Deriving Spurious Trip Rate Formulae

Dr Fan Ye, CFSE, FS Eng, GICSP, CEng, MIET | Principal Consultant, ESC Ltd, The Breeze at Carnoustie House, Kelvin Close, Birchwood, Warrington WA3 7PB

IEC 61511 (IEC, 2017) requires a spurious trip rate be specified as part of the Safety Requirement Specification (SRS) for a Safety Instrumented Function (SIF). However, safety engineers are often preoccupied with determining and verifying the Safety Integrity Level (SIL), Probability of Failure on Demand (PFD) for low demand SIF or Frequency of Failure per Hour (PFH) for high demand/continuous SIF, and are unfamiliar with the concept of spurious trip rate. The issue is exacerbated by the fact that no formulae for calculating spurious trip rate are provided in the functional safety standards such as IEC 61508 (IEC, 2010) and IEC 61511 (IEC, 2017).

This paper explains the concept of spurious trip and its importance in the design of a SIF. Each SIF has a primary objective to ensure safety (to meet its safety requirements). In addition, the SIF should keep its spurious trip rate to a minimum in order to avoid unnecessary spurious trips that could lead to loss of production, and potential increased safety risk due to human errors during reset and restart process.

This paper derives simplified formulae for calculating spurious trip rate for many common configurations such as 1 out of 1 (1oo1), 1oo2 and 2oo3, and a generalised formula that can be used for any M out of N (MooN) configuration. The Reliability Block Diagram (RBD) method is used in derivation of these formulae, and explains how RBDs used for calculating PFD / PFH can be converted to RBDs for calculating spurious trip rate and their underlying relationships. These will help safety engineers understand the relationships between PFD / PFH and Spurious Trip Rate. Issues and pitfalls are identified in constructing RBDs for spurious trip rate calculation. Examples and case studies will be used to illustrate the concepts and ideas presented in the paper.

Keywords: Spurious Trip, PFD, PFH, RBD, SIL, MooN, SRS, IEC 61511

1. Introduction

IEC 61511 (IEC, 2017) Part 1 Clause 10.3.2 requires that the “maximum allowable spurious trip rate for each SIF” be specified as part of the Safety Instrumented System (SIS) Safety Requirements Specification (SRS).

A spurious trip is the activation of a SIF when there is no demand. Spurious trip has a number of synonyms including spurious operation, spurious activation, false trip and so on. Since a SIF or safety function is designed to put the Equipment Under Control (EUC) into a safe state, spurious trips are associated with safe failures, as opposed to dangerous failures where the affected SIF fails to activate when there is a demand.

IEC 61508 (IEC, 2010) Part 4 Clause 3.6.8 defines “safe failure” as:

> failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:
>
> a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or
>
> b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state

Because spurious trip is only associated with safe failures, the requirement of specifying maximum allowable Spurious Trip Rate (STR) for each SIF is often ignored by safety engineers. Safety engineers and consultants are often preoccupied with calculating Probability of Failure on Demand (PFD) for low demand SIFs or frequency of Failure per Hour (PFH) for high demand / continuous SIFs, as these are the key parameters for determining the Safety Integrity Level (SIL) of a SIF. The issue is compounded by the fact that there is limited literature on how to calculate STR, and IEC 61511 (IEC, 2017) and IEC 61508 (IEC, 2010) offers no formulae for the calculation of STR.

Spurious trip rate needs to be taken into account during the design of a SIF for a number of reasons, including:

- High spurious trip rate undermines operator’s trust on the SIF, which may result in the SIF being bypassed / inhibited temporarily or permanently thus undermine the functional safety;
- High spurious trip rate increases the need for unnecessary human intervention to investigate and restart the process, with increased opportunity for human errors thus undermine the functional safety;
- High spurious trip rate leads to unnecessary process shutdowns, with associated production loss.

This paper presents a simplified approach for deriving STR formulae from the existing knowledge of Reliability Block Diagram (RBD) and PFD / PFH formulae that are often familiar to safety engineers and consultants.

2. Reliability Block Diagram (RBD)

Reliability Block Diagram is defined by IEC 61078 (IEC, 2016) as logical, graphical representation of a system showing how the success states of its sub-items (represented by blocks) and combination thereof, affect system success state. RBD can be used to derive analytical formulae for reliability and availability. As a result, RBD has been widely used in the field of reliability engineering, and by safety engineers to accurately present the configuration of a SIF and calculate the corresponding PFD or PFH. This section provides a more detailed description of RBD as it is used later on in this paper to derive the STR formulae.

