MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

20th Annual International Symposium
October 24-26, 2017 • College Station, Texas

# Application of functional safety to electrical power equipment and systems in process industries

Janardhanan Kallambettu P.Eng., Principal Engineer-Control Systems, Bechtel TX, U.S.A
Email: jkallamb@bechtel.com

Venkatesh Viswanathan P.Eng., Senior Electrical Engineer, Bechtel, TX, U.S.A
Email: vviswana@bechtel.com

## Abstract

In process industries, the application of functional safety in preventing major incidents is a well-established practice. The functional safety standard IEC 61511[**1**] is applied to the safety instrumented system (SIS) protection layers to avoid the undesired events or reduce the likelihood of the events or impacts due to failures in the process, process equipment, or its control system including human interactions. However, there are risks of catastrophic incidents due to electrical equipment failures as well. Therefore, one should not underestimate the importance of the management, design, installation, operation, and maintenance of electrical power systems and protection devices. Regulatory authorities, in some countries, require the owners or operators to address the risks that arise from electrical equipment failure.

The risk-based assessment, allocation of safety functions to protection devices, the establishment of integrity requirements, design, installation, operation, and maintenance of electrical protection devices must be managed like the protection layers for the process units. This paper focusses on the application of IEC 61511 to the protection of electrical equipment and systems, available industry guidelines, and the unique challenges in implementing the functional safety standards. The paper guides the electrical engineers with an example risk assessment, identification of protection device and its safety integrity level (SIL), verification of the reliability of the protection device and establishing a maintenance and operation program.

## Introduction

Functional safety is part of the overall safety relating to the process and the control system controlling the process, that depends on the correct functioning of the active protection layers. Safety instrumented systems (SIS) implementing safety instrumented functions (SIF) are active protection layers. The functional safety standard provides guidelines to identify the target performance and manage the protection system for the entire safety life cycle covering specification, design, implementation, installation, commissioning, operation, maintenance, modifications and decommissioning activities associated with the protection system. A well-managed protection system as per IEC 61511 will have the required integrity with adequate defenses against systematic failures. Internationally, the process industries accepted the functional safety standard IEC 61511 and is in use for the past two decades.

The process safety deals with the incidents due to process, process equipment, control system controlling the process, and human interaction failures. The process facility incidents such as fire and explosions are not only due to the process plant failures but also can be due to electrical power distribution systems and equipment failures. Therefore, it is imperative that the risks arising from the reliability, availability, and survivability of the electrical power supply systems and failure of electrical equipment should be systematically addressed.

The Health and Safety Executive (HSE) in the United Kingdom requires the following related to electrical power systems in chemical manufacturing processes [**2**]:

- conduct a formal risk assessment of the fire and explosion risks arising from the electrical power supply and distribution systems;
- establish a management system to design, install, operate and manage the electrical equipment and protection system;

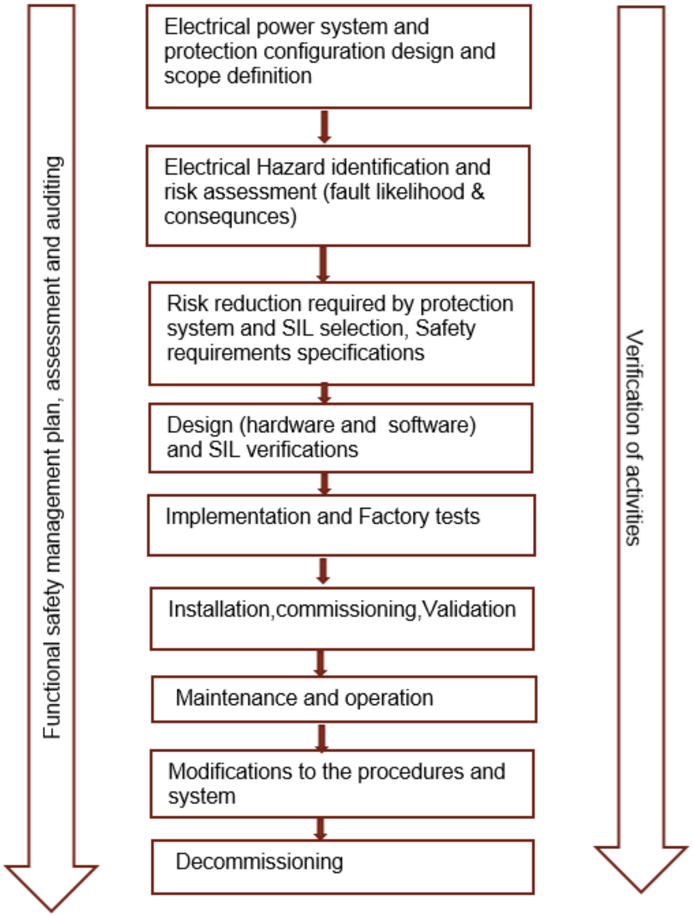
In response to the above requirements, the Energy Institute, London, published a guidance document "*Guidance on Assessing the Safety Integrity of Electrical Supply Protection*" [**3**] to manage the electrical protection systems by applying IEC 61511. In the United States of America, there is no explicit requirements or guidelines in applying the functional safety concepts for the electrical protection systems. However, applying the functional safety life cycle principle provides a practical basis for managing the electrical protection systems.

