Session Eleven:

Optimizing component arrangement in complex SIS – a case study

Hamid Jahanian
Senior Engineer, Siemens Ltd.

Abstract

The arrangement of components plays a key role in the performance of complex Safety Instrumented Systems (SIS) in which a SIS logic solver is interlocked with other logic solvers, to share a final element, for instance. The position of components and the way they are utilized affects the reliability characteristics, such as the Probability of Failure on Demand (PFD), Spurious Trip Rate (STR), architectural sensitivity and model uncertainty. A real-life example is presented in this article to highlight the impact of component arrangement. The case study uses quantitative and qualitative analysis to review two SIS architecture solutions in a renovation project where the existing turbine protection system is upgraded to incorporate a new over-speed protection system. Also, a classification for SIS components based on their response to demand is introduced, and a set of guidelines for SIS architecture engineering is developed.

1. Introduction

The key question of optimal Safety Instrumented System (SIS) architecture, which this case study tries to address, was initially raised in a turbine upgrade project where an existing mechanical over-speed protection system was to be replaced with a new microprocessor-based system. The new over-speed protection system was to be interfaced with the main turbine protection system, a PLC-based SIS which performed all the other Safety Instrumented Functions (SIFs) of the turbine. Inherently, the two safety systems would utilize their own sensors, wired to their separate CPUs; however, as the two systems were aimed at protecting the same turbine, they would need to share the final elements, i.e. turbine valves.

A preliminary study was carried out to narrow down the design options to two configurations, out of which, choosing the final optimum solution would still require further analysis. Detail study was then performed in two stages: by using 25 simplified models, to challenge the issue in basic level and to outline general principles and guidelines, and then by studying the two actual options proposed for the upgrade project, taking into account what was learnt in the first stage.

This article shares a summary of the study [6] with a focus on optimization of the SIS arrangement in the turbine upgrade project. Section 2 of this article consists of a new classification for SIS component, based on demand-and-response principle. Not only the definitions given in Section 2 are referred to in the rest of the article, but, more importantly, they are aimed at providing a *functional* perspective, on which this article tries to emphasise. Section 3 details the turbine upgrade project, and demonstrates the role of component arrangement by using simplified forms of the two configurations proposed in the upgrade project. It should be noted that the

configurations reviewed in this section are not meant to represent a specific plant or project. The original design of the turbine upgrade project has been simplified and adjusted to serve the purpose of this article with focus on the issue of component arrangement. Finally, Section 4 presents a set of design guidelines which were observed and utilized throughout the turbine upgrade project. The guidelines can be considered as general hints in other similar engineering challenges.

2. Safety components classification

PFD (Probability of Failure on Demand) is a quantitative measure for estimating the probability of failure of a SIF in *response* to a *demand*. The demand arises when a hazardous situation takes place in the process, and the response is the safety action that the SIF should take in order to isolate the process from the hazard. Failure of a SIF, and therefore the probability of the failure, can only be considered in association with a specific demand and a specific response.

A SIF consists of different subsystems (i.e. sensors, logic solver and final elements). The collective failure, or success, of a SIF in responding to its demand depends on the failure, or success, of its individual subsystems in responding to their own demands. The demand and response associated with each subsystem is different. The demand that a sensor should respond to is detecting the hazard at the right time and indicating it to the logic solver. This is different to the type of demand and response of logic solver or final element. The demand on the logic solver is to correctly process the safety logic and initiate a trip signal when the process seems to be at risk, and the final element should respond to its own demand by physically isolating the process from the hazard.

The demand-and-response perspective can be extended further to the constituting components of subsystems. Each component can be studied as a responsive function that may fail, or succeed, to respond to a specific demand. From this perspective, components can be classified into the following categories:

- ***Active***: components that constantly convert information from one form to another. Analog sensors, which read process variables and generate analog signals, and CPUs, which constantly process safety logic, are included in this category. The role of *active* elements in SIFs is not to react to particular events, but rather to correctly and constantly transform information from their inputs to their outputs. Faults in *active* components are less likely to remain undetected for a long time, because *active* components experience more transitions, resulting in faults surfacing in one form or another when they occur.
- ***Reactive***: components that respond to specific binary events by moving from a permanent normal state to a temporary trip state. Binary sensors, DO modules and interposing relays fit into this category. The main dilemma with *reactive* components is dangerous undetected failures, as these components are inherently designed to remain in one state for long periods of time. A welded contact of a relay that has been in an energized state for long time may only surface when there is a demand to de-energize it.
- ***Passive***: components of the *reactive* type, when used in an inactive arrangement different to what the components are originally designed for. Examples include: an interposing relay when its coil is not part of a SIF but its contact is, because the contact is utilized to transfer the trip signal; and a DO module that is not utilized to receive trip signals from a CPU, but it gets

depowered when a trip signal is initiated. Uncertainties and unknowns are the main issues in *passive* components. This is because the failure information that is available for a *passive* component is only good enough to cover the normal utilization (i.e. when used in *reactive* mode) and not altered setups.

- ***Link***: components such as terminals, wires and cables, which connect other components to each other but do not play a responsive role in SIFs.
- ***Supply***: components that supply other SIF elements with energy so that they remain functional. *Supplies* do not perform direct roles in SIF response loops. Power supplies, for instance, play a critical role in SIFs with energize-to-trip configurations. Undetected loss of power in such systems results in total dangerous undetected failure of the SIF. However, even in energize-to-trip systems, power supply is only the provider of energy and does not directly respond to a trip signal when a trip is initiated.

The above classification is used in the following sections of this article. It is important to differentiate between the components based on their function in SIF's overall response to a demand, rather than the function of individual components in isolation. This view affects the suitability of failure data in reliability analysis. It is not sufficient to extract the failure data of components from valid sources of information. It should also be ascertained if the given failure data correctly represent the failure modes associated with the application of the components.

3. The turbine upgrade project

This section explains the turbine upgrade project, where the existing mechanical over-speed protection mechanism is to be replaced by a new electronic system. The following assumptions are used in this analysis:

- Output module is of digital type (i.e. the output signal can be either 0 or an active voltage, L+).
- Final element is de-energize to close, and the process is safe when the final element is closed.
- Safety requirements, such as Hardware Fault Tolerance (HFT) and Common Cause Failure (CCF) [2], and Systematic Capability [4] are not addressed in the analysis.
- For simplicity, formulas given in [1] and [5] are used for calculating PFD and STR values respectively. Although, comprehensive formulas of the IEC61508 (Refer to [6] and [7]) were utilised for calculating PFD_{avg} in the actual project.