2.1. RBD basics

An RBD has two end points connected with a number of functional blocks depicted as rectangles. Each block in the diagram represents a function of a component. If the function is available, there is connection through the block, and if the function is failed, there is no connection through the block. If there is connection between the two end points, the system is functioning.

Two basic structures (or a combination of both) can be used in an RBD:

- Series structure: a system that is functioning if and only if all of its constituent components are functioning. Figure 1 gives an example of a series structure.
- Parallel structure: a system that is functioning if at least one of its constituent components is functioning. Figure 2 gives an example of a parallel structure.

Figure 1. Example series structure

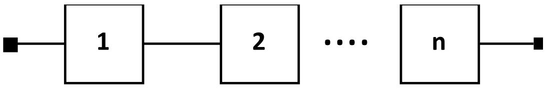
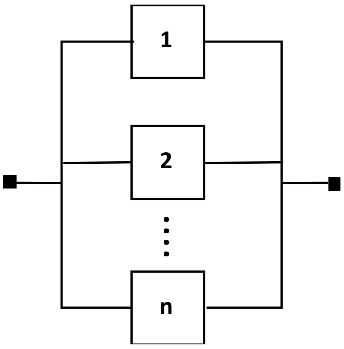


Figure 2. Example parallel structure

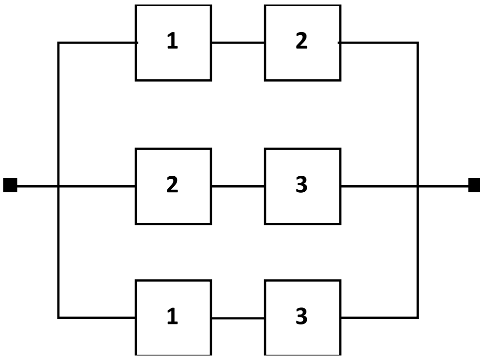


The above can be extended to a more general m-out-of-n (MooN) structure:

- A system that is functioning if and only if at least m of n components is functioning is called m-out-of-n structure. Figure 3 gives an example of MooN structure (M=2, N=3).

Series structure and parallel structure are two special cases of MooN structure, i.e. a series structure is NooN, and a parallel structure is 1ooN.

Figure 3. Two-out-of-three (2oo3) structure



In functional safety, a typical SIF consists of three subsystems: sensor, logic solver and final element. Represented on an RBD, the three subsystems would be a series system, whereas the individual subsystems maybe a parallel structure or MooN structure.

Figure 4 shows an example SIF. The SIF has its sensor subsystem comprising three pressure transmitters (PTs) configured as 2oo3, its logic solver subsystem comprising a single logic solver (LS), and its final element subsystem comprising two shutdown valves (SDVs) configured as 1oo2. If a process demand occurs (pressure reaches 48 bar), at least two of the three pressure transmitters, the logic solver, and at least one of the two shutdown valves have to function to have a successful function of the SIF. Figure 5 presents the corresponding RBD for the example SIF.

Figure 4. Physical layout of the example SIF (2oo3 sensors, 1oo1 logic solver, 1oo2 final elements)

