Risk-Based Approach – Preventing Hazardous Scenarios

An Introduction to Safety Instrumented Systems (SIS)

An ioMosaic White Paper

Jordi Dunjó, Ph.D.

Marcel Amorós

Neil Prophet

Gene Gorski

Abstract

Safety Instrumented Systems (SIS) are a specific layer of protection that requires detailed knowledge and criteria for proper definition and installation based on functional safety principles and associated standard requirements. This paper focuses on providing guidance and criteria for conducting the following tasks: (1) how to link risk analysis results with functional safety concepts, (2) basics for systems verification via calculating the average Probability of Failure on Demand (PFD_{avg}) and (3) available techniques to be used when verifying complex SIS.

Table of Contents

List of Tables

List of Figures

Introduction

Reference **[1]** provides an overview of layers of protection suitable to reduce the risk level of a process facility, i.e., measures intended to prevent and/or mitigate the identified hazardous scenarios. The cited paper **[1]** explains that based on the results of a risk-based quantitative assessment, zones or locations and their associated hazardous scenarios having the most significant intolerable risk level can be identified. . As a result, sensitivity and cost-benefit analyses can be performed with the aim to decide which safeguards achieve to reduce the risk to an acceptable level at the most reasonable cost.

From all layers of protection considered in reference **[1]**, the Safety Instrumented Systems (SIS) and performance-based Fire and Gas Detectors Systems (FGS) are safeguards that should comply with very specific requirements based on the following standards; i.e., IEC 61508 **[2]**, IEC 61511 **[3]** and ISA 84.00.TR.07 **[4]**, respectively. While performance-based FGS selection, verification and mapping guidance can be found in reference **[5]**, the main purpose of this paper is to address SIS intended to comply with standards **[2]** and **[3]**. A SIS consists of at least three subsystems:

- **Sensor subsystem**: One or more sensors that are installed to detect the demand and to send the signal to the logic solver subsystem. Examples of input systems may be switches, sensors, transmitters, transducers.

- **Logic solver subsystem**: One or more logic solvers that receive the signals from the sensor subsystem, interpret these signals and decide which actions should be taken. Examples of logic solvers may be based on electrical relays, electronic components (e.g., printed circuit boards), programmable logic controllers (PLC), computers.

- **Final element subsystem**: One or more final elements (i.e., actuating devices) that take a prescribed action from the logic solver subsystem to prevent the hazardous scenario/demand from occurring. Examples of final elements may be valves, relays, circuit breaker capable of stopping flow and isolating electrical equipment.

Therefore, all SIS subsystems must act simultaneously to detect the deviation (i.e., demand) and bring the process into a safe state by implementing a Safety Instrumented Function (SIF). This main purpose can be accomplished if the SIS achieves the necessary level of functional safety based on the process characteristics during the Safety LifeCycle (SLC).

Safety LifeCycle (SLC) Definition

The SLC is an engineering process that contains all the steps needed to achieve high levels of reliability during conception, design, operation and maintenance of instrumentation systems is an automation system designed according to SLC requirements will predictably reduce risk in an industrial process. **Figure 01** illustrates a simplified SLC diagram and the three main phases associated to it:

- Risk analysis
- Design and implementation
- Operation and maintenance

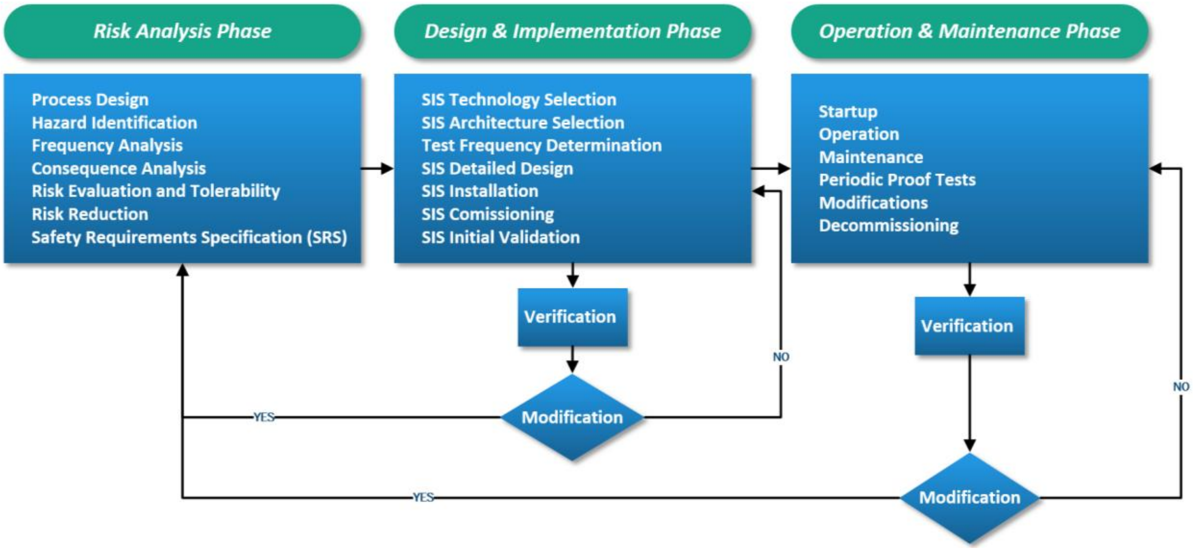

Figure 01: Simplified SLC Flowchart

Figure 01 highlights that the SLC is a feedback system incorporating two verifications: (1) verification after conceptual design and (2) periodic verification during operation.

Risk Analysis Phase

The risk analysis phase is used to identify and quantify the risk level of all potential hazardous scenarios that could occur in a process facility. Additionally, the predicted risk level is compared with internationally recognized risk tolerability criteria to verify if risk reduction is required. When the actual risk level is higher than the applicable tolerable risk level, then risk reduction measures shall be considered. Inherently, if a higher gap is identified between the actual and tolerable risk levels, installation of more reliable safeguards is required to correct the actual value to the desired tolerable risk level. This gap defines the concept, “Risk Reduction Factor (RRF)”, which is expressed as follows:

$$RRF = \frac{Actual\ Risk\ Level}{Tolerable\ Risk\ Level}$$

Equation 01

The risk analysis phase is not under the scope of the present paper and each step required to be completed (see **Figure 02**) has been fully defined in dedicated references **[5]**, **[6]**, **[7]**, **[8]**, **[9]**, **[10]**, **[11]**, **[12]** and **[13]**.

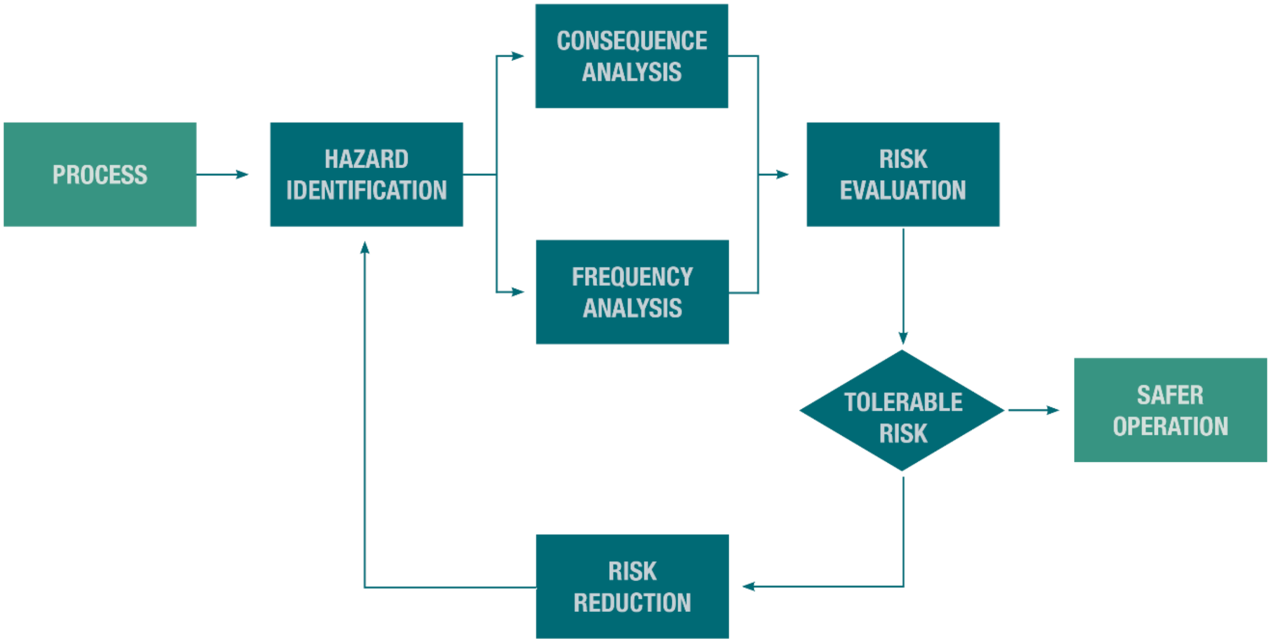

Figure 02: Simplified Risk Analysis Flowchart – Risk Analysis Phase

While the risk analysis phase can be conducted either qualitatively (e.g., via risk matrices, risk graphs) or semi-quantitatively (e.g., via Layer of Protection Analysis – LOPA), the proposed risk analysis phase is a complete risk-based quantitative assessment, which is valuable for characterizing SIS and is the basis for many other process safety and loss prevention purposes such as emergency-planning, land-use planning, facility siting, domino effect.