3.1. The scenario

All turbine SIFs, except over-speed protection, are implemented in an existing PLC-based SIS. The existing over-speed protection is a mechanical system which is to be upgraded and replaced by a new electronic system, called Over Speed Protection System (OSPS). The OSPS is a programmable 2oo3 system with its own input and output boards and its own CPUs. The OSPS reads three speed signals directly from speed sensors, monitors them, and de-energizes its trip output lines if two out of three speed signals are over the limit and/or faulty. The OSPS can also read up to six additional groups of signals, each a 2oo3 voting combination, and initiate a trip at its output lines if any of the voting groups indicates a trip state. The voting groups can be assigned to process signals, trip push buttons and other trip causes that are not necessarily related to speed.

In addition to the over-speed safety function, the OSPS generates three pulse signals which correspond to the three signals read from speed sensors. The pulse signals are used by the Turbine Governor System (TGS) to control the turbine speed. The turbine is coupled to a generator that delivers power to a universal grid. The connection between the generator and the grid is established through a circuit breaker. Generator load rejection takes place if the connection between the generator and the grid is suddenly lost (due to the circuit breaker fault, for instance). In the event of a load rejection, the TGS will try to maintain the turbine at full speed no-load state, to avoid a complete turbine shutdown and the time-consuming process of a restart.

The safety target of the overall turbine protection system is to depressurize the turbine hydraulic system to close both the Emergency Stop Valve (ESV) and Main Control Valve (MCV), and isolate the process from hazard. This is achieved by de-energizing six solenoid valves in two separate 2oo3 blocks, which drain the hydraulic oil and set the ESV and the MCV to close. Unlike the ESV trip block, which is only used to shut the ESV closed when a trip happens, the MCV trip block operates with both the turbine protection system and the TGS. If a trip is initiated, the safety system de-energizes both the ESV and MCV trip blocks, causing the valves to close and remain closed until the next turbine start-up. However, if a load rejection takes place while the turbine is running, the TGS will try to maintain the turbine at full speed. The TGS does this by rapidly closing the MCV before the steam flow drives the turbine to over-speed and then opening the MCV again to resume turbine speed control.

A key question in the turbine upgrade project, which we will try to address in the following sections, is the optimum arrangement of components in combining two SIS and one BPCS logic solvers. We will review two proposed solutions from the component arrangement perspective, to highlight the impact of component arrangement on the performance of the overall turbine protection system. It should be noted that the objective of this review is not to identify either solution as right or wrong, but only to show how component arrangement can impact SIS architecture.

3.2. The solutions

Figures 1 and 2 show two options for interlocking between the SIS, OSPS and TGS. The existing SIS and new OSPS comprise the turbine safety system, and the TGS performs as BPCS. As Figure 1 shows, in option A, the OSPS drives three safety relays (TR01-03) that supply the SIS digital output modules with power, and the DO modules drive the solenoid valves of the ESV and MCV trip blocks. Interfacing between the TGS and the safety system is done through three load rejection relays (LRR01-03) that are driven by the TGS. When a process hazard is detected at the SIS inputs a trip will be initiated by the SIS, and the DO modules will directly de-energize the trip blocks. If an over-speed is detected by the OSPS, the output contacts of the OSPS will open to de-energize the safety relays (TR01-03), cut the power to the DO modules and de-energize the trip-block solenoid valves.

Option B (Figure 2) uses a different configuration: SIS DO modules supply the safety relays (TR01-03) through the output contacts of the OSPS, and the relays drive the trip-block solenoid valves. Interface between the TGS and the safety system is done through the same relays (i.e. TR01-03), and the load rejection relays (LRR01-03) are mainly used for compatibility between the TGS outputs and the MCV solenoids. If a trip is initiated by the SIS, the output contacts of OSPS will be depowered by the DO modules DO01-03; and if an over-speed is detected by the OSPS, the output

contacts will drop open directly by the OSPS. In either case, the safety relays will be de-energized to cut the supply power to the ESV and MCV solenoid valves.

