Spurious activation analysis of safety-instrumented systems

Abraham Almaw Jigar, Yiliu Liu, Mary Ann Lundteigen

Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

Abstract

Safety-instrumented systems are used in industries to prevent the development of a process upset into an accident. For most processes, the desired response in the case of a process upset is to shutdown the process, and most safety-instrumented systems are designed so that this state is achieved in response to also specific item failures or loss of power. The side-effect of such fail-safe design may be that the safety-instrumented system is prone to spurious activation, meaning that the normal operation of the process may be interrupted in an untimely manner. In the design of a safety-instrumented system, it is therefore important to quantify the rate of spurious activation and to check the need for additional measures to ensure a stable as well as safe operation of the process. Unfortunately, weaknesses have been identified in formulas for spurious trip rate, and the aim of this paper is to present a further development of currently available analytical formulas. The paper builds the new formulas on a thorough discussion of the concepts of spurious activation, failure classification, and failure propagation in a safety-instrumented system. The proposed formulas are compared with existing ones for selected architectures, and some conclusions are drawn.

Keywords: Spurious activation; Spurious operation; Spurious trip rate (STR); Safety-instrumented system (SIS); Systematic failure, Common cause failure (CCF)

1. Introduction

Safety is a concern for complex and hazardous processes and equipment where process upsets can result in damage to humans, the environment, or material assets of high value to the society. To reduce the risk to an acceptable level, it is necessary to introduce various technical, organizational, and human measures to either prevent or mitigate the consequences of hazardous events. In the process industry, dedicated safety-instrumented systems (SISs) are installed to respond automatically or in response to manual initiation under hazardous situations. A SIS comprises (i) sensors or manual initiators, used to detect or alert about the hazardous event, (ii) programmable logic solver(s), used to decide on how to respond, and (iii) final elements, such as valves, breakers, and switches which interact with the process to achieve or maintain a safe state. Fig. 1 shows a simplified safety-instrumented system.

The SIS is usually designed for fail-safe operation, meaning that the safe state is achieved in response to loss of power and specific fault conditions (e.g., loss of communication and signal out of range). This is a favorable design principle as long as the safe state is well defined and the

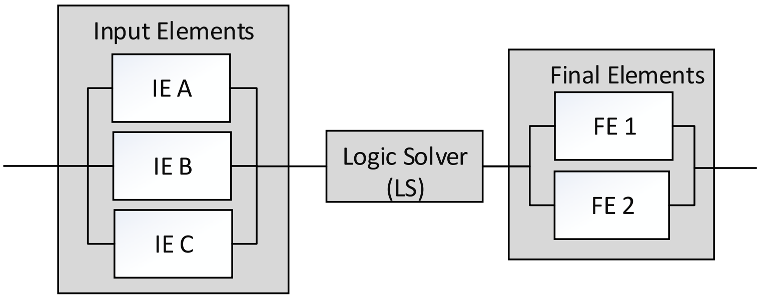

Figure 1: Reliability Block diagram of a SIS

same under all relevant modes of operation. For process industry, the safe state has traditionally been regarded as the state where the production is stopped, but this is not without exceptions. For subsea oil and gas production and processing facilities, the safest state may sometimes be to maintain production, rather than shutting down, due to the risk of major damages and loss of containment during the shutdown and restarting. In the design of a SIS, it is therefore important to not only consider the ability to perform when demanded, but also to the ability to enter a safe state upon defined fault conditions. As the two measures may put preference to different design solutions, it is necessary for system designers to balance the two to achieve the highest overall level of risk reduction.

While reliability measures and formulas in key standards of SIS are rather well defined for determining the ability of the SIS to function when demanded, no or very limited attention is given to spurious activations and the calculation of spurious activation (trip) rate. IEC 61508 [1], the generic standard for SISs, considers all spurious activations as safe failure and suggests no quantification of these. IEC 61511 [2], the process sector standard developed with basis in IEC 61508, suggests that the maximum allowable spurious trip rate (STR) is to be calculated, but gives no further advice on how. Some guidelines and industry practices, like the PDS method [3] and ISA TR 84.00.02 [4], have proposed formulas for quantifying the rate of spurious activations, but they are based on slightly different assumptions. Lundteigen and Rausand [5] did a thorough review of the treatment of spurious activations, but they did not consider the possibility of needing different types of formulas for different SIS subsystems. Even though formulas are developed on the basis of having a clear idea of what to include in the failure rate estimation, there are different views on failure classifications (e.g., [1, 3, 6]), for example on the definition of systematic and random hardware failures, and whether to include the contribution from both types or only the latter. This lack of clarity is not only relevant for spurious activation analysis, but has a general implication on reliability assessments of SISs. Understanding the assumptions and limitations of such classifications and being careful on what type of failures should be included and excluded in the model has a paramount importance.

The main purpose of this paper is, in light of the discussions above, to (i) clarify some fundamental concepts such as definition of spurious activation, its relationship with failure classification, and considerations and assumptions that are important to decide before attempting to quantify spurious trip rates, and (ii) to develop a new set of formulas for quantifying the spurious trip rate with basis in (i). A numerical example is carried out to compare the results with formulas in a selection of literatures.

The remaining part of the paper is structured as follows: Section 2 presents a discussion on the definitions and interpretations of spurious activation suggested by several authors and proposes a suitable definition. In Section 3, failure causes, classification and propagation to spurious activation of the SIS are detailed, for purposes of quantitative analysis. Based on this, analytical formulas specific to each subsystems are developed in Section 4. Finally, Section 5 provides some concluding remarks and ideas for further work.

2. Definitions and interpretations of spurious activations

Many standards and guidelines regard spurious activations as a safe event, or safe failure, since the result of the activation should be a transition to the safe state. For example, both IEC 61511 [2] and IEC 61508 [1] mention spurious activation as an example of a *safe failure* of a SIS element.

It has been suggested by Lundteigen and Rausand [5] that there are three categories of spurious activation: (i) at the SIS element level, involving a spurious operation (SO) failure of a single SIS element, (ii) at the subsystem level, where a combination of SO failures, or other events, like loss of communication, lead to a spurious activation of the subsystem, and finally, (iii) at the plant level, where a spurious activation of a subsystem or other events, such as loss of power, results in a new state of the plant (e.g., shutdown). An SO failure is defined as an activation of a SIS element without the presence of a specified process demand (see more about SO failure in [5]). The latter category is also mentioned in ISA TR 84.00.02 [4], where spurious activation is defined as failures leading to process shutdown.

The analogy suggested between "safe" and spurious activation failures does not always hold. A spurious activation may or may not have an adverse effect on safety. Consider the following cases where spurious activations have adverse effect on safety: (i) Spurious activation (release) of airbag system in a car would not be safe while driving in high speed. (ii) A spurious opening of a shutdown valve may result in an over-pressuring of downstream equipment and loss of containment. (iii) A spurious stop of a subsea processing facility, may introduce hydrate plugs in the pipelines which, when released, can result in over-pressuring of receiving facilities. In most cases, any start-up after a shutdown increases the risk of new hazardous events. For example, the BP Texas city refinery incident in March 2005 that caused 15 fatalities and 170 injuries occurred in relation to a start-up [7, 8]. This was also the case for the Tesoro Anacortes-Washington refinery accident in April 2010 [9]. (iv) Spurious activation imposes unnecessary thermal and mechanical stress on elements, which may result in a more rapid degradation of components [8, 5]. (v) Reoccurring spurious signals from sensors may result in loss of confidence to the equipment, and eventually bypassing of the signals [5].