Assuming that the risk-based quantitative assessment has been successfully completed and the RRF has already been quantified per each hazardous scenario, a Safety Requirements Specification (SRS) document is then developed. The SRS is a living document and the specific section that covers all the information related to the risk analysis phase should be continuously updated after initially quantifying the RRF of the hazardous scenario considered. The SRS must address the two main categories of requirements:

- Safety functional requirements: Which are the SIFs to be implemented to prevent or act upon demands (or hazardous scenarios)

- Safety integrity requirements: How reliable the SIFs must be to achieve adequate risk reduction. The concept of "Safety Integrity Level – (SIL)" relates the predicted RRF with the required SIF reliability level

Note that the term *reliability* is defined as the ability of an item (element, channel, subsystem, or the complete SIS) to perform a required function under a given environmental and operational conditions and for a stated period.

Safety Requirement Specification (SRS) document

The SRS is a document where all the safety requirements for a SIF are stated clearly. The requirements may come from applicable standards **[2]** / **[3]** or may be company and application-specific requirements. The SRS must address the two main categories of requirements associated with each SIF: safety functional and safety integrity requirements.

Note that the SRS is a design-related document and must be updated throughout the whole life cycle of the SIS. A proposed structure of an SRS is provided in Annex E of NOG-070 **[14]**.

Design and Implementation Phase

A conceptual design is performed by choosing the desired technology for the components that constitute the SIS. Furthermore, redundant components may be included to achieve high levels of safety integrity and/or to minimize false trips. Thereafter, the designers will review the periodic test philosophy requirements provided in the SRS, a parameter of key importance as most SIS considered in the process industry are "low demand." Finally, the SIS will be only activated when a hazardous scenario occurs. Accordingly, periodic testing has to be performed to ensure that all elements within a SIS are fully operational when the safety function is required.

Once SIS technology, architecture and periodic test intervals are defined, a reliability and safety evaluation is conducted to verify that the selected design can accomplish the target RRF estimated during the risk analysis phase. The SIS design must meet the SIL and reliability requirements established in related functional safety standards **[2]** / **[3]**. Note that covering the SIS design and implementation phase (i.e., the **probabilistic SIF verification**) is the main topic of this paper and it will focus on low demand systems.

Operation and Maintenance Phase

Prior to starting the operation and maintenance phase, the first verification shall be performed (see **Figure 01**). This verification normally is conducted by a Pre-Startup Safety Review

(PSSR), which its goal is to verify that the conceptual SIS design complies with all SRS requirements and documentation. Once the system is in operation, proper operating procedures and maintenance activities should be ensured and implemented modifications during the system lifecycle have to be analyzed, with the aim to check that no new hazardous scenarios are being introduced and that the system will continue to function as is expected, i.e., Management of Change (MOC). If the system is to be decommissioned, the decommissioning impact has to be analyzed. The operation and maintenance phase is out of the scope of the present manuscript and the reader is referred to specific standards **[2]** / **[3]**.

Functional Safety Assessment (FSA)

After introducing all phases of the SIS SLC, it is important to discuss the Functional Safety Assessment (FSA). A FSA is a systematic and independent examination of the adequacy of the functional safety achieved by the SIS within a particular environment. It is normally carried out by one or more professionals (from the company or independent third party) that should have access to all relevant individuals that have been involved in the design of the SIS and to all relevant documents.

The FSA can be performed after each phase of the SLC or after concluding a specific number of phases. The FSA should, at a minimum, verify the items listed in **Table 01**.

Note that Chapter 8 of IEC 61508-1 **[2]** provides detailed guidance for FSA requirements.

Table 01: Topics to be Reviewed During the FSA Examination

#	Description
1	Risk analysis phase recommendations are implemented
2	The SRS is followed in the Design and Implementation phase
3	Operating and Maintenance phase procedures pertaining to the SIS are in place
4	The validation of the SIS is properly done
5	Employee training related to the SIS is completed
6	Recommendations from previous FSAs have been resolved

Linking the Quantitative Risk-Based Assessment with Functional Safety

The following section explains additional steps that follow a typical quantitative risk-based assessment to ensure that all information and requirements in the SIS risk analysis phase are covered and developed. These additional steps correlate the risk evaluation results that identification hazardous scenarios requiring a certain RRF with specific safety, functional and integrity requirements to be stated in the SRS. These requirements are considered the basis for starting the SIS design and implementation phase.

Functional Safety Requirements

The Functional Safety Requirements include defining relevant and realistic SIFs for each hazardous scenario (resulting in a demand) for areas or specific targets with intolerable risk levels is required. Accordingly, a SIF will be completely defined after addressing its modes of operation and its conforming subsystems:

Two SIF modes of operation can be defined according to IEC 61511 **[3]**:

- Demand or low demand mode: The SIF is passive because it does not perform any active function during normal operation and is only called upon when a hazardous condition may occur or may be present.
- Continuous mode: The SIF plays an active role in the control of the process system and a hazardous event will occur almost immediately when a dangerous failure of the SIF occurs.

Based on the definition of these two modes of operation, the Chemical Process Industry (CPI) mainly uses mostly low demand SIFs and therefore continuous mode SIFs are not covered in this paper. Note that the SIS element can be designed according to two different principles:

- Energize-to-trip: The SIS element is normally de-energized and requires energy (e.g., by electricity, hydraulic pressure, pneumatic pressure) to perform its safety function (i.e., to *trip).* Loss of energy will, by this principle, prevent the element from performing its safety function.
- De-energize-to-trip: The SIS element is normally energized and removal of the energy will cause a trip action. By this principle, loss of energy will cause a spurious (i.e., false) activation of the safety function.

Many SIS elements are currently designed according to the de-energize-to-trip principle. This principle is also the basis for the fail-safe principle, which is a design property that causes an SIS element to go to a predetermined safe state in the event of a specific failure or malfunction.

A SIS that implements a SIF has two main functions:

- *Perform the SIF on demand.* This is the essential function of the SIS and why it has been installed. When a demand occurs, the SIS shall carry out the SIF according to the performance criteria specified in the SRS. The probability of a failure of this function is usually quantified by the average Probability of Failure on Demand (PFD$_{avg}$) and the main objective of this manuscript is to provide guidance and criteria for estimating the PFD$_{avg}$ for relevant SIS architectures.

- *Do not activate the SIF without the presence of a demand.* A failure of this function may lead to loss of production or service and have safety consequences. Such a failure is classified as a safe failure and is often called a false alarm or a spurious trip.

Note that the calculation of the probability of a Spurious Trip (i.e., STR) is out of the scope of this manuscript, but most guidance and criteria applicable to PFD$_{avg}$ evaluation is also useful for the STR characterization.

Functional Integrity Requirements

Once SIFs have been defined, its expected reliability to comply with the given tolerability risk criteria is calculated by allocating the required SIL. The SIL depends on the RRF of each demand characterized during the risk analysis phase development. Additionally, and as a function of the SIL and other parameters, the redundancy of the SIF can be defined as a procedure that allows for specifying the SIF architecture.

Reliability Requirements - Relationship Between RRF, PFD$_{avg}$ and SIL

One of the key parameters calculated during the risk analysis phase is the required availability of the safety function that is capable of reducing the actual risk level to the desired tolerable risk level. This availability is characterized by the SIL, which is a function of the predicted RRF and which directly defines the target PFD$_{avg}$ in the probabilistic SIS verification. The PFD$_{avg}$ is a term defined for low demand systems.

The relationship between RRF and PFD$_{avg}$ is illustrated in **Equation 02** and the relationship between RRF, PFD$_{avg}$ and SIL is listed in **Table 02**.

$$PFD_{avg} = \frac{1}{RRF}$$

Equation 02

Table 02: Relationship Between RRF, SIL and PFD_{avg} for Low Demand Systems

RRF	PFD_{avg}	SIL
10,000 ≤ RRF < 100,000	1.00E-05 ≤ PFD_{avg} < 1.00E-04	4
1,000 ≤ RRF < 10,000	1.00E-04 ≤ PFD_{avg} < 1.00E-03	3
100 ≤ RRF < 1,000	1.00E-03 ≤ PFD_{avg} < 1.00E-02	2
10 ≤ RRF < 100	1.00E-02 ≤ PFD_{avg} < 1.00E-01	1

Thus, estimating the RRF directly provides the required system availability as illustrated in **Table 01**.

Architecture Requirements - SIF/SIS Redundancy

Once the relationship between RRF, SIL and PFD_{avg} is defined for the SIF, additional associated requirements such as the Minimum Hardware Redundancy Requirements or Hardware Fault Tolerance, HFT, must be met based on criteria established in the functional safety standards **[2]** / **[3]**. The concept HFT is used to indicate the ability of a hardware subsystem to continue to perform a required function in the presence of faults or errors.

Therefore, these requirements are intended to protect against unrealistic parameter estimates in the PFD_{avg} calculation.