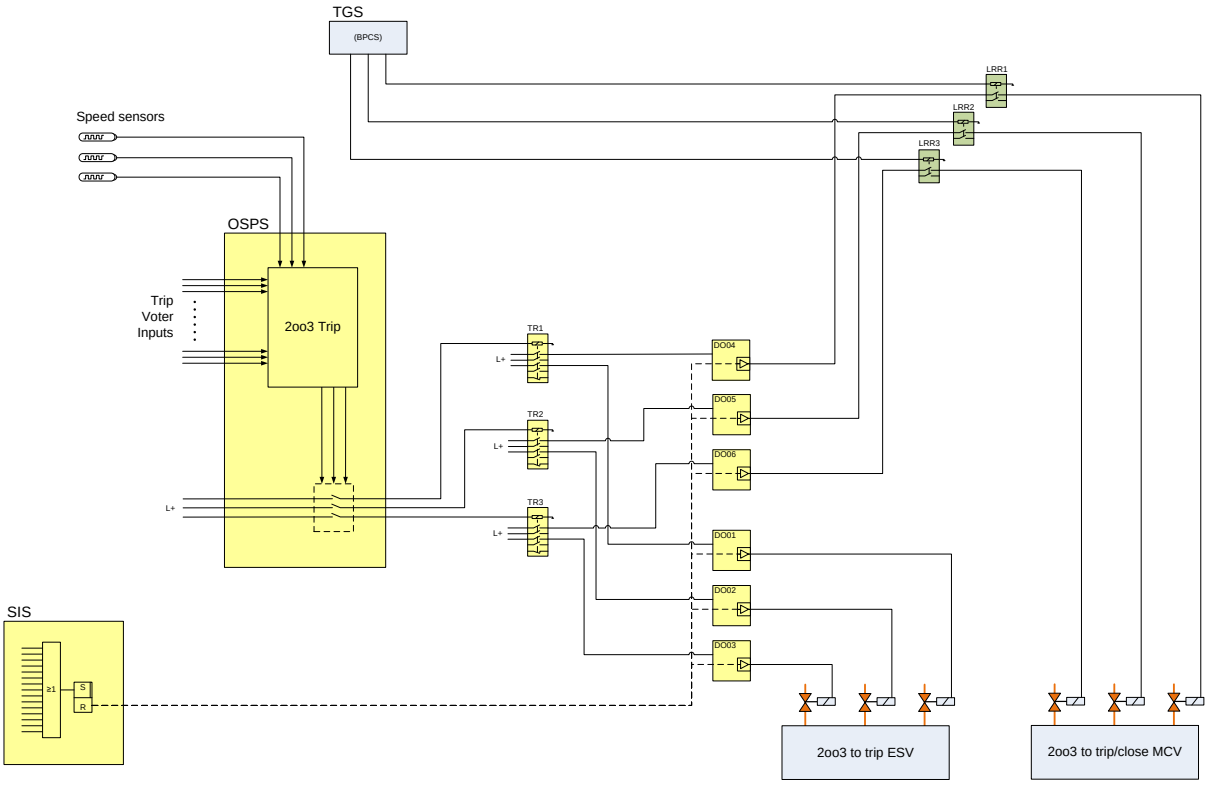

Figure 1: SIS configuration in the turbine upgrade project, option A

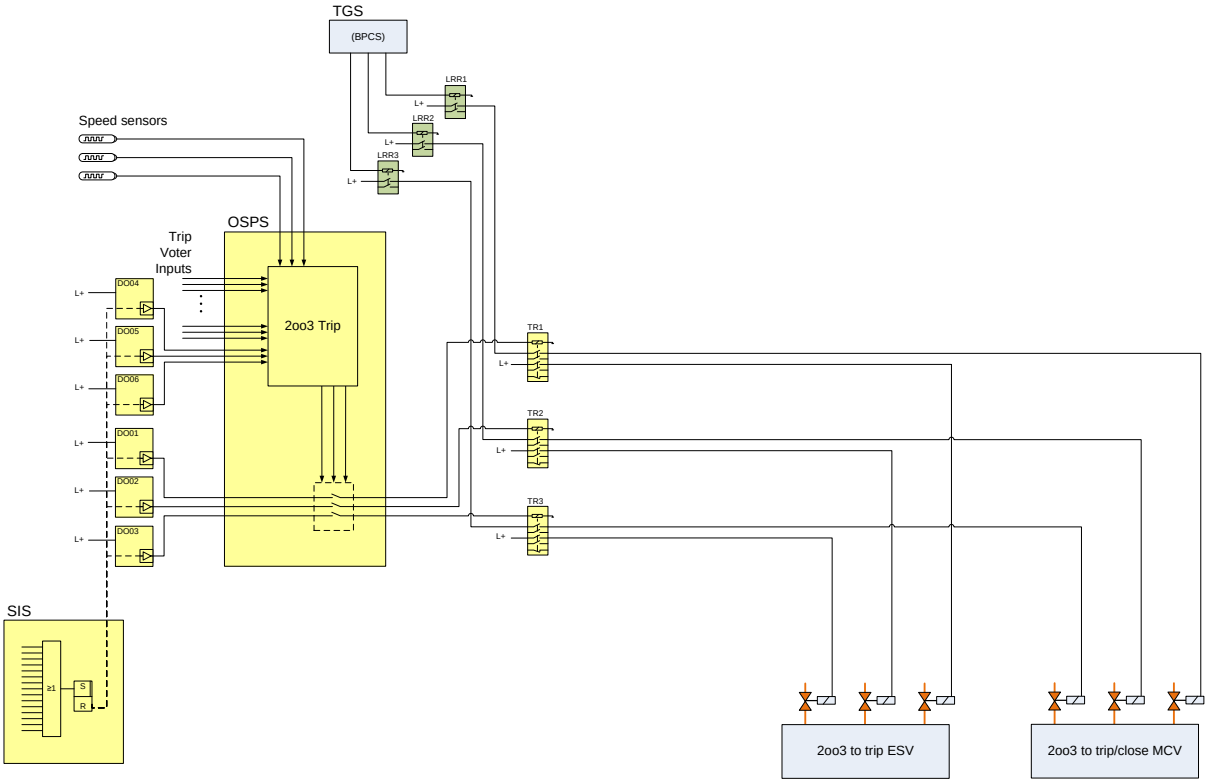

Figure 2: SIS configuration in the turbine upgrade project, option B

The existing SIS performs more than fifteen process-related safety functions (SIFs), and the new OSPS processes five, including the 2oo3 over-speed protection. For simplicity, let us just focus on the over-speed protection function in the OSPS, namely SIF#1, and one of the process-related SIFs in the existing SIS, to be referred to as SIF#2. The constituting elements of SIF#1 and SIF#2 in the two options are listed in Table 2 below. Note that SIF#1 and SIF#2 only refer to the logic solver part of the safety system, and do not include the sensors and final elements. Field instruments are not part of this analysis as they are completely identical between options A and B.

SIF	Elements in option A	Elements in option B
SIF#1	OSPS, TRs, DOs, IRs, MCVs, ESVs	OSPS, TRs, MCVs, ESVs
SIF#2	SIS CPU, DOs, IRs, MCVs, ESVs	SIS CPU, DOs, TRs, MCVs, ESVs

Table 2: Constituting elements of SIF#1 and SIF#2 in options A and B

Both options A and B use the same number and types of components, which makes it easier to focus on comparing the two options from the component arrangement point of view. Table 3 below summarizes the specifications of the individual components used in the two options. The failure rates given in Table 3 will be later used in PFD calculations for options A and B.

Element	SIL Rating	λ_{DU}	Description
OSPS	3	1.50E-08	2oo3 O/S protection system, force-guided output contacts, limited variability language (LVL)
SIS CPU	3	5.30E-09	1oo1D CPU, fixed program language (FPL)
SIS DO	3	1.00E-09	Digital output module with 0/24VDC output voltage
TR01, 02, 03	3	4.00E-10	Safety relay (electro-mechanical)
LRR01, 02, 03	N/A	6.00E-07	Interposing relay (solid-state)

Table 3: Components used in options A and B

3.3. The key differences

One of the key architectural differences between options A and B is the location and utilization of the DO modules. In option B, the safety relays are driven by the DO modules, whereas in option A, the DO modules are powered through the safety relays, and will be depowered if a trip is initiated. When using the depowering of an electronic module as a means for tripping, one should ensure that the loss of power does result in the quick depowering of output signals. This can be a reasonable assumption in option A, given that the DO modules are reliable, SIL3-certified components. However, generally speaking, one should address all unknowns and uncertainties when using such components in *passive* mode. As a minimum, one should ensure that, when disconnecting the power supply to the DO modules, all possible sources of energy to the modules will be disconnected, as some types of DO modules use multiple power inputs to segregate between communication circuit and output signals.