The most suited definition according to the authors of this paper is the one suggested in ISOTR 12489 [10]: *activation of a SIS in an untimely manner*. Untimely is characterizing the spurious activation as an event, without judging whether the consequence of the event is safe or dangerous. Untimely activation occurs when (i) the SIS performs its function without the presence of a process demand or (ii) the SIS abandons the state achieved in response to the timely or untimely activation. An example of (i) would be a spurious closure of a shutdown valve, while

(ii) would be the same valve spuriously opening after having been closed. In this paper, the main attention is directed to (i), but in some cases, it may be favorable to also consider (ii). It is also decided to use the approach from [5], where spurious operation (SO) is referred to as spurious activation at the element level, spurious trip at the subsystem (SIF[1]) level, and spurious shutdown at the plant level.

As mentioned, the consequence of a spurious trip can be economical, through production stop, or safety related, or both, and should thus be addressed in the EUC (equipment under control) risk assessment in order to achieve an optimal risk reduction. To handle the risk reduction associated with spurious trip in a formal way, one option may be to establish a standardized requirement, as for example proposed by Houtermans [11]. The author proposed the concept of spurious trip level (STL), as a complement to safety integrity level (SIL) which is used as a performance measures for the likelihood of experiencing dangerous failures, as shown in Table 1. As pointed out by Rausand [6], the approach has, however, been criticized because the levels are associated with economic loss alone, and the adverse effect on safety is not included.

Table 1: Spurious trip level [11]

STL	Probability of Fail Safe Per Year	Spurious trip cost
X	$\geq 10^{-(x+1)}$ to$<10^{-x}$	...
...	...	...
5	$\geq 10^{-6}$ to$<10^{-5}$	10M-20M EUR
4	$\geq 10^{-5}$ to$<10^{-4}$	5M-10M EUR
3	$\geq 10^{-4}$ to$<10^{-3}$	1M-5M EUR
2	$\geq 10^{-3}$ to$<10^{-2}$	500k-1M EUR
1	$\geq 10^{-2}$ to$<10^{-1}$	100k-500k EUR

3. Evaluation of the assumptions and limitations for STR of a SIF

When quantifying measures for spurious activation, it is important to consider the following questions: (i) Under what conditions and events would an element or a subsystem give an spurious activation? (ii) What would be the cascading effects on a subsequent level (i.e., for the SIF or the plant)? (iii) Are the fundamental arguments employed in failure classification, for the purpose of quantification, reasonable? (iv) What are the implications of the assumptions made in the failure classification on the STR predictions? In this section we will try to address these questions.

3.1. Factors contributing to the STR of a SIF

The consequences of spurious activation may be different for the three SIS subsystems. Spurious operation (SO) failure of individual elements may cause the SIS to spuriously activate. Spurious signals (i.e. SO failure) from *k* or more elements in a *k*-out-of-*n* (*koon*) architecture initiates

[1] SIF - safety-instrumented function carried out by a safety-instrumented system.

a spurious activation of the SIS, while no spurious activation occurs with $k-1$ or less elements having a spurious signal. The same situation applies to the logic solver subsystem. Final elements often interact directly on or with the process or equipment being protected. Therefore, some impact from spurious operation of final elements is expected even if the number is less than k in a $k$oo$n$ architecture. For example, a single valve closure in a 2oo2 architecture may reduce the production performance.

The operational strategy in relation to dangerous failures may also add more events to consider for spurious activation. In the presence of a specific number of dangerous detected (DD) failures (i.e., $n-k+1$ or more DD failures in a $k$oo$n$ architecture) it may be unsafe to continue operation and the SIS may automatically shutdown in response to this situation. In a multi-channel subsystem, we may therefore have the situation that an spurious activation is the result of SO failures, DD failures or a combination of both. Some formulas, like in [5] and [6], account for SO and DD failures separately, but we have not identified in literatures that the combination of such failures is considered in analytical formulas. ISA TR 84.00.02 [4] provides STR formulas with a combination of SO and DD failures, but the derivation of these formulas is not explained. Formulas in existing literatures are presented and discussed in Section 4, and thereby new formulas are developed to quantify the impact of SO and DD failures.

The design philosophy in connection with utility functions also plays a significant role in the spurious activation of SISs. A SIS may be designed as de-energize-to-trip or energize-to-trip. De-energize-to-trip means the SIS performs its function upon loss of power or utility systems like hydraulics, while the energize-to-trip design means that the SIS is unable to operate under the same conditions (and will maintain the state it had achieved before the loss occurred). A de-energize-to-trip system is therefore more prone to spurious activations, as loss of power will also contribute to such activations, than energize-to-trip. Nevertheless, it cannot be concluded which one of the two design principles is the safest, as this would entirely depend on what is the safe state, and if the safe state remains the same under different modes of operation. In the quantification of spurious trip rate, it is therefore important to consider the design philosophy of the SIS, to also check if the contribution from loss of utility functions must be included. Contribution from loss of utility functions may need to cover [10]:

- loss of sufficient power supply, e.g. electric/hydraulic power supply
- loss of auxiliary supply, e.g. uninterruptible power supply (UPS)
- loss of (or faulty) communication

It should be noted that loss of utility function may be an issue also for energize-to-trip design, but then in relation to dangerous failures of SIS elements. Loss of utility may result in impeding the ability of SIS elements to carry out the safety function (i.e. a dangerous failure), and the affected elements will therefore have a dangerous failure that is either detected or undetected. The effects of the DD failure mode must be considered for the specific SIS in question, and may be modeled as a separate event, for example as an explicit CCF event of DD failures. This paper however does not cover the quantification of utility systems as such, but the proposed approach/concept for the three SIS subsystems may be extended and used to accommodate utility systems.

Depending on how often the demand occurs, SISs are classified as low-demand systems and high-demand systems, where the frequency of once per year is set as a borderline [1]. The state of the EUC (and also the SIS itself) after the SIS has successfully responded to a demand may vary significantly for low- and high-demand systems. In case of low-demand systems the EUC often remains in the safe state after the SIS has responded to a demand while in high-demand systems the EUC may return immediately back to normal operation. Hence, the demand frequency and demand duration may have impact on the spurious activation of the SIS and should be accounted for in the STR calculation, as argued by Pham and Schwarz [12]. However, in this paper demand is not taken into account (i.e., equivalent to say that demand assumed to be too infrequent or that demand duration is negligible) and the main focus is on low-demand system.

3.2. Failure classifications

It is important to have a well defined approach to the classification of failures, in the sense of deciding which failure modes and failure effects are important to include in the quantification of STR. In this paper, the failure classification is based on terminologies used in IEC 61508 [1]. Even so, there are some unclear issues in the application, since most focus is directed to the handling of DD and DU failures in this and related standards.

3.2.1. Considerations about systematic failures and random hardware failures

SIS elements may subject to either random or systematic failures that may affect the STR. According to IEC standards [1, 2], systematic failure cannot be predicted statistically with a reasonable accuracy due to their deterministic nature. These are failures introduced due to errors made in design, manufacturing, installation, usage and maintenance [1]. For example, an SO failure caused by a software error in the logic solver or by a design error leading to internal leakage of a valve actuator. A sensor responding to a false demand can also be an example of systematic failure, as this may be attributed to a design error (unable to foresee the false demand to choose a proper design accordingly).

Random hardware failures, as defined by IEC 61508 [1], are failures occurring at a random time, which result from one or more of the possible degradation mechanisms in the hardware. The underlying assumption is that the operating and maintenance conditions are within the design envelope [13]. Following this definition of IEC 61508, the PDS method [3] specifically stated that the cause for random hardware failure is aging. Internal leakage of a valve actuator due to natural degradation (aging) can be an instance of SO random hardware failure [5]. However, it seems impractical to claim or differentiate in most cases if a failure is due merely to aging, as aging can overlap with other factors such as excessive stress, improper handling, maintenance and so on. An SO failure of a sensor, for example, may be caused by an electronic component failure. However, electronic components can fail without a recognizable degradation (aging) mechanism. Consequently, Rausand [6] argues that random hardware failure of an element is not only due to aging but can also be caused, for example, by inadequate maintenance, stress, human error and so on. The categorization of some human errors as a cause for random hardware failure is also acknowledged by ISOTR 12489 [10].