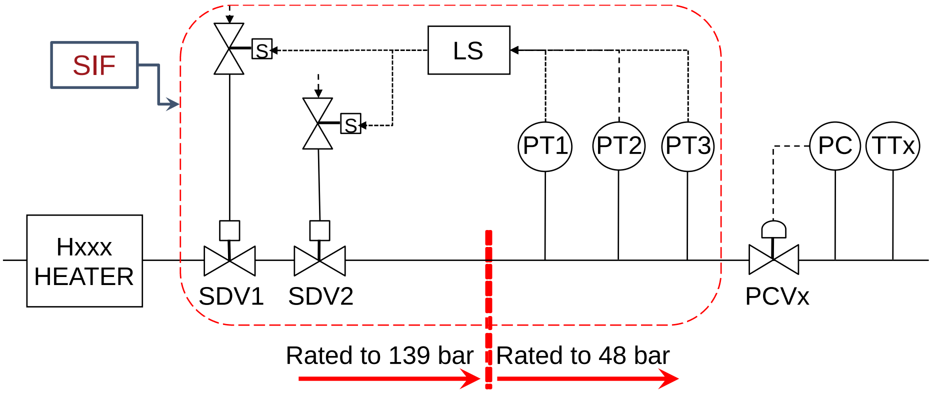
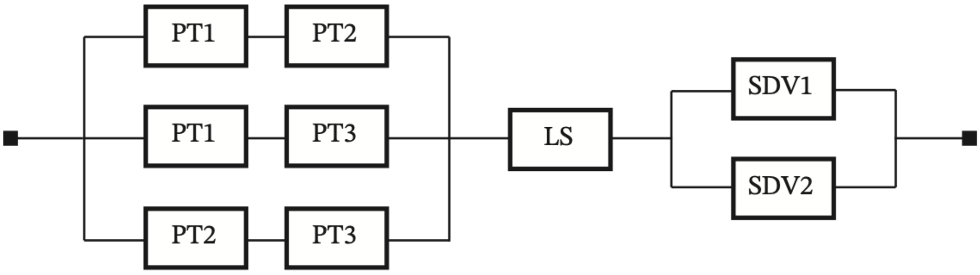


Figure 5. RBD of the example SIF (2oo3 sensors, 1oo1 logic solver, 1oo2 final elements)



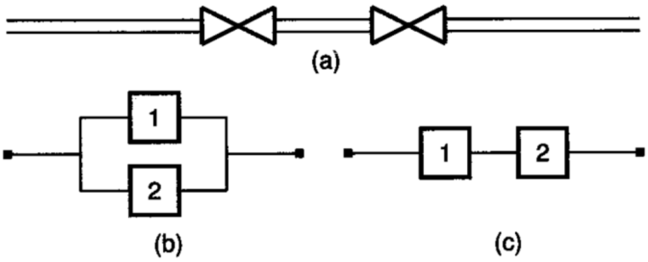
2.2. One RBD per function

An RBD is a success-oriented network describing a specific function of a system. It shows the logical connections of (functioning) components needed to fulfil a specified system function. If the system has more than one function, each function must be considered individually, and a separate reliability block diagram has to be established for each system function.

Consider a pipeline with two independent safety valves SDV1 and SDV2 that are physically installed in series, as illustrated in Figure 6 (a). In normal operation, both valves are held open. For this discussion, we are concerned about two functions:

- **Safety barrier function:** to close the valves and stop the flow in the pipeline in case of an emergency. Since it is sufficient that one of the valves closes in order to stop the flow, the valves will form a parallel system with respect to the safety barrier function, as shown in Figure 6 (b).
- **Avoiding spurious closure function:** to not close the valves spuriously when there is no demand / emergency. In order to avoid the flow being spuriously stopped, neither of the valves shall close spuriously. As a result, the two valves will form a series system with respect to the function of avoiding spurious closure, as shown in Figure 6 (c).

Figure 6. Two safety valves in a pipeline: (a) physical layout, (b) RBD for safety barrier function, (c) RBD for avoiding spurious closure



Notice the different meanings of the functional blocks in Figure 6 (b) and Figure 6 (c). in Figure 6 (b), connection through the block i means that valve i is able to stop the flow in the pipeline, while connection through i in Figure 6 (c) means that valve i does not close spuriously, for i=1, 2.

Based on the discussion using the simple example above, for any SIF, the safety barrier function and avoiding spurious trip function are two distinct functions, and two separate RBDs must be constructed. The RBD for the safety barrier function can be used to calculate PFD / PFH, and the RBD for avoiding spurious trip function can be used to calculate the Spurious Trip Rate (STR). The corresponding Hardware Fault Tolerance (HFT) would also be different in each case.

2.3. Deriving RBD for STR

Safety engineers / consultants would be familiar with the process of constructing the RBD for a SIF for the safety barrier function, as a basis for calculating PFD / PFH and examining HFT. For calculating STR for the same SIF, a separate RBD needs to be constructed, for the function of avoiding spurious trip. For ease of reference, the two RBDs will be referred to as $RBD_{PFD/PFH}$ and RBD_{STR}. The two RBDs for any given SIF are interrelated. We can easily derive one RBD from the other. The rules and explanations are given below.