In this paper, discussed the application of IEC 61511 for the power protection systems, and how it differs from the process plant application. Also, provided example Safety Integrity Level (SIL) selection, SIL verification, and other safety life cycle activities relevant to the electrical protection systems.

## Safety life cycle

The fundamental concept of IEC 61511 is the application of safety life cycle to the protection systems. A simplified safety life cycle model for electrical protection systems is shown **Figure 1**.

**Figure1. Electrical Protection Systems -Safety Life Cycle**


Electrical power system and protection configuration design and scope definition
Electrical Hazard identification and risk assessment (fault likelihood & consequnces)
Risk reduction required by protection system and SIL selection, Safety requirements specifications
Design (hardware and software) and SIL verifications
Implementation and Factory tests
Installation,commissioning,Validation
Maintenance and operation
Modifications to the procedures and system
Decommissioning
Functional safety management plan, assessment and auditing
Verification of activities

In the following sections, each activity is discussed in brief to illustrate the concepts.

## Risk assessment -Electrical H&RA

In process plants, the equipment under control (EUC) is the process units/equipment. The process hazard and risk assessment (Process H&RA) is performed on the process units. Similarly, in electrical supply and distribution systems, the electrical hazard and risk assessment (Electrical H&RA) is carried out on the electrical supply systems and equipment such as generators, transformers, switchgears, MCCs, motors, etc. The risk assessment steps such as identification of hazards and hazardous events, causes or the failures that lead to the hazardous events, estimating the likelihood and the consequence severity of the hazardous events, and determining the required risk reduction by the protection system meeting the risk tolerance criteria are essentially the same. However, there are differences between a process H&RA and an electrical H&RA as summarized in **Table 1**.

**Table 1. Process and Electrical H&RA- a comparison**

| Item | Process H&RA | Electrical H&RA | Similar/Difference |
|---|---|---|---|
| Equipment under control (EUC) | Process and equipment | Electrical supply and distribution equipment | Difference |
| Hazardous events | leading to fire and explosion | leading to fire and explosion | Similar |
| Consequence severity | Serious injury/fatality | Serious injury/fatality | Similar |
| Risk category | Safety, environment, and commercial (asset) | Safety and commercial (asset) | - |
| Risk tolerance criteria | Tolerable hazardous events/year | Tolerable hazardous events/year | Similar |
| Initiating events | Process and control system failures, human failures and mechanical equipment failures | Short circuit, overload, etc. | Difference |
| Documents required for the risk assessment | P&IDs,<br>Cause and Effect Diagrams,<br>Control/ shutdown narratives<br>Alarm and trip setpoints | Design Criteria,<br>Operating Philosophy,<br>Protection and Control Philosophy,<br>Power System Studies (Load Flow, Short Circuit, Harmonic Analysis, Motor Starting Studies) | Difference |
| SIL assessment methodology | Risk graphs,<br>LOPA,<br>Hazard matrices | Risk graphs,<br>LOPA | Similar |
| Team composition for H&RA | Process and control systems engineers | Electrical engineers | Difference |
| Protection layers | Non-instrumented and instrumented | Protection relays (overcurrent, thermal ground fault, etc.),<br>Fuses, and Circuit Breakers | Difference |
| Integrity analysis | Individual independent safety instrumented protection layer is analyzed for meeting target SIL | Overall protection arrangement is analyzed for meeting target SIL | Difference |
| Conditional modifiers | Probability of ignition, probability of personnel presence, and | Probability of ignition, probability of personnel presence, | Similar |

| Item | Process H&RA | Electrical H&RA | Similar/Difference |
|---|---|---|---|
|  | probability of injury or fatality | and probability of injury or fatality |  |