IEC 61508 suggests that only random hardware failures to be included in the quantitative analysis, but not all analysts and guidelines agree on that (e.g., [3, 10]). The PDS method [3] claims that systematic failures should be included (implicitly in the element's failure rate) and one of the arguments for this is that excluding systematic failures provides unrealistic (optimistic) result. Some authors are even more optimistic and argue that systematic failures can be predicted explicitly (e.g., [4, 14]).

The main purpose of classifying failures as systematic and random hardware failures is to establish a basis for quantification by identifying causes (failures) that can statistically be predicted. It is therefore important that the analyst has a clear idea about the benefit and limitation of the classification and also what causes are (should be) included and excluded from the STR analysis.

3.2.2. Considerations about independent and common cause failures

Failures may occur due to an independent cause (independent failures) or due to a shared cause (common cause failures [CCF]). A CCF may be defined as an event involving multiple component failures, that occur close in time and due to a shared cause [1, 15, 10, 6]. A CCF may be caused by an explicitly known cause(s), e.g., power system failure that is common for several elements, or by causes with no clear deterministic explanation. Modeling explicit CCFs is often preferred if the causal relationship between the cause and the failure (event) is very clear and the analysis can be supported by data (e.g., the rate of occurrence). Implicit modeling is often more suited if these conditions are not met. The effect of a CCF can be a complete SIS failure (i.e., spurious activation of the SIS), or a partial failure (i.e., SO failure of an element). Some CCF models make the assumptions about complete SIS failure (e.g., standard beta factor model), while others allow to also model the effects of partial failure (e.g., multiple greek letter model and extended beta factor model) [15]. The most frequently used model in the process industry is based on the beta factor model, or the extended beta factor model. These models are discussed in detail in Section 4.4.

With regard to dangerous failures, few initiatives have been taken to support the models with experience data about why and how often CCFs occur. Two exceptions are the ICDE project carried out in the nuclear industry [16, 17] and an initiative through the PDS forum in Norway for the oil and gas industry [18, 19]. The PDS method had recently come up with an estimate for β ranging from 11% (for process shutdown valve) to 20% (for fire dampers). An alternative to the data driven estimate for β is to use various types of checklists (e.g. the checklist proposed in IEC 61508), or to rely on expert judgments made in data handbooks, such as the PDS data handbook [20]. The IEC 61508 has proposed the maximum β value to be 5% for logic solver and 10% for sensor and final element. CCFs may occur at different points in time and for dangerous failures, in particular dangerous undetected (DU) failures, all dependent failures occurring in the same test interval can reasonably be attributed to the same CCF. Since each SO failure will be notified, it is likely that a repair is carried out before the next failure occurs, if the cause is not a shock-like exposure. It is therefore unreasonably conservative to assume as high β value for SO failures as for dangerous failures. Moreover, the underlying causes for SO failures are different from dangerous failures and thus care should be taken while quantifying STR due to CCF.

This section discussed important aspects of spurious activation to establish a clear ground to formulate a quantification measure for SIS operating in low-demand mode. In the following section, spurious activation implies an untimely activation of a SIS, and that results from untimely activation of one of the SIS subsystems, which is referred to as spurious trip. Spurious trip, in turn, results from untimely activation of constituting elements/channels (i.e. spurious operation). The term spurious shutdown is used for process shutdown as a result of spurious activation of the SIS. In addition to spurious operation (SO) failures, DD failures are treated as contributing factor to spurious trip and thus they are accommodated in the formulas established in the section below.

4. Spurious trip rate of a SIF

The main reliability measure for spurious activation is the rate of occurrence, often called spurious trip rate (STR) [6], but other measures could also be used, for example, the probability of experiencing a spurious activation before the next scheduled plant shutdown. In this paper, the focus is placed on the STR, as this rate can also be used as input for determining other measures such as the loss in production availability. The STR of a SIF can be calculated by summing up the STRs of the individual subsystems, which may fail due to either independent (I) or CCFs (C), as shown in Eq. 1.

$$\mathrm{STR}_{\mathrm{SIF}} = \sum_{i \in \{\mathrm{IE,LS,FE}\}} \left(\mathrm{STR}_i^{(\mathrm{I})} + \mathrm{STR}_i^{(\mathrm{C})} \right) \tag{1}$$

Only the three subsystems, namely input element (IE), logic solver (LS) and final element (FE) are considered. Loss of utility may be an integral part of the CCF evaluation at the subsystem level or for the whole SIF. The quantification of the contribution of loss of utility is outside the scope of this paper, but a very good treatment of the reliability quantification of redundant power systems can be seen in [21, 22]. Moreover, one should also consider the contribution from false demand. Sensors may give wrong signals by reading a false demand that has a similar form and characteristics as the real demand. If λ_{FD} is the rate of occurrence of a false demand and $\mathrm{PFD}_{\mathrm{avg}}$ is the average probability of dangerous failure of the SIF on demand, then the STR due to the false demand can be calculated as

$$\begin{aligned} \mathrm{STR}_{\mathrm{FD}} &= \lambda_{\mathrm{FD}}(1 - \mathrm{PFD}_{\mathrm{avg}}) \\ &\approx \lambda_{\mathrm{FD}} \end{aligned} \tag{2}$$

A brief discussion about false demand can be found in [6].

4.1. Existing approaches

An overview of formulas for calculating the STR that have been identified in the literatures are presented in Table 2. Note that in order to be consistent we use SO failure (λ_{SO}) even if safe failure (λ_{S}) are used as notation in the original papers (e.g. in [4, 23, 3]). For the purpose of brevity, we also use λ instead of $(1-\beta)\lambda$ for independent failures as $(1-\beta)\lambda \approx \lambda$.

The formulas and the associated literatures do not discus the need to model subsystems differently, due to the different effect of SO and DD failures on subsystems. The formulas presented in the table above are developed and suggested to be used irrespective of the type of subsystem. However, as discussed in Section 3 SO and DD failures do not impose the same effect across subsystems and thus it is important to develop formulas that are specific to a specific subsystem.