1. **Series structure in $RBD_{PFD/PFH}$ (i.e. NooN) will be converted to parallel structure in RBD_{STR} (i.e. 1ooN).** If all N components are required to be functioning in order for the complete SIF to function, we would also need all N components to activate spuriously for the SIF to be spuriously activated. Therefore, if at least one of the N components does not activate spuriously, the SIF will not be spuriously activated. This forms an RBD with parallel structure for the purpose of calculating STR.

2. **Parallel structure in $RBD_{PFD/PFH}$ (i.e. 1ooN) will be converted to series structure in RBD_{STR} (i.e. NooN).** If only one of N components is required to be functioning in order for the complete SIF to function, we would also need only one component to activate spuriously for the SIF to be spuriously activated. Therefore, in order to avoid spurious activation of the SIF, none of the N components can activate spuriously. This forms an RBD with series structure for the purpose of calculating STR.

3. **MooN structure in $RBD_{PFD/PFH}$ will be converted to (N-M+1)ooN structure in RBD_{STR}.** If a minimum of M out of N components are required to be functioning in order for the complete SIF to function, we would also need a minimum of M out of N components to activate spuriously for the SIF to be spuriously activated. Therefore, in order to avoid spurious activation of the SIF, a minimum of N-M+1 components must not activate spuriously (i.e. the maximum number of components that can activate spuriously is M-1, not enough to make the complete SIF to activate spuriously). For example, if a SIF has a sensor configuration 2oo5 for the safety barrier function, i.e. the SIF will activate if a minimum of 2 sensors confirm a process demand is present; similarly, the SIF would activate spuriously, if a minimum of 2 sensors give spurious readings suggesting a process demand is present when in fact this is not the case. For the example SIF not to activate spuriously, we would need at least 4 sensors (=5-2+1) not give spurious readings (falsely suggesting a process demand is present).

Note rules 1 and 2 are special cases of the more general rule 3. MooN in $RBD_{PFD/PFH}$ always converts to (N-M+1)ooN in RBD_{STR}. When M=N, rule 3 becomes rule 1, and when M=1, rule 3 becomes rule 2.

3. PFD / PFH formulae

There are a number of sources that are provide PFD and PFH formulae including:

1. **IEC 61508:2010** (IEC, 2016). Part 6 of the standard (IEC 61508-6) provides PFD formulae for some common configurations including 1oo1, 1oo2, 2oo2, 1oo3, 2oo3. No generic formulae for MooN configuration are provided.

2. **PDS Method Handbook** on Reliability Prediction Method for Safety Instrumented Systems, 2013 (SINTEF, 2013). This book presents simplified PFD and PFH formulae without details of their derivation.

3. **Reliability, Maintainability and Risk: Practical Methods for Engineers** (Smith, 2017). This book provides derivation of PFD and PFH formulae, and generic formulae for MooN configuration.

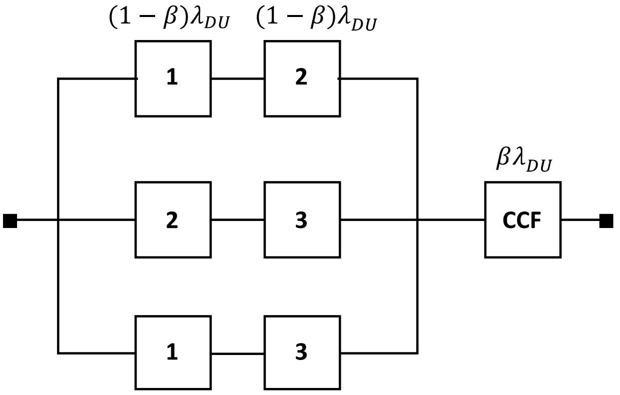
4. **Reliability of Safety-Critical Systems: Theory and Applications** (Rausand, 2014).

Readers are referred to the above sources for details regarding the derivation of relevant PFD / PFH formulae.

In functional safety, for the purpose of calculating PFD and PFH, dangerous failures of a component are divided into two categories with different downtime associated with each category: dangerous detected (revealed, failure rate denoted as λ_{DD}) and dangerous undetected (unrevealed, failure rate denoted as λ_{DU}). For dangerous detected failures, the downtime is dominated by Mean Time To Restoration (MTTR), for dangerous undetected failures, the downtime is determined by the Proof Test Interval (denoted as T).