For electrical equipment located in hazardous areas, the consequences of electrical power supply and distribution systems' faults are uncontrolled arcs, short circuits, heating, etc., resulting in a fire or explosion, if flammable gases are present. Any of the above could lead to injuries to the personnel and /or equipment damage in that area. The failures mentioned are typically caused by random failure events, incorrect design, and installation. The intent of this paper is to focus on random failure events described above.

For example, a prolonged *locked rotor* situation due to mechanical jam could result in heating of the motor windings thereby causing the surface temperature of the motor enclosure to rise above its rated value. If this event were to occur in the presence of flammable gases and vapors, it could lead to a fire or an explosion. In this example, the locked rotor is a fault which is the initiating event. The consequence is exceeding the surface temperature and igniting a vapor cloud resulting in injury to personnel.

The likelihood and the consequence severity determines the risk of the scenario. The above-assessed risk should be compared with the established risk tolerance criteria and determine whether any risk reduction is required. The protection arrangement applicable to the scenario should meet the required risk reduction. If a scenario risk meets the tolerable risk criteria and there is no further risk reduction is needed then, the protection arrangement does not have any special requirements as per the functional safety standards. Regardless of risk reduction requirements, the protection arrangements shall comply with the applicable codes, standards, and local regulations.

The following documents are required for the electrical H&RA as a minimum:

- Single line diagram (SLD) showing all the major components;
- Operating and design philosophy document;
- Power system protection philosophy including protection arrangement drawings;
- Power system study report with fault level definitions and any transient analysis performed;
- Failure rate data for various failures associated with the electrical equipment;
- Hazardous area classification lay outs
- Tolerable risk criteria;

The team composition for electrical H&RA should include the following:

- Electrical engineers well conversant with the power system and its protection;
- A facilitator who is familiar with the risk assessment methodology and the electrical equipment and the processes being protected;
- Operations and electrical maintenance representatives;
- Vendor specialists as required;