The architectural constraints consider the following:

- The complexity and type of each element of the SIS. IEC 61508-2 **[2]** divides elements into two types, (Type A and Type B). **Table 03** lists the main characteristics of these types.

- The Safety Failure Fraction (SFF), used to quantify the inherent tendency of a SIF to fail towards a safe state. It is an element property as it is independent of its implementation and normally is supplied by the manufacturer. The SFF is calculated according to **Equation 03**.

Table 03: Complexity and Type of Each SIS Element

Type	Feature
A	Failure modes of all constituent components of the element are well defined, **AND**
	Behavior of the element under fault conditions can be completely determined, **AND**
	Sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failure are met
B	Failure mode of at least one constituent component of the element is not well defined, **OR**
	Behavior of the element under fault conditions cannot be completely determined, **OR**
	Insufficient failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failure are met

Note: Most of logic solvers are Type B.

$$SFF = \frac{Sum\ of\ the\ rate\ of\ safe\ and\ detected\ dangerous\ \ failures\ of\ the\ element}{Sum\ of\ the\ rate\ of\ safe\ and\ dangerous\ failures\ of\ the\ element} \quad \textbf{Equation 03}$$

***Note that the "failure rate" concept is introduced later in this manuscript.

IEC 61508 **[2]** suggests two different routes to compliance for each SIS element:

- **Route 1$_H$**: Based on HFT and SFF criteria, which is illustrated in **Table 04**.
- **Route 2$_H$**: Based on only the HFT and SIL criteria if there is high confidence (90%) in the quality of the failure data. SFF is not considered. (see **Table 05**). Route 2$_H$ does not differentiate between Type A or Type B.

Table 04: IEC 61508 Architecture Requirements – Route 1$_H$

SFF [%]	HFT = 0		HFT = 1		HFT = 2	
	Type A	**Type B**	**Type A**	**Type B**	**Type A**	**Type B**
SFF < 60	SIL 1	Not Allowed	SIL 2	SIL 1	SIL 3	SIL 2
60 ≤ SFF < 90	SIL 2	SIL 1	SIL 3	SIL 2	SIL 4	SIL 3
90 ≤ SFF < 99	SIL 3	SIL 2	SIL 4	SIL 3	SIL 4	SIL 4
SFF ≥ 99	SIL 3	SIL 3	SIL 4	SIL 4	SIL 4	SIL 4

Table 05: IEC 61511 Architecture Constrains – Route 2_H

SIL	HFT
1	0
2	0
3	1
4	2

The HFT accounts for the required redundancy, which means having two or more items, such that if one item fails, the system can continue to function by using the other items. The concept of redundancy introduces the Voting concept.

Voting

Figure 03 illustrates the sensor, logic solver and final element subsystems of a SIS. Each subsystem may have one or more voted groups or channels. A channel is defined as a structure of one or more elements that can independently perform a safety function. For example, the block denoted as "pressure transmitter" (see **Figure 03**) is a channel intended to detect when the pressure goes beyond acceptable limits and send a signal to the logic solver subsystem.

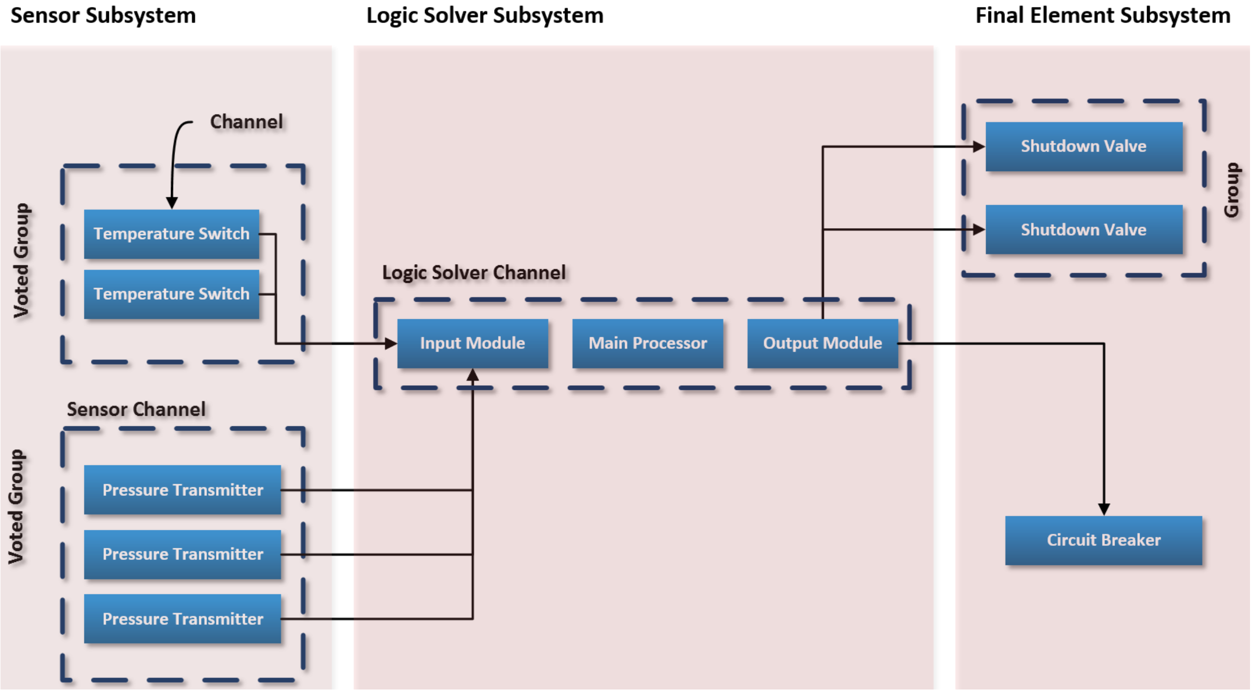

Figure 03: SIS Subsystems Including Groups and Channels

A group of ***n*** identical channels can be configured in several ways. One extreme is when the group is functioning only when all the ***n*** channels are functioning; the other extreme is when the group is functioning as soon as at least one channel is functioning.

The first extreme case is called an **n-out-of-n** voted structure and the second a **1-out-of-n** voted structure. In a general case, the group may be configured such that it is functioning when at least ***k*** of its ***n*** channels is functioning (a ***k-out-of-n*** voted structure). Such a structure is often written ***koon*** and is said to be ***koon*** voting*.*

Assume a 2oo3 voting of a group of three pressure transmitters as illustrated in **Figure 03**. The voted group of the three pressure transmitters is functioning when at least two of the transmitters are able to detect and transmit signal when the pressure goes beyond the acceptable limits. When the logic solver subsystem receives signals from at least two transmitters, the signals are treated and a decision about action is made. Therefore, a HFT = 1 means that if a channel fails, there is one other channel that is able to perform the same function, or that the subsystem can tolerate one failure and still be able to function. A subsystem of three channels that are voted 2oo3 is functioning as long as two of its three channels are functioning. This means that the subsystem can tolerate that one channel fails and still function as normal.

The hardware fault tolerance of the 2oo3 voted group is, HFT = 1. The same concept is applicable for explaining HFT = 0 and HFT = 2. HFT can be defined as the ability of a functional unit to perform a required function in the presence of faults. A HFT of ***N*** means that ***N+1*** faults could cause a loss of the safety function.

While redundancy can improve the reliability of the system, it introduces additional potential failures due to common cause failures. For example, if a 1oo2 voting configuration is powered by the same power supply, the SIF will not be performed if a failure occurs in this power supply. Common cause failures will be addressed in this paper after introducing the concept of failure rates.

“Safety Culture” Requirements - SIF/SIS Systematic Capability

IEC 61508 **[2]** defines two different categories of failures:

- Random Hardware Failure: Failure occurring randomly, which result from one or more of the possible degradation mechanisms in the hardware.

- Systematic failures: Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors.

Random hardware failure characterization is performed via the probabilistic analysis of the SIF during verification. Knowledge on RRF, SIL, HFT, SFF and additional parameters allow performing mathematical calculations that ensure the reliability of the SIS.

However, systematic failures are not covered during the SIS verification calculations and this justifies the systematic capability requirements. The concept of systematic capability was introduced in the 2010 edition of IEC 61508 **[2]** and is a measure of the effectiveness of quality management techniques applied to components. Therefore, because systematic failures are not included in any calculation, these have to be addressed by improved organizational safety culture. Systematic capability requirements are intended to ensure improvements in, for example, process, training, documentation, review process and testing procedures.

Basics for SIF Verification

The completion of the risk analysis phase allows for defining SIF/SIS features and requirements. From hazard identification to quantification of the RRF, systematic and random features can be established in the SRS document:

Table 06 lists the information that is generated during the risk analysis phase development and should be included in the SRS.

