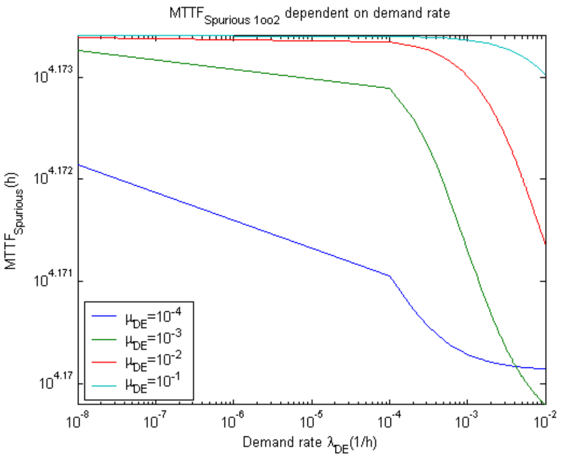


Fig. 15 $MTTF_{Spurious}$ with different rate of 1oo2-architecture

Fig. 16 and Fig. 17 show the function of $STR_{1oo2}$ in dependence on diagnostic coverage factor DC with different methods, with Fig. 17 is the enlargement of Fig. 16. The function of $STR_{1oo2}$ utilising the method of Machleidt & Litz [16] is like the functions of $STR_{1oo2}$ using the reliability block diagram method, which is different to this work. $STR_{1oo2}$ function using the Markov model, which is different from this work, is over another function.

## VII. Conclusion

This article has analyzed the relationship between SIS reliability and demand rate, as well as the demand duration for 1oo1- and 1oo2-architecture. Finally, the Markov model provides advanced method to analyse this relationship than the block diagram. Therefore, it can be stated that it is not always possible to use a common formula of reliability calculation for all system modes. PFS values of a system architecture are not equal to all modes of operation. The same is true for STR and $MTTF_{Spurious}$. This is based on the recent revision of IEC 61508.

## References


[1] IEC 61508, "Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems," Part 1-7, Deutsche Fassung EN 61508:2010.

[2] H. Guo, X. Yang, "A simple reliability block diagram method for safety integrity verification", Reliability Engineering and System Safety, Volume 92, Issue 9, Page(s):1267-1273, 2007.

[3] ISA-TR84.00.02-2002, Part 1-5, 2002

[4] IEC 61511, "Functional safety: safety instrumented systems for the process industry sector", Part 1-3, CDV versions.
[5] M. Houtermans, "Safety Availability versus Prozess Availability, Introduction Spurious Trip Levels™", White paper, Risknowlogy Expert in Risk, Reliability and Safety, May 2006.
[6] C.d. Sails, "SIL certs can seriously impair plant safety", Process Engineering, January / February, 2008
[7] G. Gabor and D. Zmaranda, "Techniques used to design safe and reliable critical control or shutdown systems", Journal of Computer Science and Control Systems, 01/2008.
[8] SINTEF, "Reliability prediction method for safety instrumented systems", PDS Method Handbook, 2010 Edition", SINTEF 2010.
[9] M. A. Lundteigen, M. Rausand, "Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas", Reliability Engineering and System Safety 93 (2008), 1208-1217.
[10] Hui Jin, Mary Ann Lundteigen, Marvin Rausand, "Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation", Reliability Engineering and Safety, Volume 96, Issue 3, Page(s): 365-373, 2011.
[11] J. Bukowski, "Incorporating process demand into models for assessment of safety system performance", Proceedings of RAMS'06 symposium, USA, 2006.
[12] F. Innal, Y. Dutuit, A. Rauzy, J. Signoret, "New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems", Journal of Risk and Reliability, Volume 224, Page(s): 75-86, July 2010.
[13] Yiliu Liu, Marvin Rausand, "Reliability assessment of safety instrumented systems subject to different demand modes", Journal of Loss Prevention in the Process Industries 24, Page(s): 49-56, 2011.
[14] P. Holub, J.Börcsök, "Advanced PFH Calculation for Safety Integrity Systems with High Diagnostic", ICAT 2009 XXII International Symposium on Information, Communication and Automation Technologies, 2009.
[15] Dave Macdonald, "Practical Hazops, Trips and Alarms, IDC Technologies, Netherlands", 2004.
[16] Konstantin Machleidt, Lothar Litz, "An optimization approach for safety instrumented system design", Reliability and Maintainability Symposium (RAMS), Page(s) 1-6, 2011 Proceeding – Annual.
[17] prEN ISO 13849-1, DRAFT, "Safety of machinery – Safety-related parts of control systems – Part 1. General principles for design (ISO/DIS 13849-1:2004)", 2004.
[18] Börcsök J., Holub P., "Consideration of Common Cause Failures in Safety Systems, Recent Advances in Systems, Communications & Computers", Selected Papers from the WSEAS Conferences in Hangzhou, China, April 6-8, 2008.
[19] Holub P., Börcsök J., "LOPA – A Method to Analyse Safety Integrity Systems according to IEC 61511", $6^{th}$ WSEAS Int. Conference on Computational Intelligence, Man-Machine Systems and Cybernetics, Tenerife, Spain, December 14-16, 2007.
[20] Börcsök J., Holub P., "Model for Determining of MTTF for Safety Related Electronical Systems by Monte Carlo Simulation by means of 1 2oo4-System", Proceedings of the $6^{th}$ WSEAS International Conference on Applied Computer Science, Tenerife, Canary Islands, Spain, December 16-18, 2006.