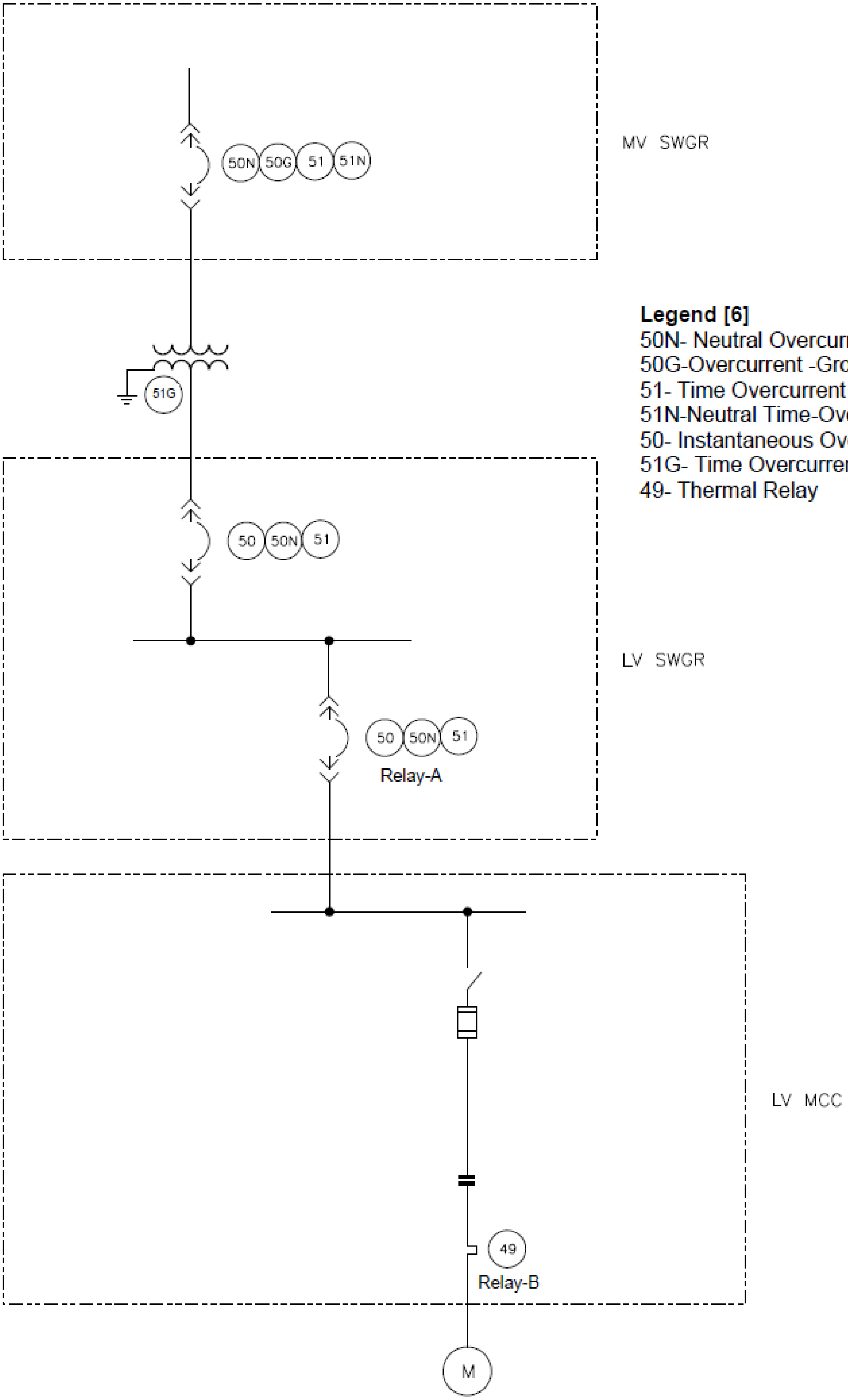
- Scribe to document the H&RA;

The H&RA shall be recorded systematically with complete traceability to the various critical decisions, observations, and assumptions made during the risk analysis.

**SIL selection**

The electrical H&RA provides the likelihood and the consequence severity of a scenario which determines the risk.  The next step is to select safety integrity level (SIL) of the protection arrangement that meets the required risk reduction. A typical protection arrangement for an induction motor located in a hazardous area as shown in **Figure 2** is considered to illustrate the SIL selection process.

**Figure 2. Protection arrangement of typical low voltage induction motor**



**Legend [6]**
50N- Neutral Overcurrent
50G-Overcurrent -Ground
51- Time Overcurrent
51N-Neutral Time-Overcurrent
50- Instantaneous Overcurrent
51G- Time Overcurrent- Ground
49- Thermal Relay

For the scenario described in the “Risk assessment” section above,

| | |
|---|---|
| **Initiating event (IE)** | locked rotor |
| **IE frequency** | 0.01/year [**3**] |
| **Consequence** | causing overcurrent in an induction motor located in a Zone 1 hazardous area resulting in overheat of the windings with external and internal surface temperatures exceeding the specific T ratings of the hazardous area, and causing ignition of a co-incident gas release; |
| **Consequence severity** | injury/fatality to 1 or 2 persons. |
| **Tolerable frequency** | 1.0E-05/year |

Risk graph or Layer Protection Analysis (LOPA) is the commonly used methods to determine the required Risk Reduction Factor (RRF) and SIL. In this paper, LOPA methodology is used to determine the RRF and SIL.

The LOPA equation is,

$$\begin{aligned} &\mathit{Tolerable\ Frequency} \\ &\qquad = IE * (\ \mathit{PFDavg\ of\ the\ protection\ arrangement}) * \mathit{Pgas\ present} * \mathit{Pign} * \mathit{Pocu} * \mathit{Pinj} \end{aligned} \quad (\textbf{EQ-1})$$

Where,

| | |
|---|---|
| IE | Initiating event frequency (per year) |
| $\mathrm{PFD}_{\mathrm{avg}}$ | average probability of failure on demand |
| $\mathit{Pgas\ present}$ | Probability of gas present |
| $\mathit{Pign}$ | Probability of ignition |
| $\mathit{Pign}$ | Probability of occupancy |
| $\mathit{Pinj}$ | Probability of injury/fatality |