Table 06: SRS Requirements

#	Information
1	Definition of the Safe State of the process
2	Description of all SIFs
4	Assumed sources of demand and demand rate
5	Response time requirements for the SIF to bring the process to a safe state
6	SIL and mode of operation (continuous or demand)
7	Description of SIF measurements, trip points and output actions
8	Functional logic, math functions and any required permissive
9	Requirements for manual shutdown
10	Requirements relating to energize or de-energize to trip
11	Requirements for resetting the SIS after a shutdown
12	Description of modes of the plant and each SIF required to operate within each mode
13	Requirements for overrides / inhibits / bypasses including how they will be cleared
14	All environmental conditions that are likely to be encountered by the SIS
15	Definition of the requirements for any SIF to survive a major accident event

However, additional parameters that are developed after the completion of the risk analysis phase (see **Table 07**) must to be included in the SRS. Most of the listed requirements are a function of the selected equipment/elements within the SIS (e.g., failure rate) or end-user practices (e.g., proof test interval) play a key role when performing the mathematical calculations for the SIF PFD$_{avg}$ verification. **Table 07** lists the key parameters that can be classified into two main categories and require different sources of information. First, it is critical to identify the failure rate data of each component of the SIS. Second, it is important to establish test and maintenance data.

- Failure Rate data, which is the length of time a device is expected to last in operation before the failure occurs. This type of data is called Reliability Data, which are predictions of failure rates and may be classified as:
    - Generic data: Generic data that has been collected by an organization and published in a handbook or as a computerized database. Generic failure rate sources can be found in reference **[15]**.
    - Manufacturer provided data: Reliability data for a specific product prepared by the manufacturer of the product or by a consultant and can be based on testing, comparison with similar products and/or field experience.
    - User-provided data: Reliability data based on recorded failures at a specific site or in a specific application. This data may be based on data from maintenance databases, or shutdown reports.
    - Expert judgment: This option should be used for new technology where experience data is not available.
- Test and maintenance data, which is used with the intention to characterize intervals, durations and other features of tests and inspections, to be performed in the device during the SLC.

Note that once the proof test interval parameter is introduced, the formal definition of “low demand mode” can be stated: the frequency of demands must be no greater than twice the proof test frequency.

Table 07: Key Parameters to be Considered During SIF Verification

#	Parameter	Symbol	Definition
1	Failure Rate	λ	Frequency of the occurrence of failures. Failures can be classified based on consequence (i.e., Dangerous or Safe) and detectability (i.e., Detected or Undetected).
2	Mission Time	MT	Maximum period of time for which a system is intended to be used. After this period of time, the system must be replaced.
3	Proof Test Interval	TI	Time interval between two proof tests, i.e., periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an “as new” condition or as close as practical to this condition.
4	Proof Test Coverage	C_{PT}	Indicates the effectiveness of a proof test. A 100% proof test coverage would mean that 100% of all dangerous failures would be detected in the test.
5	Proof Test Duration	PTD	Duration of the proof test while the safety function is put into bypass.
6	Mean Time to Restore	$MTTR$	Expected time required to detect that a failure has occurred as well as the time required to make a repair once the failure has been detected and identified, i.e., average value which includes diagnostic detection time and actual repair time.
7	Common Cause Failure	CCF	Condition that affects the operation of multiple devices that would otherwise be considered independent, i.e., redundant devices.
8	System Capability	SC	Measure of the effectiveness of quality management techniques applied to components, i.e., Operational-Maintenance Capability.

The SIL of an entire SIF must be verified by the estimation of PFD_{avg} considering the specific failure rates of all products included in the SIF, proof test intervals, proof test effectiveness, automatic diagnostics, average restore time and redundant architectures, where each element must be checked to ensure compliance with minimum HFT requirements. In other words, the SIF verification requires addressing parameters that have been estimated during the risk analysis phase and additional parameters are defined after selecting the technology and establishing the testing and maintenance strategy:

a. Parameters estimated during the risk analysis phase up to technology selection:

- The RRF of hazardous scenarios identified with an intolerable risk level and accordingly, it is necessary to define the required SIFs.
- Linking the concept of RRF with functional safety principles allows calculating the SIL of the SIF via estimation of the required PFD_{avg}.
- After selecting the components to be part of the SIS structure and acquiring the associated failure rates, the SFF can be estimated. For components following route 1_H, the relationship between SFF and SIL allows estimating the HFT as a function of component type. For components following route 2_H, the HFT is only a function of the SIL.

b. Parameters to be defined after technology selection, which are intended to establish criteria for testing and inspections to be conducted in all devices selected over the mission time of the SIF.

While RRF, SIL, SFF and HFT concepts have been already addressed in the present paper, the following key concepts are introduced for ensuring that all variables for SIF verification have been characterized.

- Failure Rate data
- Test and Maintenance data

Failure Rate Data

Failure Rate Definition

Failure Rate: number of failures per unit operating hours, which is normally represented by the symbol Lambda, $\boldsymbol{\lambda}$, (see **Equation 04**).

$$\lambda = \frac{Number\ of\ failures}{Time\ period\ of\ interest} \qquad \textbf{Equation 04}$$

Note that many components have been shown to follow the so-called “Bathtub” curve model, which identifies three separate regions over the mission time of the device:

- Increased failure rate at the start of the device life which quickly decreases
- Failure rate reaches a minimum constant value over a long period of time
- Increase in the failure rate observed, usually due to wear-out

The “bathtub curve” behavior allows considering a conservative average and constant failure rates during the “useful life” in order to simplify calculations. The “useful life” refers to the portion of the component life that confirms almost constant failure rates by extracting the initial operation and component wear-out. Based on this assumption, the concept of Mean Time to Failure (MTTF) can be defined as illustrated by **Equation 05**:

$$MTTF = \frac{1}{\lambda} \qquad \textbf{Equation 05}$$

Failure Rate Classification

In the section “*Safety Culture” Requirements - SIF/SIS Systematic Capability*” of the present manuscript, differentiation between Random Hardware Failures and Systematic Failures is made. Additionally, this section is focused on addressing hardware failures, which can be classified based on two different criteria:

- Consequence criteria (i.e., dangerous or safe)
  - **Dangerous (D) failure**: Failure that brings the item into a state where it is not able to perform its SIFs. When the item is in such a state, it is said to have a dangerous (D) fault. If a demand should occur when the item has D fault, the item is not able to respond to the demand (i.e., PFD_{avg}).
  - **Safe (S) failure:** Failure that does not leave the item in a state where it is not able to perform its SIFs. A safe failure is often a spurious operation of the safety function that brings the process into a safe state (i.e., STR).

*****Note that also other failure modes can be defined, i.e., No Effects, Annunciation.

- Detectability criteria (i.e., detected or undetected)
  - **Detected (D) failure**: A fault that is detected by automatic diagnostic testing, internal in the item, or connected to a logic solver.
  - **Undetected (U) failure:** A fault that is not detected (not diagnosed) by automatic diagnostic testing, internal in the item, or connected to a logic solver. Undetected faults are usually revealed in proof tests or if a demand should occur.

Therefore, the following categories of failures can be distinguished (see **Table 08**):

- **Dangerous Undetected (DU)**: Prevents activation on demand and are revealed only by proof-testing or when a demand occurs. It is of vital importance when calculating the SIF reliability as they are a main contributor to SIF unavailability. For this reason, the proposed approach for PFD$_{avg}$ calculations is focused on this type of failures.
- **Dangerous Detected (DD)**: Detected in a short time after they occur by automatic diagnostic testing.
- **Safe Undetected (SU):** non-dangerous failures that are not detected by automatic self-testing.
- **Safe Detected (SD)**: Non-dangerous failures that are detected by automatic self-testing. In some configurations, early detection of failures may prevent an actual spurious trip of the system.

Table 08: Classification of Failure Rates and Associated Symbols

Failure Rates	Dangerous	Safe
Undetected	$\boldsymbol{\lambda_{DU}}$	$\boldsymbol{\lambda_{SU}}$
Detected	$\boldsymbol{\lambda_{DD}}$	$\boldsymbol{\lambda_{SD}}$
ALL	$\boldsymbol{\lambda_{D}}$	$\boldsymbol{\lambda_{S}}$

After classifying the failure rates as illustrated in **Table 08**, these terms can be incorporated into the concept of SFF that was introduced in **Equation 03** and is the ratio between the fraction of DU failures among ALL failures of the item (see **Equation 06**).

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D} = \frac{\lambda_{SU} + \lambda_{SD} + \lambda_{DD}}{\lambda_{SU} + \lambda_{SD} + \lambda_{DU} + \lambda_{DD}} = 1 - \frac{\lambda_{DU}}{\lambda_T}$$

Equation 06

$$\lambda_T = \lambda_D + \lambda_S$$

Linking Failure Rate and Probability of Failure

The main purpose of SIF verification is to calculate the probabilities of failure. Thus, it is necessary to transform data from failure rate to probability of failure (on demand), i.e., PFD. Assuming the failure rate is constant, the failure probability of a component can be determined by applying **Equation 07**, which defines the so-called unreliability function, i.e., $\boldsymbol{F(t)}$:

$$F(t) = PFD = 1 - e^{-\lambda_D t}$$

Equation 07

From **Equation 07**, an additional assumption may be to consider low values of failure probabilities. The exponential portion of the expression can be expressed in the form of a Taylor series. Therefore, if the failure probability is low enough, the assumption of taking only the first order of the Taylor series gives the following simplified expression for the probability function (see **Equation 08**):

$$F(t) = PFD = \lambda_D t$$ **Equation 08**

At this point, the probability of failure has been defined as a linear function of the time period of interest. This time period is the remaining key parameter to be defined, as it accounts for a repairable or unrepairable system. In other words, if a system is not repairable and the failure rate and mission time are given, the probability of failure is directly calculated by multiplying both parameters. However, for repairable systems, the test and maintenance related data should be accounted for and the time period is redefined accordingly.