Table 2: Existing STR formulas

Author	Formula					
	STR		Independent failures		CCF	
ISA TR 84.00.02 [4]	$\text{STR}_{1\text{oo}1}$	=	$\lambda_{\text{SO}} + \lambda_{\text{DD}}$			
	$\text{STR}_{1\text{oo}i}$	=	$i\,(\lambda_{\text{SO}} + \lambda_{\text{DD}})$	+	$\beta(\lambda_{\text{SO}} + \lambda_{\text{DD}})$	for $i = 2, 3$
	$\text{STR}_{2\text{oo}2}$	=	$2\lambda_{\text{SO}}\,(\lambda_{\text{SO}} + \lambda_{\text{DD}})\,\text{MTTR}^{*}$	+	$\beta(\lambda_{\text{SO}} + \lambda_{\text{DD}})$	
	$\text{STR}_{2\text{oo}3}$	=	$6\lambda_{\text{SO}}\,(\lambda_{\text{SO}} + \lambda_{\text{DD}})\,\text{MTTR}$	+	$\beta(\lambda_{\text{SO}} + \lambda_{\text{DD}})$	
	$\text{STR}_{2\text{oo}4}$	=	$12\lambda_{\text{SO}}\,(\lambda_{\text{SO}} + \lambda_{\text{DD}})^{3}\,\text{MTTR}^{2}$	+	$\beta(\lambda_{\text{SO}} + \lambda_{\text{DD}})$	
Lundteigen and Rausand [5]	$\text{STR}_{k\text{oo}n}$	=	$n\lambda_{\text{SO}} \sum_{i=k-1}^{n-1} \binom{n-1}{i} p^{i}(1-p)^{n-1-i} + n\lambda_{\text{DD}} \sum_{i=n-k}^{n-1} \binom{n-1}{i} q^{i}(1-q)^{n-1-i}$	+	$\beta_{\text{SO}}\lambda_{\text{SO}} + \beta_{\text{DD}}\lambda_{\text{DD}}$	
			where $p = 1 - \mathrm{e}^{-\lambda_{\text{SO}}\text{MTTR}_{\text{SO}}}$, and $q = 1 - \mathrm{e}^{-\lambda_{\text{DD}}\text{MTTR}_{\text{DD}}}$			
		$\approx$	$n\binom{n-1}{k-1}\lambda_{\text{SO}}^{k}\text{MTTR}_{\text{SO}}^{k-1} + n\binom{n-1}{n-k}\lambda_{\text{DD}}^{n-k+1}\text{MTTR}_{\text{DD}}^{n-k}$	+	$\beta_{\text{SO}}\lambda_{\text{SO}} + \beta_{\text{DD}}\lambda_{\text{DD}}$	
Innal et al. [23]	$\text{STR}_{k\text{oo}n}$	=	$\frac{n!}{(n-k)!}\lambda_{\text{SO}}^{k} \prod_{i=1}^{k-1} \text{EMDT}_{i} + \frac{n!}{(k-1)!}\lambda_{\text{DD}}^{n-k+1} \prod_{i=1}^{n-k} \frac{\text{MTTR}_{DD}}{i}$	+	$\beta_{\text{SOU}}\lambda_{\text{SOU}} + \beta_{\text{SOD}}\lambda_{\text{SOD}} + \beta_{\text{DD}}\lambda_{\text{DD}}$	
			where $\text{EMDT}_{i}^{**} = \frac{\lambda_{\text{SOU}}}{\lambda_{\text{SOU}}+\lambda_{\text{SOD}}}\left(\frac{\tau}{i+1} + \text{MRT}\right) + \frac{\lambda_{\text{SOD}}}{\lambda_{\text{SOU}}+\lambda_{\text{SOD}}}\text{MTTR}_{\text{SOD}}$			
PDS method [3]	$\text{STR}_{1\text{oo}n}$	=	$n\lambda_{\text{SO}}$			
	$\text{STR}_{k\text{oo}n}$	=			$\beta C_{(n-k+1)\text{oo}n}\lambda_{\text{SO}}$ for $i = 1, 2, 3$	
			where C is the modification factor for various voting configurations			

*MTTR is the mean time to restoration, which is the same for SO and DD failures

**EMDT_i is equivalent mean downtime time of detected SO failures (SOD) and undetected SO failures (SOU), τ is the test interval to detect SOU failures and MRT is mean repair time of SOU failure

In addition, the formulas do not account for the possible combination of SO and DD failures in a multichannel subsystem. For example, one SO and one DD failures in a 2oo3 input element subsystem may have similar effect as two DD failures.

The PDS method [3] formula disregards the contribution from independent failures for *k*oo*n*, where $k > 1$, but in light of previous discussions about CCFs occurring at slightly different times, the approach should be applied with caution. Contribution from DD failures is acknowledged, but no formula is suggested in the PDS method for this purpose. ISA TR 84.00.02 [4] assumes that a single DD failure leads to spurious activation of 1oo2/3 architecture, even if a single DD failure does not prevent the SIF from functioning on demand. The formulas assume also the same MTTR for SO and DD failures, but this may not necessarily be the case due to having different failure causes.

Innal et al. [23] have introduced the equivalent mean downtime concept in relation to spurious activation. The equivalent mean downtime, a weighted average of the downtimes due to detected and undetected failures where failure rates are used as weights, corresponds to MTTR associated to SO failures in other literatures (e.g. [5]). This measure has reasonably been used to compute PFD_{avg} since part of dangerous failures in an element can be detected or undetected. However, it is questionable to implement this measure for spurious activation as SO failure of an element is an evident failure. If a sensor fails SO, it means that a dangerous situation is detected (spuriously) and thus a message will be sent to the control room and the failure becomes evident which will then lead to an action (isolation, restoration and so on). The same would also apply to SO failure in the logic solver. For final element, an SO failure can not be hidden as it is an (spurious) activation due to a failure, for example, in the actuator.

Some basic differences have also been noticed between authors regarding CCF modeling, especially for 1oo*n*, where $n > 1$, architectures. Using a β-factor model, do we need to consider contribution of CCF due to SO failure for 1oo$n$? The PDS method [3] does not consider while other authors (i.e. [4, 5, 23]) have considered it.

Based on these and some of the considerations discussed in Section 3 we propose a new set of formulas in the remaining part of this sections. The new formulas are presented first for independent failures in Section 4.2, and then for CCFs in Section 4.3. Separate formulas are suggested for input elements, logic solver, and final elements.

4.2. New formulas for independent failures

4.2.1. General model assumptions

An element at a certain point in time can be in one of the following states: SO failure (SO), dangerous detected (DD), dangerous undetected (DU) or functioning (OK). These states at the element level are mutually exclusive and exhaustive as illustrated in Fig. 2. Assume now that elements are identical and independent of each other as well as their failure rates are constant over time. With these assumptions, if we have a subsystem consisting n elements, the following properties can be derived:

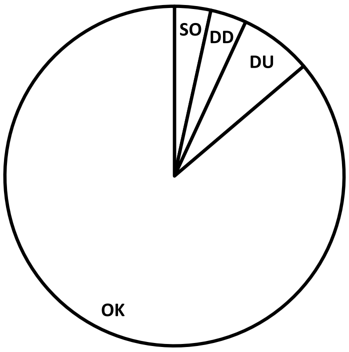

Figure 2: Mutually exclusive and exhaustive states of an element

1. Because elements are independent, the outcome on one element does not affect the outcome on other elements.
2. Because elements are identical, each element has a set of possible outcomes (SO, DD, DU, OK) and the probability that a particular outcome will occur is the same in each element (let the associated probabilities be p, q, r and $s = 1 - p - q - r$).

These two properties allow to use a multinomial distribution, a generalized form of binomial distribution. Let X, Y and Z be the number of times that SO, DD, and DU failures occur. Then, the probability that SO occurs x times, DD occurs y times and DU occurs z times can be calculated as

$$\begin{aligned} g(X = x, Y = y, Z = z) &= \frac{n!}{x!y!z!(n - x - y - z)!} p^x q^y r^z (1 - p - q - r)^{n-x-y-z} \\ &\approx \frac{n!}{x!y!z!(n - x - y - z)!} p^x q^y r^z \end{aligned} \tag{3}$$

At a specific point in time, we may find the element in the OK state or DU state. From the perspective of STR, neither of the two states has a direct contribution. However, for time dependent STR calculation it would not be the same because once an element fails DU it may not give rise to spurious activation until the failure is corrected and restored to an OK state. Since in this paper we are computing a time-independent STR, these two states (DU and OK) can be merged and considered as a "no trip (NT)" state. Therefore, we will have only three states SO, DD and NT with the associated probabilities p, q and $1 - p - q$. As a result, the probability of finding x SO failures and y DD failures can be rewritten as

$$\begin{aligned} g(X = x, Y = y) &= \frac{n!}{x!y!(n-x-y)!} p^x q^y (1-p-q)^{n-x-y} \\ &\approx \frac{n!}{x!y!(n-x-y)!} p^x q^y \end{aligned} \tag{4}$$