For redundant configuration MooN (M<N), Common Cause Failure (CCF) must be taking into account when calculating PFD and PFH. A beta-factor model is commonly used where a proportion of the overall component failures are taken as CCF (denoted as β) which affect all redundant components at the same time.

Figure 7. RBD for 2oo3 with CCF modelled using the beta-factor model for dangerous undetected failures



According to reference at item 3 above, for repairable systems, the MooN system unavailability (i.e. PFD) and system failure rate (i.e. PFH) with respect to revealed (dangerous detected failures) and unrevealed failures (i.e. dangerous undetected failures) are:

$$\begin{aligned} PFD_{revealed,MooN} &= \binom{N}{N-M+1}((1-\beta)\lambda_{DD})^{N-M+1}MDT^{N-M+1} + \beta\lambda_{DD}MDT \\ &= \frac{N!}{(M-1)!\,(N-M+1)!}((1-\beta)\lambda_{DD})^{N-M+1}MDT^{N-M+1} + \beta\lambda_{DD}MDT \end{aligned} \tag{1}$$

$$\begin{aligned} PFH_{revealed,MooN} &= (N-M+1)\binom{N}{N-M+1}((1-\beta)\lambda_{DD})^{N-M+1}MDT^{N-M} + \beta\lambda_{DD} \\ &= \frac{N!}{(M-1)!\,(N-M)!}((1-\beta)\lambda_{DD})^{N-M+1}MDT^{N-M} + \beta\lambda_{DD} \end{aligned} \tag{2}$$

$$\begin{aligned} PFD_{unrevealed,MooN} &= \frac{1}{N-M+2}\binom{N}{N-M+1}((1-\beta)\lambda_{DU})^{N-M+1}T^{N-M+1} + \frac{\beta\lambda_{DU}T}{2} \\ &= \frac{N!}{(M-1)!\,(N-M+2)!}((1-\beta)\lambda_{DU})^{N-M+1}T^{N-M+1} + \frac{\beta\lambda_{DU}T}{2} \end{aligned} \tag{3}$$

$$\begin{aligned} PFH_{unrevealed,MooN} &= \binom{N}{N-M+1}((1-\beta)\lambda_{DU})^{N-M+1}T^{N-M} + \beta\lambda_{DU} \\ &= \frac{N!}{(M-1)!\,(N-M+1)!}((1-\beta)\lambda_{DU})^{N-M+1}T^{N-M} + \beta\lambda_{DU} \end{aligned} \tag{4}$$

where:

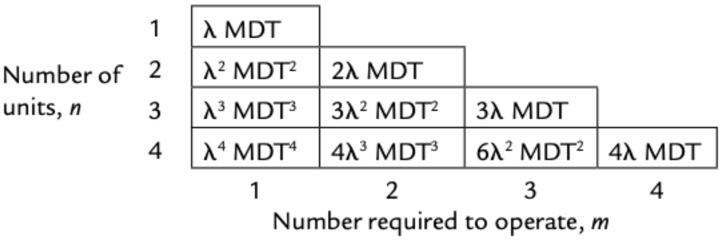
- $\binom{N}{M} = \frac{N!}{M!(N-M)!}$ Note: $\binom{N}{0} = \binom{N}{N} = 1;\ \ 0! = 1$
- λ_{DD} – Dangerous Detected failure rate of a single channel. It is assumed that all N channels are identical.
- λ_{DU} – Dangerous Undetected failure rate of a single channel. It is assumed that all N channels are identical.
- MDT – Mean down time. For dangerous detected failures, the mean down time is MTTR.
- T – Proof test interval.
- β – Beta factor for calculating CCF.

Note:

- The second part of the equations (1) – (4) are CCF contribution to the PFD / PFH. The CCF term only exists if M<N (i.e. there is some redundancy). If M=N, the CCF term becomes 0 (i.e. $\beta = 0$).
- From the reliability theory, $Unavailability = 1 - e^{-\lambda t}$. The equation can be simplified to $Unavailability = \lambda t$ only if $\lambda t \ll 1$. This assumption applies to the simplified equations (1) – (4) above. Full exponential equation should be used if the assumption $\lambda t \ll 1$ does not hold, see Chapter 5 of The Safety Critical Systems Handbook (Smith and Simpson, 2016).