Note that key Test and Maintenance data or parameters were already introduced in **Table 07** (from item 2 to item 7)**.** Based on this information and assuming all key failure rate characteristics, the following section addresses the test and maintenance data for repairable systems. Thus, it is focused on identifying the measure capable of providing the probability associated to the successful situation where a repair can be done.

Test and Maintenance Data

According to **Equation 08**, the time period of interest is a key parameter to be defined. Assuming the system is not repaired during the specific Mission Time (MT), the probability of failure is expressed as follows (see **Equation 09**):

$$PFD = \lambda_{DU} \cdot MT$$ **Equation 09**

*****Note that the MT is an attribute of end-user practices.

However, if over the mission time of the device performance a proof test interval (assigned by end-user practices) is considered and applied, the time period of interest is modified accordingly.

Periodic Perfect Proof-Testing

A periodic proof test and associated repair actions may be considered perfect under the following conditions: (1) the periodic proof test is carried out under conditions that are identical to all relevant demand conditions, (2) all DU faults and all element faults that increase the likelihood of a DU fault are revealed by the periodic proof test and (3) all channels with a revealed DU fault are repaired and all channels are always restarted in an as-good-as-new condition.

Assuming a perfect periodic proof test and repair (i.e., everything in the system is detected, repaired and time to perform these actions is negligible), the time of interest can be considered equivalent to the periodic proof test interval (TI) and the probability of failure can be estimated by using **Equation 10**:

$$PFD = \lambda_{DU} \cdot TI$$ **Equation 10**

However, the PFD is a time-dependent parameter (it is assumed to vary linearly over the proof test interval) and it is expected to have a lower PFD value if the demand occurs just after the proof test execution instead of occurring just before the next proof test interval.

To obtain the simplest possible statement in respect of the reliability of a SIF and to simplify the associated calculations, the mentioned time dependency is eliminated by the generation of mean values and the definition of the pursued PFD$_{avg}$ value can be accomplished. Therefore, if the events that cause a demand are independent from failures in the SIF equipment, an average value is appropriate and can be calculated using **Equation 11**:

$$PFD_{avg} = \frac{1}{t}\int_0^t F(t) \cdot dt$$ **Equation 11**

where t is the time period of interest

Note that for a perfect proof test, **Equation 11** can be written as follows (**Equation 12**):

$$PFD_{avg}{}^{(IND)} = \lambda_{DU} \cdot \frac{TI}{2}$$ **Equation 12**

Note that the superscript *(IND)* has been introduced in **Equation 12** to emphasize that a single item is currently analyzed. This nomenclature is useful when introducing the basis for redundant devices. Considering a perfect proof test is an idealization and for more accurate calculations, the effectiveness of the proof test should be addressed.

Periodic Imperfect Proof-Testing

A proof test is said to be perfect and have 100% coverage if it is able to reveal all the DU faults. In reality, many proof tests cannot cover all possible DU faults and are not perfect. The quantification of this imperfection is conducted by defining the effectiveness of the proof test, which inherently requires the introduction of the effectiveness coverage concept (see **Equation 13)**:

$$C_{PT} = \frac{\lambda_{DU}{}^{(R)}}{\lambda_{DU}{}^{(R)} + \lambda_{DU}{}^{(NR)}} = \frac{\lambda_{DU}{}^{(R)}}{\lambda_{DU}}$$ **Equation 13**

Equation 13 divides the DU faults into two types: (a) DU faults that can be revealed by the proof test (*R-faults*) and (b) DU faults that cannot be revealed by the proof test (*NR-faults*). Accordingly, the Proof Test Coverage, C_{PT} , is defined as the fraction of all DU faults that are revealed by a periodic proof test.

Once an imperfect periodic test has been completed with a given effectiveness coverage C_{PT}, the remaining PFD of the SIF is greater than zero (note that for a perfect periodic test, the PFD was considered zero after each test performed) and it increases after each test performed over the mission time of the SIF. **Equation 14** provides a simplified PFD_{avg} expression when accounting for the effectiveness coverage:

$$PFD_{avg}{}^{(IND)} = C_{PT} \cdot \lambda_{DU} \cdot \frac{TI}{2} + (1 - C_{PT}) \cdot \frac{MT}{2} \qquad \textbf{Equation 14}$$

Periodic proof test can be performed online (while the process is operating and performing its intended functions), or offline (while the process is not operating). Therefore, if a periodic test is performed offline, the duration and time to repair the identified faults are not relevant due to the absence of demands as the process is not running. However, if a periodic test is performed online, other sources of imperfection when conducting periodic proof tests is: (1) duration (when the SIF is put into bypass, the PFD is equal to 1) and (2) the required time to restore the system when a failure is found and must be repaired. For this reason, when conducting proof testing online, the Proof Test Duration (PTD) and the Mean Time to Restore ($MTTR$) are two parameters that need to be defined and considered when evaluating the PFD_{avg} of the SIF (see **Table 07** for a detailed definition of these two parameters). **Equation 15** provides a simplified PFD_{avg} expression considering the duration of the proof test while the SIF is in bypass and the time required to restore the SIF in case a fault is found during the test:

$$PFD_{avg}{}^{(IND)} = C_{PT} \cdot \lambda_{DU} \cdot \frac{TI}{2} + (1 - C_{PT}) \cdot \frac{MT}{2} + \frac{PTD}{TI} + \lambda_{DU} \cdot MTTR \qquad \textbf{Equation 15}$$

Additionally, periodic proof tests can be classified as follows:

- Automatic: the test is initiated and executed without human involvement
- Semi-automatic: human intervention is required for initiating or executing the test
- Manual: all test tasks require human intervention

Based on this categorization, it becomes evident that automatic tests have potential for detecting failures which can improve safety, reduce false trips and provide diagnosis. The diagnostic capability is normally characterized by defining a Diagnostic Coverage factor (DC), which is the conditional probability that a failure will be detected if a failure occurs. Normally, the DC is correlated to dangerous faults and is expressed as DC_D and can be expressed as the mean fraction of all detected faults of an item that are detected by diagnostic self-testing (see **Equation 16**):

$$DC_D = \frac{\lambda_{DD}}{\lambda_D} = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}}$$ **Equation 16**

*****Note that the mean fraction of dangerous faults not revealed by the diagnostic testing is expressed as $(1 - DC_D)$.

Based on **Equation 15**, a simplified PFD_{avg} expression accounting for the diagnostic coverage factor can be derived (see **Equation 17**):

$${PFD_{avg}}^{(IND)} = C_{PT}\lambda_{DU}\frac{TI}{2} + (1 - C_{PT})\lambda_{DU}\frac{MT}{2} + \frac{PTD}{TI} + \lambda_{DU}MTTR + \lambda_{DD}MTTR_{DD}$$ **Equation 17**

where $MTTR_{DD}$ is the mean time to restore a DD failure detected by automatic diagnostics

Equation 17 completes the analysis of how to quantify the PFD_{avg} of a single device of the SIF with imperfect proof-testing and with automatic diagnostics. The portion of the equation that accounts for automatic diagnostics can be removed if diagnostics are not applicable. Hereafter, the following contents of this manuscript are intended to provide guidance on quantifying the PFD_{avg} of the whole SIF by taking into consideration all the SIF architecture characteristics, including redundant items.

The redundant devices require the definition of an additional parameter for quantifying the $\boldsymbol{PFD_{avg}}$. Based on this parameter being applicable for all SIFs with redundancy, this topic is covered in the next section prior to introducing the knowledge for characterizing the whole SIF. This parameter is called Common Cause Failure (CCF) and it is a condition that affects the operation of multiple devices that would otherwise be considered independent.

Redundant Devices – Common Cause Failures

A Common Cause Failure (CCF) is defined as a failure resulting from a shared cause in which two or more separate channels in a multiple channel system simultaneously fail, leading to system fault. It is important to mention that standard IEC 61508 **[2]** points at the need to control $CCFs$ in order to maintain the safety integrity of SIFs. Reference **[2]** suggests calculating the reliability of a SIF and the *beta-factor* is one of the models used for of $CCFs$ characterization.

Beta-Factor Model

The beta-factor model splits the failure rate of an item in two parts, one part covering the individual failures of the channel ($\lambda^{(IND)}$) and another part covering $CCFs$ ($\lambda^{(CCF)}$). It defines the beta-factor β according to **Equation 18**:

$$\beta = \frac{\lambda^{(CCF)}}{\lambda} = \frac{\lambda^{(CCF)}}{\lambda^{(IND)} + \lambda^{(CCF)}}$$

$$\lambda^{(CCF)} = \beta\lambda$$ **Equation 18**

$$\lambda^{(IND)} = (1 - \beta) \cdot \lambda$$

Note that the beta-factor can be different for the various categories of channel failures. Assuming that β denotes the CCF rate for DU failures and β_D for DD failures, the overall rate of dangerous CCFs is defined by **Equation 19**:

$$\lambda^{(CCF)} = \beta\lambda_{DU} + \beta_D\lambda_{DD}$$ **Equation 19**

Therefore, with the aim to account for CCF, an estimation of the β factor is required. However, the β factor is strongly influenced by local, plant-specific conditions and it is not easy to accurately estimate the β factor by using generic data sources. In this sense, guidance can be found in IEC 61508-6 **[2]**, where a checklist is available for β factor estimation (see **Table 09** for generic guidance for β factor estimation).