Another downside of depowering DO modules for tripping is the loss of communication between DO modules and the CPU for the period of time when the

modules are off. All potential fault events will be masked for that period of time, and diagnostics information, which would otherwise be known to the CPU, will remain undetected and unused.

Option B resolves all these issues simply by changing the arrangement of the SIS components. Unlike option A, the DO modules in option B are set up in *reactive* mode, and are constantly powered, regardless of the state of the trip signal. This resolves the uncertainties associated with the depowering in option A, and it also enhances the diagnostics, as the modules are always on and the diagnostics information always available.

Another key architectural difference between options A and B is the location of the interposing relays. In option A, the relays are used as frontline elements, i.e. the last SIF elements before the final elements (MCV and ESV trip blocks). In option B, the interposing relays are moved to the back of the SIL-certified safety relays, leaving these relays as the frontline elements. As explained before, the main purpose of the interposing relays is to interface between the TGS and MCV block during load rejection. The TGS de-energizes the relays, and the open contacts of the relays de-energize the MCV solenoid valves.

With the contacts of the interposing relays in series with the DO signals, option A requires the diagnostics of the DO channels to be deactivated. With active diagnostics, the disconnected DO link will be identified as a fault and the DO channel will be set to passive state, requiring acknowledgement by operator or SIS logic. The acknowledgement may not be fast enough to restore the DO channel before the TGS re-energizes the interposing relays to open the MCV, keeping turbine speed under control. This issue is resolved in option B simply by moving the interposing relays out of the connection path between the DO modules and the MCV solenoid valves. In this option, the output circuit of the DO modules get disconnected only when a trip takes place, which is when the turbine valves are required to close and remain closed.

As for the diagnostics coverage of the DOs, option A covers the connections up to the three ESV solenoid valves, which are installed close to the turbine and far from the installation location of the SIS. The diagnostics of the DO modules connected to the MCV is completely deactivated in option A. Option B, on the other hand, provides full coverage for its six DO channels, all of which are installed closer to the SIS, rather than the turbine. Option A covers a longer distance for fewer elements (three solenoids), whereas option B covers shorter distances for more components: three trip relays, three OSPS contacts and three OSPS voting group inputs.

Another issue that should be noted is the unknowns and uncertainties associated with using Solid-State Relays (SSRs) in *passive* mode in option A. The problem is related to the potential faults of the internal electronics of SSRs, which may result in a sustained supply voltage at the output of the relay, preventing the trip command from tripping the final element. Using such an element at the forefront of the safety system can undermine all other highly reliable upstream components, such as the 2oo3, SIL3-certified OSPS. The dilemma here is not the fault itself, as every component may fail one day, but rather the lack of information and the difficulties in obtaining the required failure data. It is not always easy, or even possible, to get documented failure rates for non SIL-certified components, or if the failure rates in question are related to uncommon failure modes, such as internal breakage in an SSR. One may argue that more reliable, and perhaps SIL-certified, relays would be an alternative option here. However, one should not forget other engineering

restrictions, such as compatibility and cost, which may challenge using such components. Option B addresses this issue simply by relocating the interposing relays, to use them in *reactive* rather than *passive* mode. Not only does this simple adjustment in the component arrangement resolves the issue of potential internal faults of the SSR by avoiding the problem, and utilizing the relay in a better-known mode, but it also fixes the passivation problem and deactivation of diagnostics that were discussed earlier. As a result, a dangerous failure of the interposing relays will not lead to the dangerous failure of the whole safety system, unlike in option A. In the worst case scenario, if the interposing relays become faulty and the contacts keep supplying active voltage, the load rejection function may get affected but not the safety functions. Basically, option B turns the dangerous failure of the relays into an ineffective fault in relation to the safety system, without adding any failure modes to the TGS function.

Options A and B can also be compared from SIFs priority perspective. The target SIL for the over-speed function (SIF#1) is identified as 3 and for other existing safety functions (SIF#2) it is either 1 or 2. As Table 2 compares SIF#1 and SIF#2, option B is preferable from this perspective too, because in this option the SIF with higher SIL (SIF#1) consists of fewer components, which means less chance of failure and a shorter path to trip the final element. Even when comparing the number of elements for SIF#1 alone, fewer elements are involved in option B than in option A. In other words, compared to option A, SIF#1's trip signal in option B has to make it through fewer layers of failure and delay before reaching the final elements.

3.4. Quantitative comparison

The qualitative comparison between options A and B in the previous subsection showed that option B seems to be a better choice. Let us now have a look at the calculations to see whether the numbers confirm this judgment as well. Reliability Block Diagrams (RBDs) and PFD_{avg} are used in this section for a quantitative comparison between options A and B. Since the focus of this analysis is on differences between options A and B, the RBD models do not include the repeated elements, i.e. MCV, ESV, SIS CPU and OSPS.

Two safety targets can be defined for the purpose of this analysis: two out of three lines connected to the MCV block to be de-energized when a trip is initiated; and two out of three lines connected to the ESV block are to be de-energized when a trip is initiated. In other words, a dangerous failure of the MCV block occurs if more than one line connected to the MCV solenoids are not able to de-energize in response to a trip demand, and likewise, the ESV block is in a dangerous failure state if more than one line connected to the ESV solenoids are stuck in energized state and cannot de-energize if required. The RBDs shown in Figure 3 depict the following models that are used for calculating the PFD_{avg} of these two safety targets:

- **Option A, SIF#1, MCV Block (RBD#1)**: RBD#1 models the dangerous failure of the components in between the OSPS and the three lines connected to the MCV trip block. Both DO modules and interposing relays in this model are utilized in *passive* mode, and therefore their failure rates are not necessarily identical to the failure rates in Table 3.