Based on the general equations (1) to (4) for the MooN configuration, the PFD and PFH for many common configurations (without the CCF part) can be derived as shown in Figure 8 to Figure 11 below (Smith, 2017):

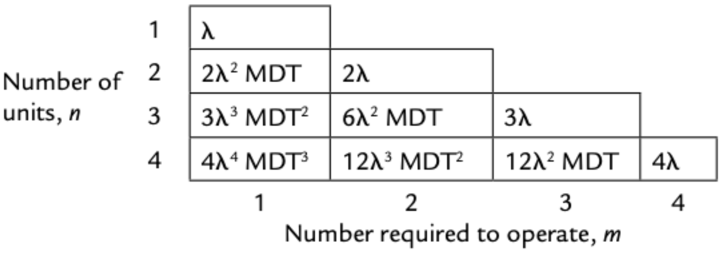
Figure 8. System unavailabilities (revealed) – PFD (revealed)



Number of units, n	1	2	3	4
1	λ MDT			
2	λ^2 MDT^2	2λ MDT		
3	λ^3 MDT^3	$3\lambda^2$ MDT^2	3λ MDT	
4	λ^4 MDT^4	$4\lambda^3$ MDT^3	$6\lambda^2$ MDT^2	4λ MDT

Number required to operate, m

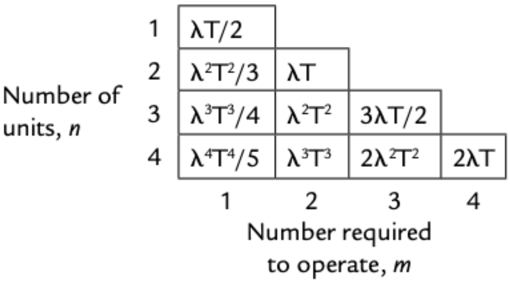
Figure 9. System failure rates (revealed) – PFH (revealed)



Number of units, n	1	2	3	4
1	λ			
2	$2\lambda^2$ MDT	2λ		
3	$3\lambda^3$ MDT^2	$6\lambda^2$ MDT	3λ	
4	$4\lambda^4$ MDT^3	$12\lambda^3$ MDT^2	$12\lambda^2$ MDT	4λ

Number required to operate, m

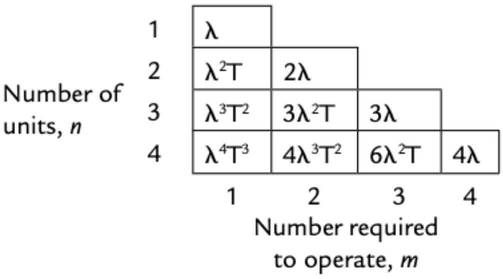
Figure 10. System unavailabilities (unrevealed) – PFD (unrevealed)



Number of units, n	1	2	3	4
1	$\lambda T/2$			
2	$\lambda^2T^2/3$	λT		
3	$\lambda^3T^3/4$	λ^2T^2	$3\lambda T/2$	
4	$\lambda^4T^4/5$	λ^3T^3	$2\lambda^2T^2$	$2\lambda T$

Number required to operate, m

Figure 11. System failure rates (unrevealed) – PFH (unrevealed)



Number of units, n	1	2	3	4
1	λ			
2	λ^2T	2λ		
3	λ^3T^2	$3\lambda^2T$	3λ	
4	λ^4T^3	$4\lambda^3T^2$	$6\lambda^2T$	4λ

Number required to operate, m

4. STR formulae derivation

We now have all the tools available in order to derive STR formulae, not from the first principles of reliability engineering, but from the RBD and the formulae already established for calculating PFD / PFH.