Table 09: Generic Guidance for Beta-Factor Estimation

Source	β Factor [%]
NASA Space Shuttle Study	11
IEC 61508, Part 6 Annex D.6 (Programmable Electronic Equipment)	$0.5 \leq \beta > 5$
IEC 61508, Part 6 Annex D.6 (Field Equipment)	$1 \leq \beta > 10$
Generic Recommended Value when missing information	10

The PFD_{avg} of a series structure of independent items is approximately equal to the sum of the PFD_{avg} of the item of the series structure. Therefore, the PFD_{avg} of a voted group modeled with the beta-factor model can be calculated by using **Equation 20**:

$$PFD_{avg} = PFD_{avg}{}^{(IND)} + PFD_{avg}{}^{(CCF)}$$ **Equation 20**

$\boldsymbol{PFD_{avg}{}^{(IND)}}$: PFD_{avg} of the voted group of independent channels, each with failure rate defined per **Equation 21**:

$$\lambda_{DU}{}^{(IND)} = (1 - \beta) \cdot \lambda_{DU}$$ **Equation 21**

$\boldsymbol{PFD_{avg}{}^{(CCF)}}$: PFD_{avg} of the virtual CCF element with failure rate defined per **Equation 22**:

$$\lambda_{DU}{}^{(CCF)} = \beta \cdot \lambda_{DU}$$ **Equation 22**

Note that $PFD_{avg}{}^{(CCF)}$ of the CCF element does not change when the architecture is changed and the β-factor model will therefore always be calculated by using **Equation 23**:

$$PFD_{avg} = PFD_{avg}{}^{(IND)} + \beta \cdot \lambda_{DU}\frac{TI}{2}$$ **Equation 23**

Tools for SIF Reliability Quantification and Verification

Criteria established in this section assume that the SIF is independent of the process control system and is a separate and dormant protection layer that is only activated when a hazardous event in the process occurs (demand).

Three subsystems may be considered for a safety loop performing a SIF (1) sensor, (2) logic solver and (3) final element. The three subsystems are configured as a series system, as illustrated in **Figure 03**. Because all three subsystems must function for the SIF to function on demand, the SIF fails on demand if any of the subsystems fail. Therefore, assuming $\mathrm{PFD_{avg}}^{(\mathrm{S})}$ denotes the $\mathrm{PFD_{avg}}$ of the sensor subsystem, $\mathrm{PFD_{avg}}^{(\mathrm{LS})}$ the $\mathrm{PFD_{avg}}$ of the logic solver subsystem and $\mathrm{PFD_{avg}}^{(\mathrm{FE})}$ the $\mathrm{PFD_{avg}}$ of the final element subsystem, the average probability that the SIF fails on demand $\mathrm{PFD_{avg}}^{(\mathrm{SIF})}$ is calculated by the addition rule (see **Equation 24**):

$$PFD_{avg}{}^{(SIF)} = PFD_{avg}{}^{(S)} + PFD_{avg}{}^{(LS)} + PFD_{avg}{}^{(FE)} - a - b - c + d$$

$$a = PFD_{avg}{}^{(S)} \cdot PFD_{avg}{}^{(LS)}$$

$$b = PFD_{avg}{}^{(S)} \cdot PFD_{avg}{}^{(FE)}$$ **Equation 24**

$$c = PFD_{avg}{}^{(LS)} \cdot PFD_{avg}{}^{(FE)}$$

$$d = PFD_{avg}{}^{(S)} \cdot PFD_{avg}{}^{(LS)} \cdot PFD_{avg}{}^{(FE)}$$

However, when the three subsystems are independent and have high reliability, the probability that two or three subsystems fail at the same time is negligible (i.e., a, b, c and d are negligible terms in **Equation 24**) and the $PFD_{avg}{}^{(SIF)}$ can therefore be determined by adding the $\mathrm{PFD_{avg}}$'s for the three subsystems:

$$PFD_{avg}{}^{(SIF)} = PFD_{avg}{}^{(S)} + PFD_{avg}{}^{(LS)} + PFD_{avg}{}^{(FE)}$$ **Equation 25**

Therefore, the $PFD_{avg}{}^{(SIF)}$ is fully characterized after individually quantifying each of the mentioned subsystems. Note that each subsystem may be:

- a single channel (a 1oo1 voted group)
- a group of n identical channels voted *koon* (a *koon* voted group)
- two or more voted groups with different voted configurations

The SIF verification procedure consists of ensuring that the target $PFD_{avg}{}^{(SIF)}$ (based on the RRF calculated during the risk analysis phase) is satisfied with the selected items within each subsystem of the SIF. Therefore, after selecting the technology and proposing a specific SIF architecture, calculations for estimating $PFD_{avg}^{(SIF)}$ are conducted. Hereafter, the reliability, architecture requirements and system capability are verified if the actual SIF configuration complies with all SIF functional safety requirements. This is normally performed by an iterative approach, which is considered finished when the pursued compliance is met.

The verification of SIFs may be complex and are engineering tools or techniques that help perform these types of calculations by graphically defining the configuration and interconnection of the systems that model the SIF. Fault Trees (FTs), Reliability Block Diagrams (RBDs), Markov and Petri Net approaches are examples of these techniques.

FTs and RBDs are methods of graphically showing probability combinations. The primary difference is that the RBD is focused on system success and the FT is focused on a failure event. A FT AND gate is equivalent to parallel systems in a RBD and a FT OR gate is equivalent to systems in series in a RBD. Note that the FT drawings clearly show the specific failure mode under consideration; therefore, it is preferred to use FTs over RBDs when doing safety instrumented function verification calculations. **Figure 04** illustrates a FT for a 1oo2 channel with diagnostics. Note that the FT has been developed by using the software ioLogic™ **[16]**.

Detailed information of these mentioned techniques is out of the present manuscript scope. Further information can be found in references **[8]**, **[15]** and **[17]**.

The verification of a complex SIF requires the use of one of the mentioned techniques for minimizing calculation errors and set up time. ioMosaic has developed ioLogic™ for FT analysis. **[16]**. ioLogic™ is a component of the ioMosaic's Process Safety Office™ (PSO). **Table 10** lists the main characteristics of ioLogic™.

Table 10: ioLogic™ Main Features

#	Feature
1	Easy to create and edit FTs for any purpose as it offers a *What-You-See-Is-What-You-Get* (WYSIWYG) graphical user interface that instantly generates compact, pleasing new layouts whenever a user edits the tree.
2	Highly intuitive graphical interface enables new users to begin drawing FTs within minutes. Commands for pruning, cloning and grafting simplify the creation and editing of individual symbols or entire branches.
3	Handles all the labor-intensive drafting of the tree, allowing users to concentrate on critical logic issues. A full range of options makes it simple to customize the appearance and arrangement of FTs.
4	Predefined FT structures for many different voting groups
5	Capability to quantitatively compute the FTs, including the identification and calculation of minimal cut sets and minimal path sets valuable for sensitivity analysis.
6	Built-in failure data bases

With the aim to illustrate how complex a SIF verification may be due to all interconnections of its subsystems and associated groups and channels, **Figures 04-05** illustrate a generic FT which shows all logical relationships of a 1oo2D voting group. Note that only the $\mathrm{PFD}_{\mathrm{avg}}$ (TOP) 1oo2D voting group is analyzed in the illustrated FT. Based on the specific features of additional groups, channels and subsystems that constitute the SIF, the complete SIF verification may entail further FTs development for finally ensuring that the $\mathrm{PFD}_{\mathrm{avg}}$ of each subsystem is analyzed and sum these $\mathrm{PFD}_{\mathrm{avg}}$ (i.e., sensor, logic solver and final element subsystems) to obtain the $\mathrm{PFD}_{\mathrm{avg}}$ of the whole SIF under analysis.