The motor is in Zone 1 area; therefore, the probability of gas present is 0.01. Assuming, if the gas is present at the time of the fault then, ignition is certain, and people are present most of the time in the area, and explosion will impact them, then,

$\mathit{Pign}$ = 1
$\mathit{Pocu}$ = 1
$\mathit{Pinj}$ = 1

Applying the above factors, failure rate and tolerable frequency in the equation **EQ-1** above, we have

1.0E-05/year = (0.01/year) * $\mathit{PFDavg\ of\ the\ protection\ arrangement}$ * (0.01) *1*1*1

Therefore, $\mathit{PFDavg\ of\ the\ protection\ arrangement}$ = 0.1, and

$RRF = (1/PFDavg)$, i.e. RRF= 1/ (0.1) = 10.

The above RRF (10) is within the range of SIL 1 per Table 4, IEC 61511-1. Therefore, the protection arrangement must meet the integrity of **SIL 1**.

### *Independent protection layers*

In the protection arrangement shown in **Figure 2**, only the thermal relay B, tripping the motor contactor will be applicable as a protection layer. Neither the fuse nor the upstream overcurrent relay A will prevent the consequence from occurring.

Therefore, *it is important to note that the relevant protection devices for any scenario depend upon the nature of fault (i.e., initiating event). For a short circuit situation, the Fuse (primary protection) and the overcurrent relay A (backup protection) tripping the motor contactor are the appropriate protection devices and not the thermal relay A.*

In electrical systems, in most of the scenarios, the protection layers are not independent. All the protection devices trip the same final actuation device such as a *breaker or a contactor*. For instance, in the locked rotor fault scenario described above, sometimes *stall protection* is provided in addition to *thermal relay*. But both the protection devices trip the same final element, motor contactor. Therefore, the stall protection and thermal protection are not independent and hence they should be combined as a single protection layer and analyzed accordingly.

Also, due to the advancement in the microprocessor based programmable device technology, many protections are implemented in a single device, known as "multi-function relay". For example, electronic overload relays (EOL), depending on manufacturer/ model typically have protective capabilities such as overload, jam protection, current imbalance, phase loss, ground fault, phase reversal etc. In such cases, the independency between the various protection devices is lost and, therefore, common cause failures must be considered in the reliability analysis.

## SIL Verification

After selecting a SIL target for the relevant protection arrangement, the next step is to verify that the protection arrangement will provide the required integrity. IEC 61511 and IEC 61508 require the following as part of the SIL verification:

- Calculated $PFD_{avg}$ of the protection system shall be less than the target $PFD_{avg}$ obtained in the LOPA;
- Hardware fault tolerance (HFT) of the protection arrangement shall meet the requirements of either IEC 61508 Route $1_H$ or $2_H$ or Table 6, IEC 61511-1 for the specified target SIL;

## $PFD_{avg}$ Calculation

Probability of failure on demand of a protection layer depends on various parameters:

- Failure rates of the components performing the protective function;
- Redundant configuration of the devices and their logical voting to trip the breaker or contactor;
- Testing interval and the extent of testing;
- Diagnostics to detect the dangerous failures and the mean time to repair/restore;

### *Failure rates*

The failure of a component can be spurious or dangerous. The spurious failure results in tripping the circuit without a demand. IEC 61511 designate these failures as safe failures. Dangerous failures are those that fail to trip a breaker or a contactor when demand (fault) occurs. In probability of failure on demand calculations, the dangerous failure rates are required.

There is always an uncertainty in the quantification of random failures. The failure rate is, probably, the least precise parameter used in performing SIL verifications [**4**]. Therefore, one must acknowledge that the results of the quantification are not real values, but rather a basis for comparing different design options and for monitoring the reliability performance during the operational phase of the safety lifecycle. The analysis is only a prediction. Historical performance is not the same as future performance.

If the failure rates are conservative, then achieving target SIL will be demanding. However, optimistic failure rates will result in inadequate protection integrity. Therefore, the failure rates of components used in the analysis should be sufficiently realistic.

There are many sources of failure rate data, such as application-specific, site-specific, company-specific, manufacturer-specific, industry-specific, and generic data. These failure rates can vary significantly by several orders of magnitude. While application specific or site specific data is the best option, but it can often be difficult to obtain.