STR, is a failure rate calculated based on the RBD established for the function of avoiding spurious trip, which is similar to the PFH calculated based on the RBD established for the safety barrier function of the SIF. To calculate STR, the following is required:

- **RBD for STR.** From the RBD for the safety barrier function, establish a separate RBD for the function of avoiding spurious trip, following the rules described in Section 2.3. That is, change the original MooN configuration to (N-M+1)ooN configuration, add or remove CCF component based on HFT of the resulting configuration**.**
- **Spurious trip failure rate (λ_{STR}).** By definition, safe failures could lead to spurious trip. Sometimes SIFs are designed so that dangerous detected failures also activate the SIF and put the system in a safe state. Therefore, depending on how the SIF is configured, λ_{STR} could be
  - λ_S – if only safe failure trips the system
  - $(\lambda_S + \lambda_{DD})$ – if dangerous detected failure also trips the system

  Note safe failures could be further categorised into safe detected (λ_{SD}) and safe undetected (λ_{SU}) failures, and separate formulae derived for revealed and unrevealed failures as with the PFD / PFH formulae presented in Section

3. However, it is believed that most failures contributing to a spurious trip are revealed, either by diagnostics, routine inspections, or the occurrence of a spurious trip (when there is no redundancy with respect to avoiding spurious trip). Furthermore, most industry failure rate databases only provide λ_S for a device rather than a more granular λ_{SD} and λ_{SU}. As a result, λ_{STR} will be treated as revealed.

The STR formulae can now be derived from the PFH formulae at equation (2) with the following changes:

- Replace M with N-M+1, due to the change of RBD configuration for the two different functions
- Replace λ_{DD} with λ_{STR}

$$\begin{aligned} STR_{MooN} &= M\binom{N}{M}((1-\beta)\lambda_{STR})^M MDT^{M-1} + \beta\lambda_{STR} \\ &= \frac{N!}{(M-1)!\,(N-M)!}((1-\beta)\lambda_{STR})^M MDT^{M-1} + \beta\lambda_{STR} \end{aligned} \tag{5}$$

where:

- λ_{STR} – spurious trip failure rate for individual channel. Depending on the configuration of specific systems, this could be λ_S or $(\lambda_S + \lambda_{DD})$.
- MDT – Mean down time. Since STR is revealed, the mean down time is MTTR.
- β – Beta factor for calculating CCF. Note this may be different from the beta factor used for calculating PFD / PFH.
- STR_{MooN} – STR for (N-M+1)ooN configuration (the corresponding safety barrier function RBD would be MooN configuration). Note MooN is used as subscript to be the same as the RBD configuration used for PFD / PFH to avoid confusing safety engineers / consultants (they usually have one configuration in mind for a SIF).

Note:

- The CCF term (second part of the equation) only exists if (N-M+1)<N. If M=1, the CCF term becomes 0 (i.e. $\beta = 0$).
- It is assumed that $\lambda_{STR}MDT \ll 1$ in the simplified equation (5). This assumption should be valid in vast majority of cases as MDT for revealed failures are often small (<100 hours), and λ_{STR} would be in unit of fpmh (failures per million hours).

For detailed discussion regarding the generic STR formula derivation, refer to Chapter 12 of Marvin Rausand’s book on Reliability of Safety-Critical Systems (Rausand, 2014).

5. Specific STR formulae for common configurations

This section presents the specific formulae for calculating STR of some typical MooN configurations, based on equation (5) above.

The formulae below are in line with the ones presented in Reliability of Safety-Critical Systems (Rausand, 2014) and ISA-TR84.00.02-2002 Part 2 (ISA, 2002), and the formulae used by Saudi Aramco (SAEP-250, 2018) are taken from the ISA-TR84.00.02. Note some of the formulae are incorrect, e.g. the formula for 2oo4 in ISA-TR84.00.02 fails to recognize that 2oo4 corresponds to 3oo4 configuration for calculating STR.

Since the probability of multiple independent channel failures in a short interval is usually so small that it can be neglected. The MooN STR formula can be simplified for $2 \le M \le N$ as equation (6) below. This is the STR formula presented in the PDS Method Handbook (SINTEF, 2013).

$$\boldsymbol{\lambda_{STR,MooN}} = \beta\lambda_{STR} \tag{6}$$

The generic formulae assume all redundant channels are identical. The formulae can be extended to deal with dissimilar redundant channels and each with a different failure rate, e.g. $\lambda_{STR,1}$, $\lambda_{STR,2}$. Table 1 below presents STR formulae for common SIF configurations, both identical and dissimilar channels.