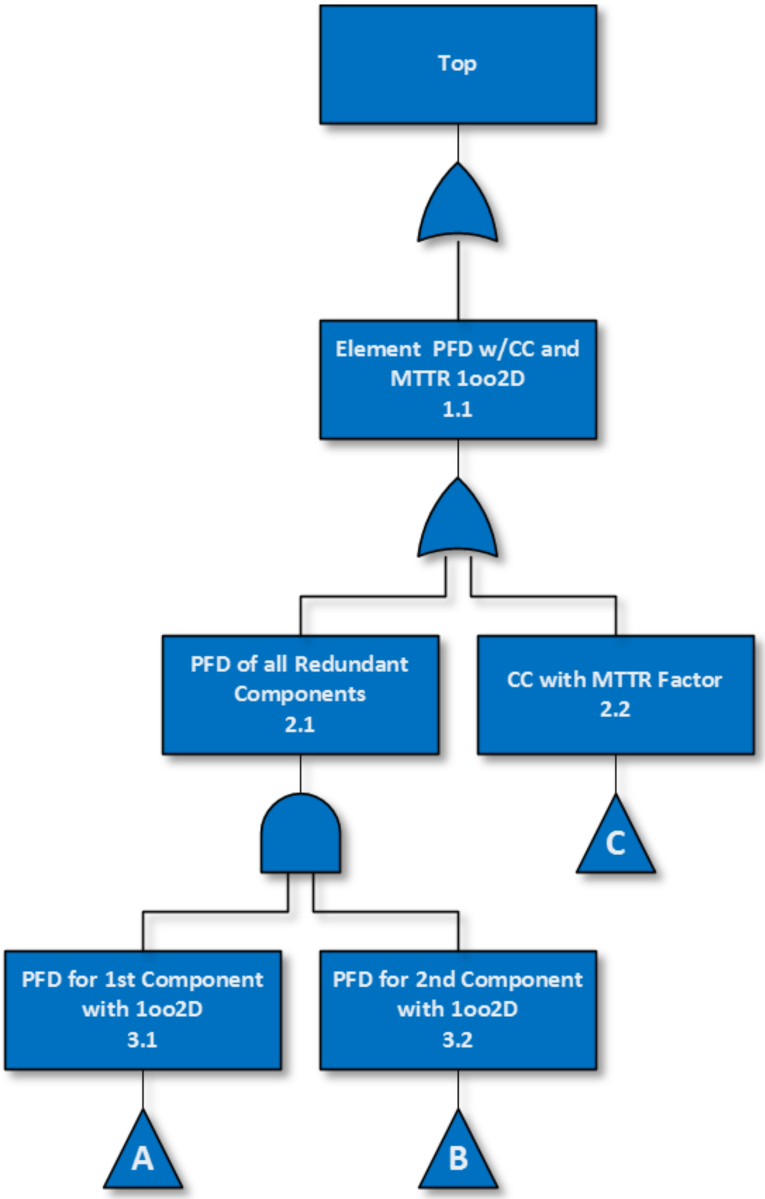
Top
Element PFD w/CC and MTTR 1oo2D 1.1
PFD of all Redundant Components 2.1
CC with MTTR Factor 2.2
C
PFD for 1st Component with 1oo2D 3.1
PFD for 2nd Component with 1oo2D 3.2
A
B

Figure 04: Fault Tree a 1oo2D Voted Group Using ioLogic™ – Part I (Main)

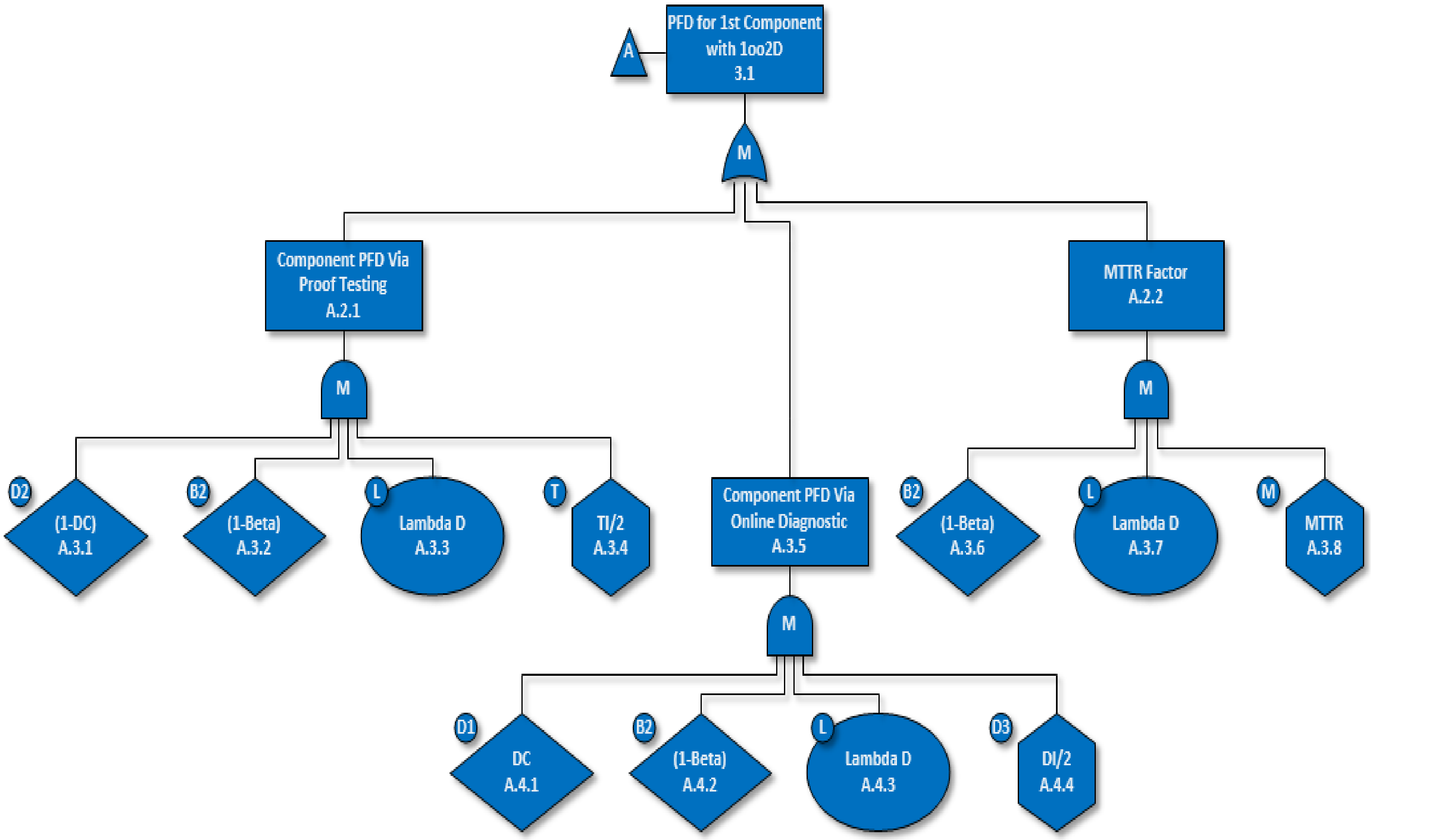

Figure 05a: Fault Tree a 1oo2D Voted Group Using ioLogic™ – Part II (PFD$_{avg}$ A Individual)

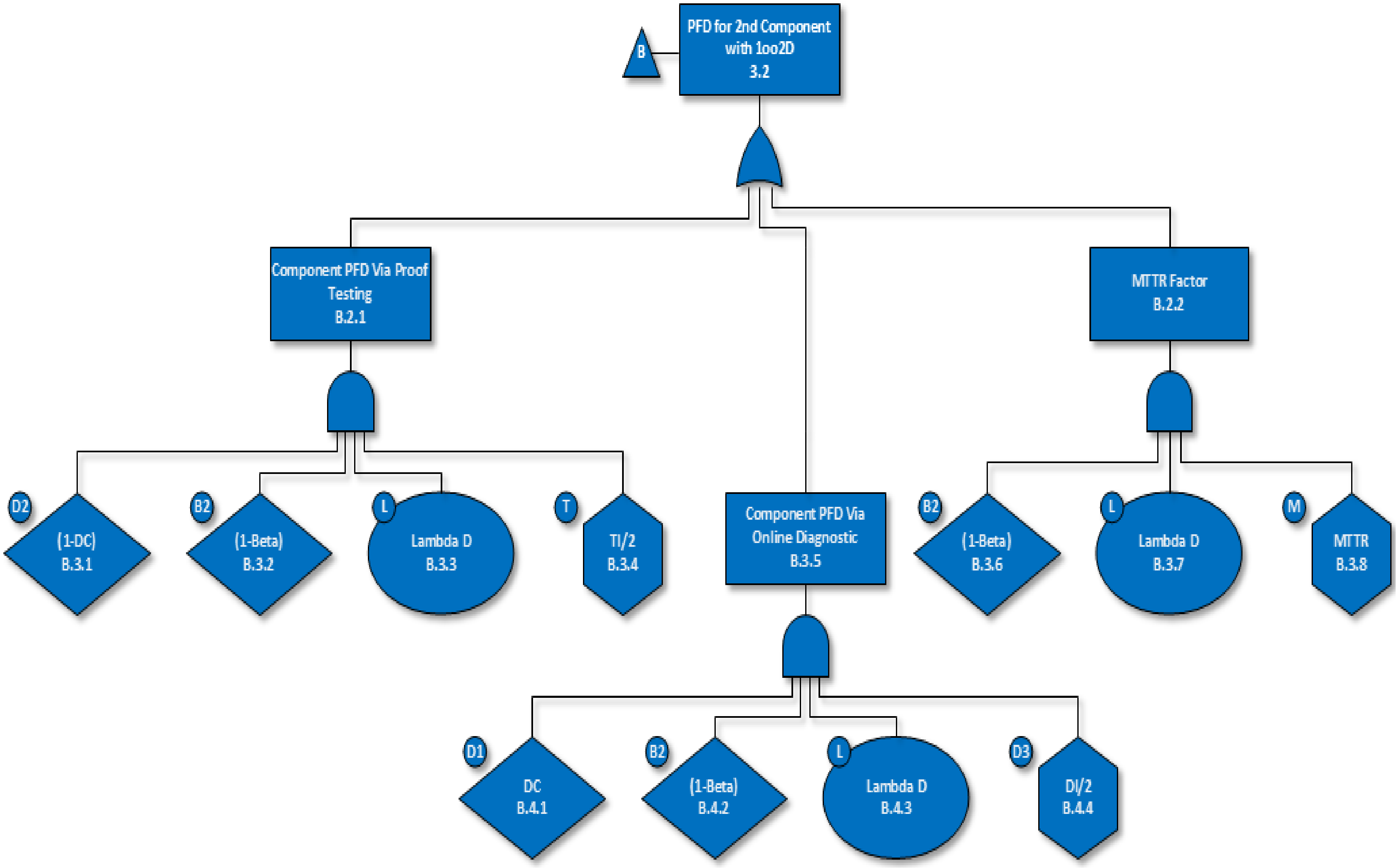

Figure 05b: Fault Tree a 1oo2D Voted Group Using ioLogic™ – Part III (PFD$_{avg}$ B Individual)