Moreover, if the purpose is to compute STR due to only SO failures we will then have a binomial situation such that DD failure will be considered as a NT state, i.e.

$$g(X = x) = \frac{n!}{x!(n-x)!} p^x (1-p)^{(n-x)} \approx \frac{n!}{x!(n-x)!} p^x \tag{5}$$

and for DD failures

$$g(Y = y) \approx \frac{n!}{y!(n-y)!} q^y \tag{6}$$

The quantification approach proposed in this paper is based on the approach first proposed by Lundteigen and Rausand [5] and published later in the book by Rausand [6]. For a single element the STR is approximated by the associated failure rate, i.e.

$$\mathrm{STR}_{\mathrm{SO}} = \frac{1}{\mathrm{MTBF}_{\mathrm{SO}}} = \frac{1}{\mathrm{MTTF}_{\mathrm{SO}} + \mathrm{MTTR}_{\mathrm{SO}}} = \frac{\lambda_{\mathrm{SO}}}{1 + \lambda_{\mathrm{SO}}\mathrm{MTTR}_{\mathrm{SO}}} \approx \lambda_{\mathrm{SO}} \tag{7}$$

$$\mathrm{STR}_{\mathrm{DD}} = \frac{1}{\mathrm{MTBF}_{\mathrm{DD}}} = \frac{1}{\mathrm{MTTF}_{\mathrm{DD}} + \mathrm{MTTR}_{\mathrm{DD}}} = \frac{\lambda_{\mathrm{DD}}}{1 + \lambda_{\mathrm{DD}}\mathrm{MTTR}_{\mathrm{DD}}} \approx \lambda_{\mathrm{DD}} \tag{8}$$

the approximation is valid for small MTTR compared to MTTF. In situations where restoration is considerably long such as in subsea production and processing systems, the above approximation may not be valid. However, in this paper we applied this approximation. It is also assumed that the restoration activity is perfect that it brings the subsystem in an "as good as new" state. Further, once the element is activated spuriously, the assumption is that it remains faulty until restoration is completed.

4.2.2. Specific considerations for input element

For a *koon* input element subsystem spurious trip occurs when either k or more elements fail SO, $n-k+1$ or more elements fail DD, or combination of SO and DD failures occur. As mentioned, upon $n - k + 1$ DD failures, the SIS is no longer available for safety such that the process has to be shutdown. When a combination of $n-k+1$ SO and DD failures occur – the combination contains no greater than $k-1$ SO failures and no greater than $n-k$ DD failures – the system is no longer available as it is the case for $n-k+1$ DD failures. The assumption here is that once an element sends false signal, it should no longer be trusted and can then be considered as a failed element. It may be possible that the failed element is isolated and the system runs with degraded mode. However, degraded mode is outside the scope of this paper.Thus, spurious activation occurs in two mutually exclusive possibilities and the STR formula can be calculated considering these possibilities:

1. first is an SO failure and then
   - $k-1$ SO failures occur before the first SO failure is being restored, or
   - $n-k$ combination of SO and DD failures occur before the first SO failure is being restored
2. first is a DD failure and then
   - $n-k$ DD failures occur before the first DD failure is being restored, or
   - $n-k$ combination of SO and DD failures occur before the first DD failure is being restored

For a $k$oo$n$ system, let $f_\gamma(x,y)$ be the probability that x and y number of SO *and* DD failures occur out of $n-1$ elements before the restoration of the first failure, denoted γ, is completed. γ will be either SO or DD failure whichever occurs first. From Eq. 4, we have,

$$\begin{aligned} f_\gamma(X=x, Y=y) &= \frac{(n-1)!}{x!y!(n-x-y-1)!}\left(1-\mathrm{e}^{-\lambda_{\mathrm{SO}}\mathrm{MTTR}_\gamma}\right)^x\left(1-\mathrm{e}^{-\lambda_{\mathrm{DD}}\mathrm{MTTR}_\gamma}\right)^y \\ &\approx \frac{(n-1)!}{x!y!(n-x-y-1)!}(\lambda_{\mathrm{SO}}\mathrm{MTTR}_\gamma)^x(\lambda_{\mathrm{DD}}\mathrm{MTTR}_\gamma)^y \end{aligned} \tag{9}$$

Further, $f_\gamma(x)$ is the probability that x number of SO failures out of $n-1$ elements occur before the restoration due to γ failure is completed. Similar definition can be made for $f_\gamma(y)$. We have

$$\begin{aligned} f_\gamma(X=x) &\approx \frac{(n-1)!}{x!(n-x-1)!}(\lambda_{\mathrm{SO}}\mathrm{MTTR}_\gamma)^x \\ f_\gamma(Y=y) &\approx \frac{(n-1)!}{y!(n-y-1)!}(\lambda_{\mathrm{DD}}\mathrm{MTTR}_\gamma)^y \end{aligned} \tag{10}$$

Moreover, the probability of finding w number of SO *or* DD failure before the restoration due to γ failure is completed is

$$f_\gamma(W=w) \approx \frac{(n-1)!}{w!(n-w-1)!}((\lambda_{\mathrm{SO}}+\lambda_{\mathrm{DD}})\mathrm{MTTR}_\gamma)^w \tag{11}$$

When an input element experiences SO failure, its safety function will be terminated until the restoration is completed. If the operational philosophy does not allow operating in degraded mode, the decision will then be to shut down when the number of "out of order" elements (due to SO and DD failure) is greater than $n - k$. Operating in degraded mode is used to maintain production although it may impact the level of the achieved risk reduction. STR formulas for common architectures without considering degraded mode are presented below:

$$
\begin{aligned}
\mathrm{STR}^{(\mathrm{I})}_{\mathrm{IE,\,1oo1}} &= \lambda_{\mathrm{SO}} + \lambda_{\mathrm{DD}} && (12)\\
\mathrm{STR}^{(\mathrm{I})}_{\mathrm{IE,\,1oo2}} &= 2\lambda_{\mathrm{SO}} + 2\lambda_{\mathrm{DD}} f_{\mathrm{DD}}(Y = 1) \approx 2\left(\lambda_{\mathrm{SO}} + \lambda^2_{\mathrm{DD}}\mathrm{MTTR}_{\mathrm{DD}}\right) && (13)\\
\mathrm{STR}^{(\mathrm{I})}_{\mathrm{IE,\,2oo2}} &= 2\lambda_{\mathrm{SO}} f_{\mathrm{SO}}(X = 1) + 2\lambda_{\mathrm{DD}} \approx 2\left(\lambda^2_{\mathrm{SO}}\mathrm{MTTR}_{\mathrm{SO}} + \lambda_{\mathrm{DD}}\right) && (14)\\
\mathrm{STR}^{(\mathrm{I})}_{\mathrm{IE,\,1oo3}} &= 3\lambda_{\mathrm{SO}} + 3\lambda_{\mathrm{DD}} f_{\mathrm{DD}}(Y = 2) \approx 3\left(\lambda_{\mathrm{SO}} + \lambda^3_{\mathrm{DD}}\mathrm{MTTR}^2_{\mathrm{DD}}\right) && (15)\\
\mathrm{STR}^{(\mathrm{I})}_{\mathrm{IE,\,2oo3}} &= 3\lambda_{\mathrm{SO}} f_{\mathrm{SO}}(W \geq 1) + 3\lambda_{\mathrm{DD}} f_{\mathrm{DD}}(W \geq 1)\\
&\approx 3\lambda_{\mathrm{SO}} f_{\mathrm{SO}}(W = 1) + 3\lambda_{\mathrm{DD}} f_{\mathrm{DD}}(W = 1)\\
&= 6\left(\lambda_{\mathrm{SO}} + \lambda_{\mathrm{DD}}\right)\left[\lambda_{\mathrm{SO}}\mathrm{MTTR}_{\mathrm{SO}} + \lambda_{\mathrm{DD}}\mathrm{MTTR}_{\mathrm{DD}}\right] && (16)\\
\mathrm{STR}^{(\mathrm{I})}_{\mathrm{IE,\,2oo4}} &= 4\lambda_{\mathrm{SO}}\left[f_{\mathrm{SO}}(X \geq 1) + f_{\mathrm{SO}}(Y \geq 2)\right] + 4\lambda_{\mathrm{DD}}\left[f_{\mathrm{DD}}(Y \geq 2) + f_{\mathrm{DD}}(X = 1, Y = 1)\right]\\
&\approx 4\lambda_{\mathrm{SO}}\left[f_{\mathrm{SO}}(X = 1) + f_{\mathrm{SO}}(Y = 2)\right] + 4\lambda_{\mathrm{DD}}\left[f_{\mathrm{DD}}(Y = 2) + f_{\mathrm{DD}}(X = 1, Y = 1)\right]\\
&= 12\lambda_{\mathrm{SO}}\mathrm{MTTR}_{\mathrm{SO}}\left[\lambda_{\mathrm{SO}} + \lambda^2_{\mathrm{DD}}\mathrm{MTTR}_{\mathrm{SO}}\right] + 12\lambda^2_{\mathrm{DD}}\mathrm{MTTR}^2_{\mathrm{DD}}\left[\lambda_{\mathrm{DD}} + 2\lambda_{\mathrm{SO}}\right] && (17)\\
\mathrm{STR}^{(\mathrm{I})}_{\mathrm{IE,\,3oo4}} &= 4\lambda_{\mathrm{SO}}\left[f_{\mathrm{SO}}(X \geq 2) + f_{\mathrm{SO}}(Y = 1)\right] + 4\lambda_{\mathrm{DD}} f_{\mathrm{DD}}(W \geq 1)\\
&\approx 4\lambda_{\mathrm{SO}}\left[f_{\mathrm{SO}}(X = 2) + f_{\mathrm{SO}}(Y = 1)\right] + 4\lambda_{\mathrm{DD}} f_{\mathrm{DD}}(W = 1)\\
&= 12\lambda_{\mathrm{SO}}\mathrm{MTTR}_{\mathrm{SO}}\left[\lambda^2_{\mathrm{SO}}\mathrm{MTTR}_{\mathrm{SO}} + \lambda_{\mathrm{DD}}\right] + 12\lambda_{\mathrm{DD}}(\lambda_{\mathrm{SO}} + \lambda_{\mathrm{DD}})\mathrm{MTTR}_{\mathrm{DD}} && (18)
\end{aligned}
$$

It seems complex, if not impossible, to develop a general $k$oo$n$ formula for input element. However, it is straightforward to develop a formula for any $k$oo$n$ system by using the same concept as used above.

4.2.3. Special considerations for final elements

Final elements normally interact with the EUC, and the effect of SO and DD failures on the safety function and the EUC may therefore be different from input elements. For a $k$oo$n$ input element subsystem at least k SO failures are needed for the SIS to activate spuriously, but for final elements less than k SO failures may have an impact. Consider a 2oo3 valve. Even if two elements are required to function for the SIS to function, one spurious activation may, for example, cause undesired flow-pressure combination, so that the EUC needs to be shutdown. It is therefore reasonable to calculate STR for a $k$oo$n$ final element due to SO failure as $n\lambda_{\mathrm{SO}}$. Observe that under this assumption the STR contribution from combination of failures (SO failures *and* DD failures) vanishes.

DD failures of final elements, e.g. valve stuck in open position, bell failed to ring and so on, also behave differently. As far as a spurious activation performed by the SIS is concerned DD failures should be considered in STR calculation only if the SIS is able to use the remaining final elements for activation. It may therefore be meaningless to talk about spurious activation due to DD failure of $n$oo$n$ final element. For a $k$oo$n$ architecture, where $k < n$, it depends on how many

DD failures can be tolerated before a spurious activation. If we denote the maximum tolerable number of DD failures by ν, i.e., upon $\nu + 1$ DD failures the SIS activates, STR can be calculated as

$$\begin{aligned} \mathrm{STR}^{(\mathrm{I})}_{\mathrm{FE},\, koon} &= n\lambda_{\mathrm{SO}} + n\lambda_{\mathrm{DD}} \sum_{i=\nu}^{n-k-1} \binom{n-k-1}{i} q^{i}(1-q)^{n-k-1-i} \qquad \text{for } \nu < n-k \\ &\approx n\lambda_{\mathrm{SO}} + n\binom{n-k-1}{\nu}\lambda_{\mathrm{DD}}^{\nu+1}\mathrm{MTTR}_{\mathrm{DD}}^{\nu} \end{aligned} \tag{19}$$

Note that if $\nu \geq n-k$ the SIS is no longer be able to perform its function since more than $n-k$ dangerous failures cause the SIS to fail – activation by the SIS is not possible. Nevertheless, if the SIS is not able to perform its function when more than $n-k$ elements fail DD, the EUC may be shutdown manually by using other means. For example, if a SIS in a subsea gas compression system fails to stop a flow downstream upon a demand, an action can be taken to stop the flow upstream using valves such as a master valve. In other words, another safety layer takes over the safety function of the SIS and brings the EUC into a safe state. If this can be considered as spurious activation of the SIS, i.e. failure of the final elements subsystem leading to unintended shutdown, STR due to final elements failure can be calculated as

$$\begin{aligned} \mathrm{STR}^{(\mathrm{I})}_{\mathrm{FE},\, \mathrm{koo}n} &= n\lambda_{\mathrm{SO}} + n\lambda_{\mathrm{DD}} \sum_{i=n-k}^{n-1} \binom{n-1}{i} q^{i}(1-q)^{n-1-i} \\ &\approx n\lambda_{\mathrm{SO}} + n\binom{n-1}{n-k}\lambda_{\mathrm{DD}}^{n-k+1}\mathrm{MTTR}^{n-k} \end{aligned} \tag{20}$$

4.2.4. Logic solver

An SO failure of the logic solver is a failure that results in sending false shutdown signal to the actuator in the final element. If we consider a *koon* logic solver the effect of SO failure will be the same as the input element subsystem – at least k SO failures needed to spuriously activate the SIS.

As input and final elements, no more than $n-k$ DD failures can be tolerated for the logic solver subsystem. Like final element if more than than $n-k$ elements have DD failure, the SIS cannot automatically be activated by itself. If however manual shutdown follows upon more $n-k$ DD failures, the same formula as input elements can be used. These two scenarios are treated in the final element.

4.3. Numerical comparison

In this section a numerical comparison between the proposed method and the methods suggested by ISA TR 84.00.02 [4] and Lundteigen and Rausand [5] is made using the following input data: $\lambda_{\mathrm{SO}} = 1.00\mathrm{E}-06, \lambda_{\mathrm{DD}} = 5.00\mathrm{E}-06, \mathrm{MTTR}_{\mathrm{DD}} = \mathrm{MTTR}_{\mathrm{SO}} = 8$ hours. As can be observed from Table 3, for 1oo1 architecture there is no difference among all the methods. ISA provides conservative results for 1oo2 and 1oo3 architectures as it assumes a single DD failure leads to spurious activation. The proposed method provides the same result as Lundteigen and Rausand

[5] for all 1oo$n$ architectures because there is no contribution from combination of SO and DD failures as well as for these architectures one SO failure is sufficient for final element to spuriously activate. For 2oo3 and 2oo4 input element architectures the proposed method provides slightly higher result due to contribution from combination of failures. The contribution from combination of failure modes (which is the product of SO and DD failure rates) is smaller than that of the contribution from same failure modes due to the fact that $\lambda_{\mathrm{DD}}^2 \geq \lambda_{\mathrm{DD}} \cdot \lambda_{\mathrm{SO}} \geq \lambda_{\mathrm{SO}}^2$, if $\lambda_{\mathrm{DD}} \geq \lambda_{\mathrm{SO}}$, or $\lambda_{\mathrm{SO}}^2 \geq \lambda_{\mathrm{DD}} \cdot \lambda_{\mathrm{SO}} \geq \lambda_{\mathrm{DD}}^2$, if $\lambda_{\mathrm{SO}} \geq \lambda_{\mathrm{DD}}$. Nevertheless, such small differences become significant for an installation with many SIFs since the total STR (of the installation) is the sum of the STRs of all the SIFs, if they are independent of each other. For multichannel final element, however, applying the same assumption and formula as input element will provide an overly optimistic result, as one SO failure may be sufficient to experience spurious activation. As can be seen from the table, for 2oo3 and 2oo4 architectures the difference is respectively in three and five orders of magnitude compared to the result by Lundteigen and Rausand [5] formula.