Table 1. STR formulae for common SIF configurations

SIF config.	STR Formulae (identical channels)	STR Formulae (dissimilar channels)
1oo1	λ_{STR}	λ_{STR}
1oo2	$2\lambda_{STR}$	$\lambda_{STR,1} + \lambda_{STR,2}$
2oo2	$2(1-\beta)^2\lambda_{STR}^2 MDT + \beta\lambda_{STR}$	$2(1-\beta)^2\lambda_{STR,1}\lambda_{STR,2}MDT + \beta\lambda_{STR}$
1oo3	$3\lambda_{STR}$	$\lambda_{STR,1} + \lambda_{STR,2} + \lambda_{STR,3}$

SIF config.	STR Formulae (identical channels)	STR Formulae (dissimilar channels)
2oo3	$6(1-\beta)^2\lambda_{STR}^2 MDT+\beta\lambda_{STR}$	$2(1-\beta)^2(\lambda_{STR,1}\lambda_{STR,2}+\lambda_{STR,1}\lambda_{STR,3}+\lambda_{STR,2}\lambda_{STR,3})MDT+\beta\lambda_{STR}$
3oo3	$3(1-\beta)^3\lambda_{STR}^3 MDT^2+\beta\lambda_{STR}$	$3(1-\beta)^3\lambda_{STR,1}\lambda_{STR,2}\lambda_{STR,3}MDT^2+\beta\lambda_{STR}$
1oo4	$4\lambda_{STR}$	$\lambda_{STR,1}+\lambda_{STR,2}+\lambda_{STR,3}+\lambda_{STR,4}$
2oo4	$12(1-\beta)^2\lambda_{STR}^2 MDT+\beta\lambda_{STR}$	$2(1-\beta)^2(\lambda_{STR,1}\lambda_{STR,2}+\lambda_{STR,1}\lambda_{STR,3}+\lambda_{STR,1}\lambda_{STR,4}+\lambda_{STR,2}\lambda_{STR,3}+\lambda_{STR,2}\lambda_{STR,4}+\lambda_{STR,3}\lambda_{STR,4})MDT+\beta\lambda_{STR}$
3oo4	$12(1-\beta)^3\lambda_{STR}^3 MDT^2+\beta\lambda_{STR}$	$3(1-\beta)^3(\lambda_{STR,1}\lambda_{STR,2}\lambda_{STR,3}+\lambda_{STR,1}\lambda_{STR,2}\lambda_{STR,4}+\lambda_{STR,1}\lambda_{STR,3}\lambda_{STR,4}+\lambda_{STR,2}\lambda_{STR,3}\lambda_{STR,4})MDT^2+\beta\lambda_{STR}$
4oo4	$4(1-\beta)^4\lambda_{STR}^4 MDT^3+\beta\lambda_{STR}$	$4(1-\beta)^4\lambda_{STR,1}\lambda_{STR,2}\lambda_{STR,3}\lambda_{STR,4}MDT^3+\beta\lambda_{STR}$

Note:

- The SIF config. column in Table 1 refers to the RBD configuration with respect to safety barrier function.
- The formulae treat λ_{STR} as revealed for the reasons presented in Section 4.

6. Conclusion

STR is an important factor that must be taken into account in designing a SIF, as required by IEC 61511. Unfortunately this topic is often ignored or overlooked by safety engineers and consultants. The issue has been exacerbated by the limited resources available on this topic. This paper presents a simplified approach to the derivation of STR for a SIF from the existing knowledge of RBD and PFD / PFH formulae, and illustrates the close relationship between the STR and PFH formulae.

7. References

IEC, 2010, IEC 61508:2010, Functional safety of electrical / electronic / programmable electronic safety-related systems.

IEC, 2016, IEC 61078:2016, Reliability block diagrams.

IEC, 2017, IEC 61511:2017 + A1:2017, Functional safety – Safety Instrumented systems for the process industry sector.

ISA, 2002, ISA-TR84.00.02-2002 Part 2 – Safety Instrumented Functions (SIF)-Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations.

Rausand, M., 2014, Reliability of Safety-Critical Systems: Theory and Applications.

SAEP-250, 2018, Safety Integrity Level Assignment and Verification, Saudi Aramco Engineering Procedure.

SINTEF, 2013, PDS Method Handbook: Reliability Prediction Method for Safety Instrumented Systems.

Smith, D., 2017, Reliability, Maintainability and Risk: Practical Methods for Engineers, 9th edition.

Smith, D., Simpson, K., 2016, The Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2016 Edition) & Related Guidance, 4th edition.