  Given the high reliability of the SIL3-certified DO modules, let us assume that the failure rate associated with depowering of the modules is negligible, i.e. depowering the modules always results in immediate depowering of its output channels. Therefore, the failure rate for this failure mode is considered to be 0.0, although the DO blocks are still shown in the RBD diagram.

Utilising the load rejection relays (LRR01-03) in *passive* mode changes the dominating failure mode of these relays. What affects the SIS response in Option A is not the failure of the LRR01-03 in responding to trip commands, because the relays are not driven by the SIS. Instead, what might affect the SIS here is the possible internal breakage in SSRs, which can result in leaving constant potential at the output of the relays and thus isolating the MCV trip block from the upstream SIS components.

In the absence of failure data directly representing the failure mode we have to deal with here, let us assume that the chance of internal breakage in SSRs can be formulated as a factor of the mainstream failure rate. Let us define the correction factor *cf* as follows:

$$\lambda_{DU\ (passive)} = cf\ * \lambda_{DU}$$

In the above equation, $\lambda_{DU\ (passive)}$ represents the failure rate associated with internal breakage and λ_{DU} is the original failure rate of the relay representing other modes of failure, e.g. welded contact. Based on this simplifying assumption and by applying *cf* = 0.001 as an starting point the failure rate that we are going to use in the PFD calculations for RBD#1 will be 6.0E-10, given λ_{DU} = 6.0E-07 as in Table 3. Later on, in Subsection 3.5, we will use a range of the *cf* to further analyze the impact of uncertainty associated with the failure rate of the interposing relays.

- **Option A, SIF#1, ESV Block (RBD#2)**: RBD#2 models the failure of the elements between the OSPS and the ESV lines. The DO modules in this model, too, are utilized in *passive* mode. Again, we assume the failure rate is negligible. This model is in fact a 2oo3 combination of the trip relays only. The DO blocks are still shown in the RBD diagram, but the failure rate of these blocks is considered to be 0.0.
- **Option B, SIF#1, MCV/ESV Block (RBD#3)**: The only interface between the trip outputs of the OSPS and both the ESV and MCV trip blocks in option B is the 2oo3 combination of the trip relays. The RBD for both the MCV and ESV connections will be the same, i.e. RBD#3.
- **Option A, SIF#2, MCV Block (RBD#4)**: Interposing relays in this model are utilized in *passive* mode, for which we will use the failure rate mentioned above: 6.0E-10. However, DO modules are used in *reactive* mode and therefore their original failure rate, given in Table 3, will not require any adjustments for PFD calculations. Although, we should remember that the channel diagnostics of the DOs in this model are inactive, which means a higher failure rate should be considered for the DO modules. This matter will be elaborated later in Subsection 3.5. For the time being, the PFD value will be calculated by using the original failure rate without applying any adjustments.
- **Option A, SIF#2, ESV Block (RBD#5)**: This model is comprised of a 2oo3 combination of DO modules used in *reactive* mode with their diagnostics enabled. Therefore, this model does not require any changes to the original failure rates given in Table 3.
- **Option B, SIF#2, MCV/ESV Bock (RBD#6)**: Similar to RBD#3, this model can be considered for both the MCV and ESV. The trip signal from the SIS CPU de-energizes the trip relays through two parallel routes: directly through the OSPS's output contacts, and indirectly through the OSPS's voting inputs.

The trip command from the OSPS then de-energizes the 2oo3 combination of the trip relays, in order to trip the process.

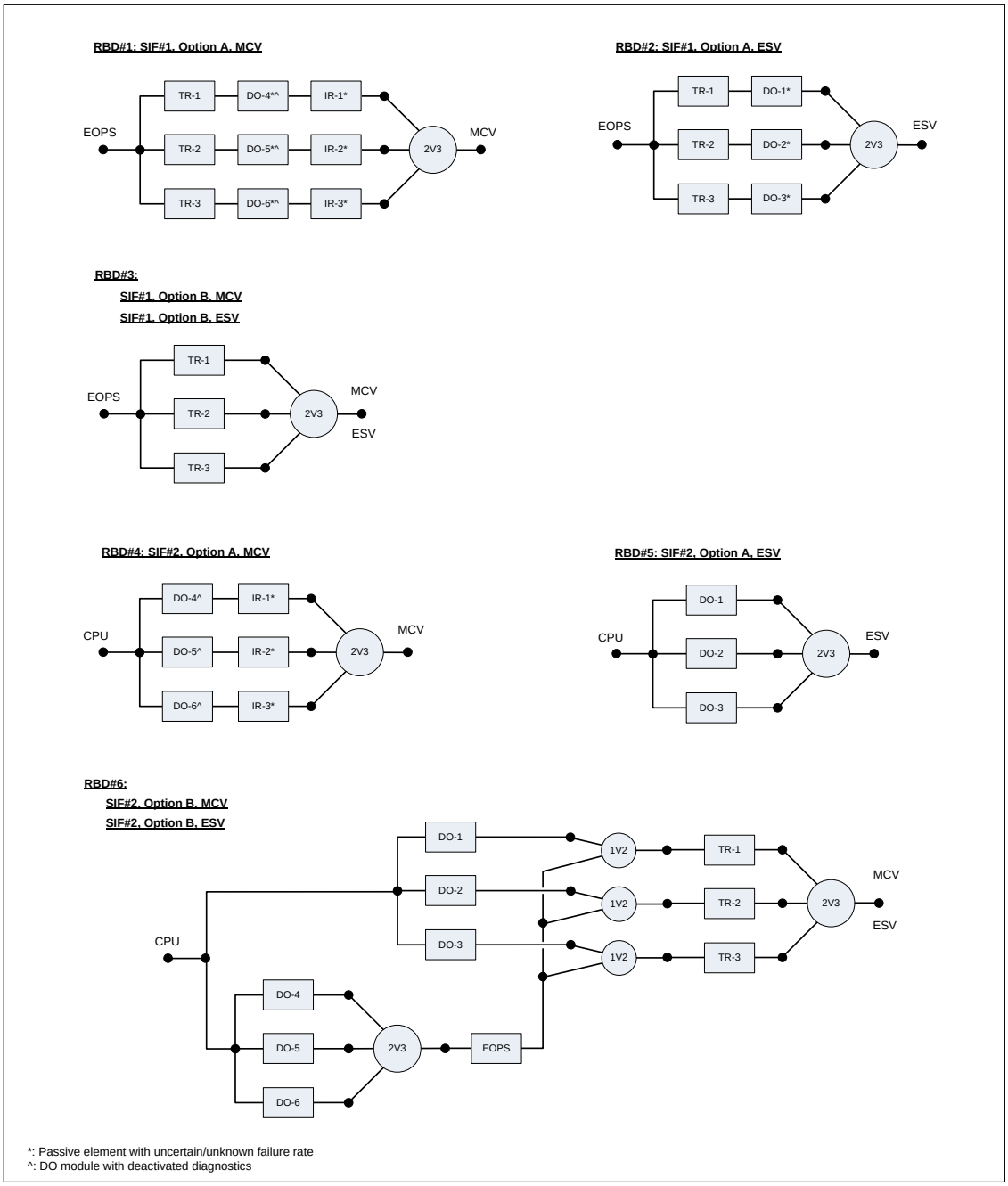

Figure 3: Reliability block diagrams (RBDs)