Table 3: Numerical comparison

Author	1oo1	1oo2	1oo3	2oo3	2oo4
ISA TR 84.00.02 [4]	6.00E-6	1.20E-5	1.80E-5	2.88E-10	1.66E-19
Lundteigen and Rausand [5]	6.00E-6	2.00E-6	3.00E-6	1.25E-9	9.61E-11
Proposed method (IE)	6.00E-6	2.00E-6	3.00E-6	1.73E-9	9.62E-11
Proposed method (FE)	6.00E-6	2.00E-6	3.00E-6	3.00E-6	4.00E-6

4.4. Contribution from CCF

The IEC 61508 [1] checklist for quantifying β-factor, enclosed in annex D of part 6, distinguishes logic solver from input and final elements. Nevertheless, once the respective β-factors are determined, the same formula can be used regardless of the type of the subsystem. This is the case when the tradition β-factor model is used. If the extended β-factor model is used, slight calibration is needed as discussed below.

4.4.1. CCF contribution for koon, $k > 1$

Traditional β-factor model: Assume that β-factor for SO failures can be estimated in a similar way as β-factor for dangerous failures, and further the assumptions (see Section 3.2.2) of β-factor model are reasonable for spurious activation. For a $k$oo$n$ subsystem, where $k > 1$, the contribution of CCF can then be calculated as

$$\mathrm{STR}^{(\mathrm{C})} = \beta_{\mathrm{SO}}\lambda_{\mathrm{SO}} + \beta_{\mathrm{DD}}\lambda_{\mathrm{DD}} \tag{21}$$

This approach is commonly used by many authors [4, 5, 23] as shown in Table 2. ISA [4] however uses the same β for SO and DD failures.

Extended β-factor model: The traditional β-factor model assumes that the probability that all n elements in a parallel architecture fail given CCF has occurred is the same, regardless of the voting and degree of redundancy. The intention of this extension is thus to consider the voting of the architecture. The extended model uses the traditional β-factor for 1oo2 architecture to compute

Table 4: The PDS method $C_{i\text{oo}j}$ values [3]

$i \backslash j$	2	3	4	5	6
1	1.0	0.5	0.3	0.2	0.15
2	-	2.0	1.1	0.8	0.6
3	-	-	2.8	1.6	1.2
4	-	-	-	3.6	1.9
5	-	-	-	-	4.5

Table 5: The IEC 61508 $C_{i\text{oo}j}$ values [1]

$i \backslash j$	2	3	4	5
1	1.0	0.5	0.3	0.2
2	-	1.5	0.6	0.4
3	-	-	1.75	0.8
4	-	-	-	2

β-factor for other $k$oo$n$ architectures using a suitable multiplier, denoted $C_{i\text{oo}j}$. For example, for 1oo3 architecture, the probability that the third element fails given that CCF has already caused the two elements to fail is assumed to be 0.5 and we know the probability that these two elements fail due to CCF is β. Therefore, a 1oo3 architecture fails due to CCF is $0.5 \cdot \beta$. Note that IEC 61508 also acknowledges the relevance of this extension and has provided its own multipliers. Table 4 and Table 5 present the multipliers suggested by the PDS method and the IEC 61508 respectively.

As far as CCF is concerned, for input elements at least k SO failures or at least $n - k + 1$ DD failures are required in order for the SIS to spuriously activate. For final elements, a single SO failure may be sufficient to be considered as spurious activation of the SIS. If so, a $k$oo$n$ final element is the same as 1oo$n$, and CCF modeling for 1oo$n$ is treated in Section 4.4.2. However, if k SO failures are required for spurious activation of the SIS, the same formula as input elements can be used. Thus, STR of a subsystem based on the extended CCF model can be calculated as

$$\text{STR}^{(\text{C})} = \tilde{\beta}_{\text{SO}} C_{(n-k+1)\text{oo}n} \lambda_{\text{SO}} + \tilde{\beta}_{\text{DD}} C_{k\text{oo}n} \lambda_{\text{DD}}, \quad 1 < k \leq n \tag{22}$$

where $\tilde{\beta}_{\text{SO}}$ and $\tilde{\beta}_{\text{DD}}$ are β-factors for 1oo2 architecture. To understand easily why $(n - k + 1)$oo$n$ is used in the first term in Eq. 22, think in terms of fault tolerance. For $k$oo$n$ architecture, fault tolerance in relation to SO failure is $k - 1$. This means that the architecture can be rewritten as $(n - k + 1)$oo$n$F, i.e., at least $(n - k + 1)$ elements should not be in SO fault in order for the architecture to be in functioning (F) state with respect to SO.

Note that for final elements, Eq. 22 assumes that when more than $n - k$ DD failures occur the EUC will be shutdown by other means, and that is considered as spurious activation of the SIS. If the design is to tolerate v DD failures, at the most, then $C_{k\text{oo}n}$ in the second term in Eq. 22 should be replaced by $C_{(n-v)\text{oo}n}$.

4.4.2. CCF Contribution for *k*oo*n*, *k*=1

Two different approaches have been used by authors:

- ISA [4] and Lundteigen et al. [5] use the same formula as Eq. 21, which quantifies the contribution of CCF even if a single SO failure leads to spurious activation. With this approach, since the CCF is fractionated from the total failure rate, the result will be strange. Spurious activation occurs due to either independent failure of elements with rate $n(1-\beta)\lambda$, or CCF with rate $\beta\lambda$. Since $n(1-\beta)\lambda + \beta\lambda = (n - (n-1)\beta)\,\lambda$, $\text{STR}^{(\text{C})}$ due to SO failure will be

$(n - (n-1)\beta_{\mathrm{SO}})\,\lambda_{\mathrm{SO}}$. This result indicates that the inclusion of CCF reduces the STR, which is unreasonable.

The approach would be correct if, hypothetically speaking, the CCF rate is not fractionated from the total failure rate, i.e., spurious activation occurs due to independent failures with rate $n\lambda_{\mathrm{SO}}$ and CCF with rate λ^*_{SO}, such that $\mathrm{STR}^{(\mathrm{C})} = n\lambda_{\mathrm{SO}} + \lambda^*_{\mathrm{SO}}$. Similarly, implementing the C-factor will also avoid the strange result obtain in the above paragraph. In the C-factor, which is introduced by Evans et al. [24], the total failure rate is the sum of individual failure rates λ, not $(1 - C) \cdot \lambda$, and CCF rate $C \cdot \lambda$.

- The PDS method [3] (which considers only SO failures and of course uses extended β-factor model) does not consider CCF for 1oo$n$. This approach gives a conservative result compared to the method used by ISA [4] and Lundteigen et al. [5].