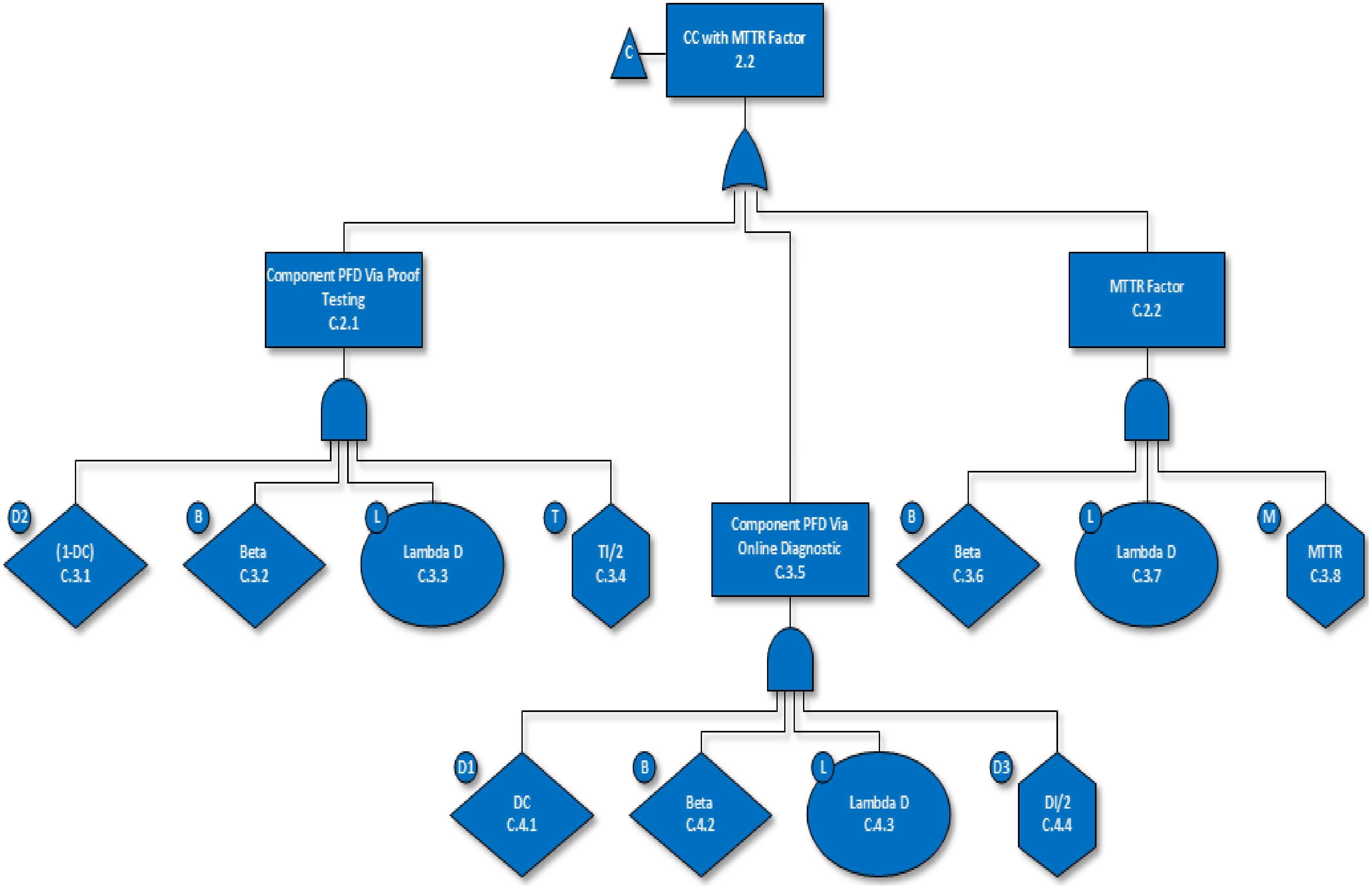

Figure 05c: Fault Tree a 1oo2D Voted Group Using ioLogic™ – Part IV (PFD$_{avg}$ C - Common Cause)

Conclusions

Once the risk-based quantitative assessment has been completed and the actual risk results have been compared with the applicable risk tolerability criteria, it is time to question if risk reduction is necessary, i.e., if there exists a gap between the actual and tolerable risk levels, which is directly correlated to the calculation of the Risk Reduction Factor – RRF. In those cases, the installation of potential risk reduction measures (e.g., Safety Instrumented Systems, SIS) should be analyzed with the aim to reduce the risk of the hazardous scenarios that lead to high risk levels.

The main purpose of the this paper is to address a specific layer of protection that requires detailed knowledge and criteria for a proper definition and installation based on functional safety principles and associated standard requirements. Therefore, providing guidance and criteria on how to link risk analysis and functional safety concepts has been the primary purpose of this paper. Once the reliability of the SIS is defined, basics for verification are established and tools available for complex systems are identified.

References

[1] Dunjó, J., Amorós, M., Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Risk Reduction. Basics of Prevention, Mitigation and Control of Loss of Containment Scenarios." An ioMosaic White Paper, ioMosaic Corporation.

[2] IEC 61508, 2010. "Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems". Parts 1-7- International Electrotechnical Commission (IEC).

[3] IEC 61511, 2016. "Functional Safety - Safety Instrumented Systems for the Process Industry Sector". Parts 1, 2 and 3. International Electrotechnical Commission (IEC).

[4] ISA 84.00.TR.07, 2010. "Guidance on the Evaluation of Fire and Gas System Effectiveness". International Society of Automation (ISA).

[5] Dunjó, J., Amorós, M., Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Mitigating Hazardous Scenarios. An Introduction to Fire and Gas Detectors Mapping Study". An ioMosaic White Paper, ioMosaic Corporation.

[6] Amorós, M., Dunjó, J., Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Quantitative Risk Assessment. Foundation of Process Safety and Loss Prevention". An ioMosaic White Paper, ioMosaic Corporation.

[7] Dunjó, J., Amorós, M., Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Hazard Identification. Guidance for Identifying Loss of Containment Scenarios". An ioMosaic White Paper, ioMosaic Corporation.

[8] Dunjó, J., Amorós, M., Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Frequency Analysis. Estimating Frequencies of Occurrence and Conditional Probabilities of Loss of Containment Scenarios". An ioMosaic White Paper, ioMosaic Corporation.

[9] Dunjó, J., Amorós, M., Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Damage Criteria. An Overview of the State-of-the-Art of Damage Criteria for People and Structures". An ioMosaic White Paper, ioMosaic Corporation.

[10] Dunjó, J., Amorós, M., Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Consequence Analysis. An Introduction to Consequence Modeling and Identification of Loss of Containment Scenarios". An ioMosaic White Paper, ioMosaic Corporation.

[11] Amorós, M., Dunjó, J., Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Risk Evaluation. Tools for Risk Characterization". An ioMosaic White Paper, ioMosaic Corporation.

[12] Dunjó, J., Amorós, M., Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Risk Tolerability Criteria. An Overview of Worldwide Risk Tolerability Criteria for Chemical Process Industries". An ioMosaic White Paper, ioMosaic Corporation.

[13] Dunjó, J., Amorós, M., Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Risk Reduction. Basics of Prevention, Mitigation and Control of Loss of Containment Scenarios". An ioMosaic White Paper, ioMosaic Corporation.

[14] NOG-070, 2004. "Application of IEC 61508 and IEC61511 in the Norwegian Petroleum Industry". The Norwegian Oil and Gas Association. Stavanger, Norway.

[15] Rausand, M., 2014. "Reliability of Safety-Critical Systems – Theory and Applications". Published by John Wiley and Sons, Inc., Hoboken, New Jersey. ISBN: 978-1-118-55340-4.

[16] iOiQ, 2016. "ioLogic^{TM} – A Visual Tool for Fault Tree and SIL/SIS Analysis". ioLogic™ A Process Safety Office™ Component.

[17] Goble, W. M., Cheddie, H., 2005. "Safety Instrumented Systems Verification. Practical Probabilistic Calculations". The Instrumentation, Systems and Automation Society (ISA). ISBN-10: 1-55617-909-X.