Table 4 contains the results of the PFD calculations for the RBDs explained above. This table uses the simplified PFD formulas given in [1] with a proof test interval of five years. A quick look at the figures in Table 4 shows that option B delivers a lower probability of failure, which confirms the outcomes of the qualitative comparison in Subsection 3.3.

The first observation one may make by looking at Table 4 is that the PFD value for RBD#3, which is only a 2oo3 combination of the safety relays TR01-03, is almost identical to the ones of RBD#6, which constitute a more complex configuration. This means the collective failure rate of the elements upstream the TRs in RBD#6 is

negligible, compared to the failure rate of the TRs. This should not be surprizing when considering the parallel trip lines through the OSPS, the 2oo3 combinations of the DO modules connected to the voting inputs of the OSPS, and the small failure rate of the OSPS itself. These factors result in a negligible collective failure rate.

No	SIF	Option	Trip Block	PFD_{avg}	RBD
1	SIF#1	A	MCV	1.92E-09	1
2			ESV	3.07E-10	2
3		B	MCV	3.07E-10	3
4			ESV	3.07E-10	3
5	SIF#2	A	MCV	4.91E-09	4
6			ESV	1.92E-09	5
7		B	MCV	3.08E-10	6
8			ESV	3.08E-10	6

Table 4: PFD_{avg} calculations for MCV/ESV trips

Another point we can observe from Table 4 is the significant difference between options A and B for SIF#2. Option B, as pointed out above, is dominated by the 2oo3 combination of TRs; whereas option A is dominated by the 2oo3 combination of DOs. Based on the failure rates in Table 3, one can easily find out why: the failure rate of the trip relay is smaller than the failure rate of the DO module. This indicates that the failure rate ratio between the DO modules and the TRs can be crucial, and option B provides a lower PFD value only if the failure rate of the TRs is not higher than the failure rate of the DO modules. This may not be hard to achieve, though, given that the TRs in this case are simple devices (Type A in accordance with IEC61508, [2]), whereas the DO modules are complex electronics (Type B in [2]).

3.5. Unknowns and uncertainties

The PFD values calculated for RBD#1 and RBD#3 in Table 4 use λ_{DU}= 6.00E-10 for the failure rate of the interposing relays, which is the original failure rate multiplied by the correction factor *cf* = 0.001. We assumed that the chance of an internal breakage in an SSR is 1000 smaller than the chance of its contact not changing its state when the state of its coil is changed. Is this a fair assumption? Could the chance of internal breakage be less, or perhaps more?

This is an example of unknowns and uncertainties associated with using *passive* elements, for which one should either find an alternative solution, like rearranging the components, or perform an analysis to narrow them down to a number of justifiable assumptions.

In order to see the impact of uncertainty in reliability modelling, we calculate the PFD values for a range of the correction factor *cf*. Figure 4 shows the results of PFD calculations for RBD#1 and RBD#4 with the *cf* given between 1.0E-06 and 1.0E-3. The PFD calculations of RBD#3 and RBD#6 are depicted on the same diagrams in Figure 4 for better comparison between options A and B. Referring to these diagrams, for a *cf* of 1.0E-06, the PFD values are:

RBD#1: 3.08E-10, RBD#3: 3.07E-10

RBD#4: 1.92E-09, RBD#6: 3.08E-10

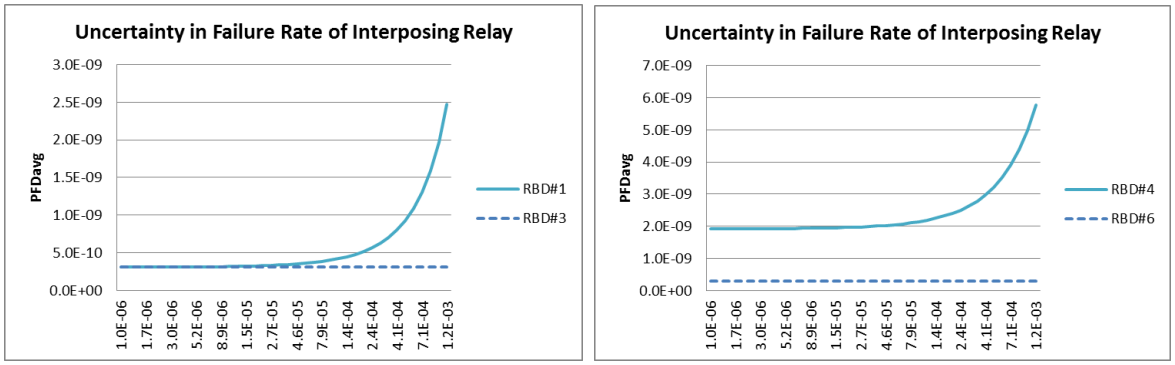

Figure 4: PFD_{avg} vs. λ_{DU} of interposing relay for RBD#1 (left) and RBD#4 (right)

As can be seen, even with a correction factor of 1.0E-06, option B is still in better shape. As *cf* increases, the PFD values of option B (i.e. RBD#3 and RBD#6) remain constant, but the PFD values of option A (i.e. RBD#1 and RBD#4) increase. For *cf* = 1.0E-03, the PFD values are:

RBD#1: 1.92E-09, RBD#3: 3.07E-10

RBD#4: 4.91E-09, RBD#6: 3.08E-10

The above figures indicate that not only option B has fewer unknowns and uncertainties, but it also delivers a lower probability of failure.