5. Concluding remarks

This paper has directed the attention to spurious activation of a SIS aiming to develop further some concepts and formulas in the existing literatures. Effort has been made to critically assess the underline concepts, definitions and assumptions related to spurious activation and spurious trip rate calculation. Several definitions have been presented and their limitations with respect to capturing some scenarios under different modes of operation and under different safe-state definitions are identified. It would be a mistake to fully associate spurious activations with safe failures, as seen in IEC standards and some literatures, as it depends on the mode of operation of the EUC when the activation is taking place and the definition of the safe-state.

The paper has also attempted to discuss briefly fundamental concepts and assumptions employed while performing quantitative analyses. We have studied critically the failure classification theory that has been used as a tool to classify failure causes according to their suitability to be statistical predicted. We see this as a fundamental concept that needs to be clear to understand what we are measuring by STR formulas, and to know what and why factors are included and excluded from the calculation – including whether it is possible in practice to clearly identify these factors, for example, during data collection. It is observed that there is a flaw in the classification of failures as random hardware and systematic failures and it is our suggestion for further research to look into fundamental concepts of failure classification from practical perspective.

Modeling of failures as common cause for purposes of spurious activation is also found to be questionable from several viewpoints. Unlike dangerous failures, spurious activation failures are evident. Hence, applying the same modeling approach as for dangerous failures (e.g. $\mathrm{PFD}_{\mathrm{avg}}$) may lead to unrealistic result. Since some CCFs are due to systematic failures, an attempt to quantify CCF contradicts with the argument, for example by the IEC 61508, that systematic failures cannot be statistically predicted. Further, since the nature of the causes of CCFs are diversified, in the sense that some are lethal-shock and others are not and the fact that CCF models are used to cater for causes for which explicit modeling is impossible because of limited knowledge and data, one should take into consideration the associated degree of uncertainty in the estimates.

The paper has also questioned some of the commonly available STR formulas and suggested a new set of formulas. Compare to the existing ones, the suggested formulas have two main distinct features. It is obvious that the development of spurious activation of a SIS from input elements is quite different from final elements. Thus, formulas are developed specific to input elements and final elements. Logic solver resembles sensor so the same formula can be used. The second distinct feature is that formulas are developed by taking into account more possible scenarios. What has been overlooked in some existing formulas is the possibility of having a combination of failure (i.e. both SO failures and DD failures) in a multi-channel subsystem, even though numerically they do not significantly alter the result.

The paper has not covered degraded mode as an alternative decision upon an element failure. For a 2oo3 input element subsystem, for example, upon an SO/DD failure or a combination of one SO and one DD failure, the decision could be to continue operating with a degraded mode. Such a philosophy is not taken into account in this paper, but it could be a good topic for further research. Further, in this paper STR formulas are developed only for common architectures. It is thus our suggestion for further research to look into developing a general STR formula for $k$oo$n$ architecture.

The paper argued that SO failures are evident failures. The involved items to make the failures evident (i.e., items involving from detecting the failure to displaying in the screen in the control room) may or may not be part of the diagnostic system, and it may be important that, in the quantification of STR, the reliability of such items is taken into account. The paper has not covered such items and so the developed formulas may require some modification if the items should be included. Moreover, aspects related to the quantification of SO failure rates are not detailed, and it is our suggestion for further research to address such topics.

Acknowledgment

The authors would like to thank the reviewers for their comments and suggestions to the improvement of this paper.

References

[1] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, Tech. Rep., International Electrotechnical Commission, Geneva, 2010.

[2] IEC 61511, Functional safety - Safety Instrumented Systems For the Process Industry sector, Tech. Rep., International Electrotechnical Commission, Geneva, 2003.

[3] SINTEF, Reliability prediction methods for safety instrumented systems, PDS method handbook, SINTEF, Trondheim, 2013.

[4] ISA TR 84.00.02, Safety instrumented functions (SIF)–safety integrity level (SIL) evaluation techniques, Part2: Determining the SIL of A SIF via simplified equations., Tech. Rep., Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 2002.

[5] M. A. Lundteigen, M. Rausand, Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas, Reliability Engineering & System Safety 93 (8) (2008) 1208–1217, ISSN 09518320.

[6] M. Rausand, Reliability of Safety-Critical Systems: Theory and Applications, John Wiley & Sons, 2014.

[7] F. I. Khan, P. R. Amyotte, Modeling of BP Texas City refinery incident, Journal of Loss Prevention in the Process Industries 20 (2007) 387–395, ISSN 09504230.

[8] S. B. Panikkar, Preventing Spurious Trips in the Chemical Process Plant : The role of Functional safety Management, The TÜV Rheinland Functional Safety Symposium, Köln, Germany, 2014.

[9] U.S. Chemical Safety and Hazard Investigation Board, Investigation Report on Tesoro Anacortes Refinery Accident: Catastrophic Rupture of Heat Exchanger (Seven Fatalities), Tech. Rep., 2014.

[10] ISOTR 12489, Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems, Draft, Tech. Rep., International organization for standardization, Geneva, 2012.

[11] M. Houtermans, Safety Availability versus Prozess Availability, Introduction Spurious Trip Levels™, White paper, Risknowlogy Expert in Risk, Reliability and Safety, 2006.

[12] N. T. D. Pham, M. Schwarz, Evaluation of Spurious Trip Rate of SIS dependent on demand rate, Mathematical Methods and Systems in Science and Engineering, ISBN 9781618042811, 17–24, 2015.

[13] M. Gentile, A. E. Summers, Common Cause Failure : How Do You Manage Them ? 25 (4) (2006) 331–338.

[14] M. Khalaquzzaman, H. G. Kang, M. C. Kim, P. H. Seong, A model for estimation of reactor spurious shutdown rate considering maintenance human errors in reactor protection system of nuclear power plants, Nuclear Engineering and Design 240 (10) (2010) 2963–2971, ISSN 00295493.

[15] P. Hokstad, M. Rausand, Common cause failure modeling: status and trends, in: Handbook of performability engineering, Springer, 621–640, 2008.

[16] NEA ICDE, Project Report: Collection and analysis of common-cause failures of safety and relief valves (NEA/CSNI/R(2002)19), Tech. Rep., Issy-les-Moulineaux: Nuclear Energy Agency, France, 2002.

[17] NEA ICDE, Project Report: Collection and analysis of common-cause failures of check valves (EA/CSNI/R(2003)15), Tech. Rep., Issy-les-Moulineaux: Nuclear Energy Agency, France, 2003.

[18] S. Hauge, S. Hå brekke, M. A. Lundteigen, Using field experience in the treatment of Common Cause Failures in reliability assessment, in: Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014, CRC Press/Balkema, ISBN 9781138026810, 1885–1893, 2015.

[19] S. Hauge, A. S. Hoem, S. Hå brekke, M. A. Lundteigen, Report CCFs in safety instrumented systems, SINTEF, Trondheim, 2014.

[20] S. Hauge, T. Onshus, Reliability Data for Safety Instrumented Systems: PDS Data Handbook, SINTEF, Trondheim, 2010.

[21] B. W. Jenney, D. J. Sherwin, Open & Short Circuit Reliability of Systems of Identical Items, IEEE Transactions on Reliability 35 (5) (1986) 532–538, ISSN 0018-9529.

[22] D. Malon, On a common error in open and short circuit reliability computation, IEEE Transactions on Reliability 38 (3) (1989) 275–276, ISSN 00189529.

[23] F. Innal, Y. Dutuit, M. Chebila, Safety and operational integrity evaluation and design optimization of safety instrumented systems, Reliability Engineering & System Safety 134 (2015) 32–50, ISSN 09518320.

[24] M. Evans, G. Parry, J. Wreathall, On the treatment of common-cause failures in system analysis, Reliability engineering 9 (2) (1984) 107–115.