Another simplifying assumption that was made in calculating the PFD values in Table 4 was that the deactivated diagnostics in the DO modules connected to the contacts of interposing relays did not have any impact on the failure rate of the DO modules, which we know cannot be true. As explained in Section 4, deactivated diagnostics can increase the failure rate of components. As good engineering practice, the first priority is to keep diagnostics active and maximize the possible coverage. However, if the diagnostics of an element needs to be deactivated for any engineering reasons, analysis will be required to assess the adverse impact on the reliability of the system.

For option A, we assume that only the diagnostics of individual channels are deactivated, and the diagnostics of common parts in the DO module remains active. Therefore, we can at least assume that the diagnostic coverage, i.e. DC, was not reduced all the way down to 0%; although the actual value of the DC remains unknown and can only be determined through a Failure Mode Effect and Diagnostics Analysis (FMEDA) by the manufacturer. Let us examine the DC for the range of 20% to 99% and recalculate the PFD, and observe the impact of this uncertainty on our models. Given that the failure rate of the DO modules in RBD#1 was considered to be 0.0, we only need to redo the calculation for RBD#4. Figure 5 shows the changes of the PFD (y-axis) of RBD#4 against the range of the DC (x-axis) from 20% to 99%.

As can be seen, depending on the DC factor, the PFD can vary considerably. To gain a better understanding of this dependency, let us have a look at the PFD values at the two ends of the DC range shown in Figure 5:

For DC = 99%: RBD#4: 4.91E-09, RBD#6: 3.08E-10

For DC = 20%: RBD#4: 1.25E-05, RBD#6: 3.08E-10

Again, the figures confirm that option B is a better choice as it lowers the probability of failure and it reduces the unknowns and uncertainties.

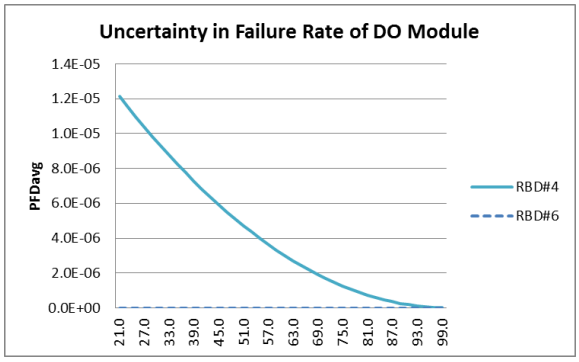

Figure 5: PFD_{avg} vs. DC for RBD#4

3.6. Spurious trip

Any random, undesired closing of either the MCV or ESV will result in a complete shutdown of the turbine. In order to calculate the STR, we should first find the possible combinations of component failures that can lead to the depowering of the 2oo3 lines of the ESV or MCV trip blocks.

Although the number and the types of components are the same in options A and B, the trip scenarios generated by faulty components can be different, depending on the locations and the functions of the faulty components. Consider DO modules DO01-03 as an example: in option B, the 2oo3 combination of safe failure of these modules closes both the ESV and the MCV. The same failure in option A only closes the ESV.

Table 5 compares different causes of spurious trips between options A and B. In option B, all trip causes except the 2oo3 combination of the interposing relays close both the MCV and the ESV. But in option A, trip scenarios are different. Different trip scenarios, depending on the initiating cause, result in closing the ESV, MCV, or both.

Safe Failure Combination	Option A	Option B
2oo3 Interposing Relays	Trips MCV	Trips MCV
2oo3 Trip Relays	Trips MCV & ESV	Trips MCV & ESV
2oo3 DO01-03	Trips ESV	Trips MCV & ESV
2oo3 DO04-06	Trips MCV	Trips MCV & ESV
OSPS	Trips MCV & ESV	Trips MCV & ESV
SIS CPU	Trips MCV & ESV	Trips MCV & ESV

Table 5: Spurious trip combinations in options A and B

In the particular example of turbine upgrade project, the STR value will be the same for both options A and B, because the trip causes and the combinations of components' failure initiating spurious trips are the same. However, an observation that we can make from this case study is that spurious trip is not all about numbers and figures. One should also consider analyzing *how* the failure combinations may result in spurious trips. Such reviews may assist with identifying potential hazards that can take place as a result of partial isolation of the process (e.g. closing some,

but not all, final elements). Table 5 shows an example of how different the trip scenarios can be even where the STR values are the same.

4. Basic rules in complex SIS arrangements

The turbine upgrade example explained in Section 3, and the comparison between simplified models given in [3], shows that SIS architecture in complex applications can be improved by establishing the following guidelines:

I. *Simplifying the architecture*: The higher the number of elements from the *active*, *reactive* and *passive* categories added in series to a SIF, the higher the PFD and STR figures will become. Having a large number of elements can also increase the number of arrangement options, and consequently the engineering time required for analysis and design optimization process.

II. *Considering the effect of dominating components*: Although SIS design should be kept as simple as possible, one should not forget the role of dominating elements, i.e. components with high failure rates.

III. *Obtaining relevant failure data*: Not only should the component data be reliable, but it should also be relevant to the arrangement in which the component is utilized. For instance, the failure rate which is given for the welded contacts of a relay is not relevant in PFD calculations if the SIS output is wired to the contacts of the relay and not to its coil, as the contacts act like a termination points in this scenario. When using *passive* components, one will also need to consider the potential faults that may not have been covered by the available information, as they can lead to dangerous failure of the SIF if they take place. Not every non-certified component comes with detailed Failure Mode Effects Analysis (FMEA) reports. Furthermore, not every FMEA report includes all 'unlikely' failure modes that may only interest a few users who utilize the component in *passive* mode. It is important to first identify the right failure modes specific to the application, and then find the right failure data that correctly represents those failure modes.

IV. *Avoiding unknowns and uncertainties*: Uncertainties and unknowns cannot be resolved by making assumptions. One should either perform the necessary analysis to back their assumptions, or consider alternative solutions to avoid unknowns and uncertainties, as long as such alternatives still meet the safety requirements. Detailed analysis of uncertainties and unknowns is not always easy. It takes effort to find the right data; it takes additional engineering time to model and analyze the data; and, worst of all, the analysis does not necessarily result in 'good news'. Alternative component arrangements can sometimes provide more reliable solutions at no additional cost. As a system integrator, one may find looking for alternative solutions more practical than analyzing the internal faults of components without access to adequate details.

V. *Giving precedence to active and reactive components: Active* components are less likely to remain in undetected failure modes for long. *Reactive* elements are more prone to undetected faults but, fortunately, access to their failure data is normally possible. When it comes to *passive* elements, the challenge is to deal with undetected failure modes for which the data may not be available at all. The question here is not about the authenticity and accuracy of existing failure data, but rather the existence of documented failure modes in the first place; and for system integrators, it is not always practically

possible to address such issues. In general, *active* components should be given precedence over *reactive* ones, where possible, and the use of *passive* elements should be minimized, unless uncertainties and unknowns are appropriately addressed.

VI. *Prioritizing between SIFs*: Different SIFs that are allocated to different logic solvers within a SIS may have different target Risk Reduction Factors (RRFs). When more than one arrangement option is available, priority may be given to the SIF with the higher target RRF. Other aspects of design, such as architectural requirements, response time requirements, and compatibility between components may also be taken into account for prioritization.

VII. *Optimizing the location of components*: A chain is as strong as its weakest link. A key factor in designing optimal SIS architecture is the location of the weaker elements. The example of turbine upgrade project showed how an easy change in the location of an interposing relay can improve the collective integrity of the SIF and eliminate uncertainties in reliability modelling. The first step in rectifying weak links is to identify them through means of reliability modelling. One can then attempt to rearrange the location of the components in order to shift the weaker elements to the locations where their failure can least affect the integrity of the SIF. Other options in fixing weak links include using stronger alternatives and/or increasing hardware redundancy. Such solutions are typically more costly, compared to optimization of component arrangement.

VIII. *Minimizing the response time and delay*: Response time can be critical in both control and safety systems. Sources of delay include additional layers of processing (e.g. when the output of BPCS has to go through SIS in order to drive a final element) and potential delay in depowering electronic modules when used in *passive* mode.

IX. *Considering the processing capacity of CPUs*: In addition to the response time and the delay that might affect a BPCS or a SIS logic solver, when their output is fed to the input of a second SIS logic solver, one should not forget the impact of the additional processing load imposed onto the second SIS logic solver itself. Depending on the processing capacity of CPUs in question, additional processing may result in reduction of performance additional chance of failure.

X. *Maximizing the extent of diagnostics*: The scope and extent of diagnostics in DO modules lessens when interposing relays are used between the modules and final elements. Moreover, where interposing relays are used for interfacing between the BPCS and SIS, the diagnostics of relevant DO channels may need to be deactivated in order to make the combination of the BPCS and SIS work together. The deactivated diagnostics will then need to be made up for by alternative measures which will, in turn, add to SIS design complexity and engineering costs. In addition to operability issues, partial deactivation of the diagnostics will increase the original failure rate as well.

XI. *Analyzing the influence of links and supplies*: Despite the quiet role of *links* and *supplies* in SIS, one should not forget that they sometimes can be sources or carriers of notorious dangerous faults. Ineffective earthing, loose terminations, unmonitored power sources, blocked instrument air filters, cables damaged by vermin, and similar types of faults can potentially lead to

dangerous failures of SIFs or spurious trip of plants. In some projects, field cabling and power sourcing is designed and installed by third party companies who may not fully realize the extent of the impact of their works on the safety system. Care should be given at all stages of the project life cycle to establish adequate coordination between the SIS designers and other parties, and to ensure that both systematic and random failures are minimized to the lowest possible level. An effective proof test can be helpful in finding and resolving such issues during commissioning. Nonetheless, the SIS arrangement should consider optimization in relation to *links* and *supplies*.

XII. *It is not all about numbers*: It should be remembered that PFD and STR are only two quantitative indications of the integrity of a SIS, and other structural criteria, such as Architectural Constraints and Systematic Capability [2], should be considered in designing the optimum arrangement for complex SIS.

5. Conclusion

The arrangement of components in complex SIS can have crucial impacts on the performance of a safety system. Small adjustments to the arrangement of components can sometimes result in considerable improvements in reliability criteria such as PFD, STR, architectural sensitivity and model uncertainty. This was demonstrated through a real-life example in Section 3.

Where more than one option is available for SIS architecture, detailed analysis should be carried out to design the optimal arrangement of SIS components. The classification of the SIS components given in Section 2 and the design guidelines given in Section 4 can assist safety engineers with the design and analysis of the complex SIS architecture. In summary, the following key points should be taken into account when designing the arrangement of components in complex SIS architectures:

- The failure rate of a component is only applicable when associated with the relevant failure mode. Depending on the utilization of a component, the failure data given by the reference sources may not be applicable.
- Unknowns and uncertainties should be thoroughly analyzed, or otherwise avoided. Better-known components and adjustments in SIS arrangement can be considered when avoidance is preferred.
- Priority should be given to using *active* elements over *reactive* elements; and to *reactive* elements over *passive* elements.
- Partial or complete deactivation of diagnostics should be avoided as it otherwise increases the failure rate of components as well as the level of uncertainty in reliability modelling.
- When studying spurious trips, in addition to STR calculations, one should address the ‘how to’ element of the trip scenarios as well.
- Rearranging the SIS components can be an effective means for optimizing the SIS architecture and improving the performance of the SIS at no additional cost.

6. References

[1] D. J. Smith, 2011, Reliability maintainability and risk - practical methods for engineers. Eight Edition, Elsevier.

[2] IEC 61508, 2011, Functional safety of electric/electronic/programmable electronic safety-related systems, Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.

[3] H. Jahanian, A. Lucas, 2015, “The role of component arrangement in complex safety instrumented systems—A case study,” Process Safety and Environmental Protection 94: 113–130.

[4] IEC 61508, 2011, Functional safety of electric/electronic/programmable electronic safety-related systems, Part 4: Definitions and abbreviation.

[5] ISA-TR84.00.02, 2002, Safety instrumented functions (SIF) - safety integrity level (SIL) evaluation techniques, Part 2: Determining the SIL of a SIF via simplified equations.

[6] IEC 61508, 2011, Functional safety of electric/electronic/programmable electronic safety-related systems, Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.

[7] H. Jahanian, 2015, “Generalizing PFD formulas of IEC61508 for KooN configurations,” ISA Transaction (currently available in online format only).