Some of the industry sources for the failure rates are:

- IEEE publication, 493 - "IEEE *Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*" [**5**].
- Energy Institute, London, publication "*Guidance on Assessing the Safety Integrity of Electrical Supply Protection*" [**3**];
- FARADIP.THREE, failure rate database, published by Technis, UK;

Among the above sources, FARADIP.THREE provides spurious (designated as $\boldsymbol{\lambda_S}$) and dangerous failures (designated as $\boldsymbol{\lambda_D}$). In this paper, FARADIP.THREE failure rates are used to demonstrate the SIL verification process.

### *Test intervals*

The protection devices must be tested. Longer the test interval, higher the PFD $_{avg}$ and difficult to meet higher SILs. The testing interval can be extended for low failure rate devices or if there are redundant devices in the protection arrangement. Frequent test interval may not be practical in a continuous process plant without shutting down the process units. Every effort should be made to coincide the testing with the plant turnaround time, typically once in every 5 years.

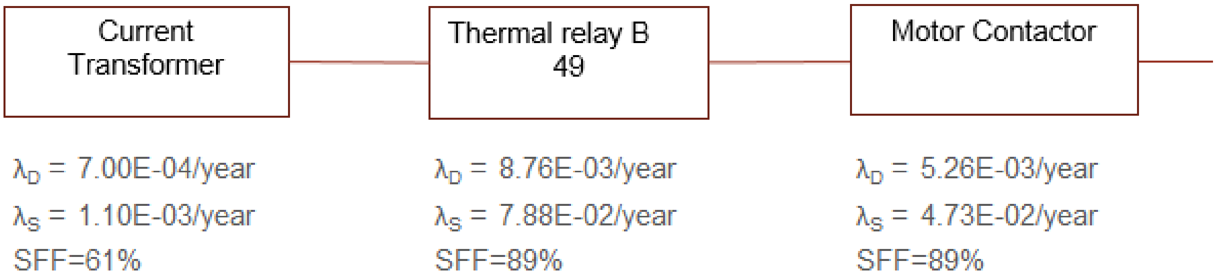
### *Diagnostics*

Microprocessor based relays are currently the industry standard, and these typically have diagnostic capability to monitor relay health. When configured appropriately, some of the dangerous failures are detected, and the protection device can be tested and repaired as required. In such situations, the undetected dangerous failures are reduced, and hence $PFD_{avg}$ is also lowered.

### *Reliability diagram*

Before performing the $PFD_{avg}$ calculation, drawing a reliability diagram depicting the protection arrangement applicable to the scenario will be useful. For the LV induction motor example described above, the reliability diagram for the locked rotor protection is shown in **Figure 3**.

**Figure 3. Reliability diagram for the LV induction motor locked rotor protection**


Current Transformer
Thermal relay B 49
Motor Contactor
$\lambda_D$ = 7.00E-04/year
$\lambda_S$ = 1.10E-03/year
SFF=61%
$\lambda_D$ = 8.76E-03/year
$\lambda_S$ = 7.88E-02/year
SFF=89%
$\lambda_D$ = 5.26E-03/year
$\lambda_S$ = 4.73E-02/year
SFF=89%

The $PFD_{avg}$ of the locked rotor protection arrangement is the sum of the $PFD_{avg}$ of all the components shown in the reliability diagram in series.

i.e. PFD $_{avg}$ (locked rotor protection) = $PFD_{avg}$ (Current Transformer) + $PFD_{avg}$ (Thermal relay B) + $PFD_{avg}$ (motor contactor)

All the above devices are simplex (not redundant) and therefore the following equation is applicable.
$PFD_{avg}$ = $\lambda D * (Test\ Interval)/2$

Considering the test interval as five years and substituting the $\boldsymbol{\lambda_D}$ for each device, we have

$PFD_{avg}$ (locked rotor protection) = [{(7.00E-04) *(5/2)} + {(8.76E-03) *(5/2)} + {(5.26E-03) *(5/2)}]
i.e. $PFD_{avg}$ (locked rotor protection) = 3.68E-02

The above calculated $PFD_{avg}$ (3.68E-02) is lower than the target $PFD_{avg}$ (0.1) and, therefore, the locked rotor protection arrangement comprising of *thermal protection relay tripping the motor contactor* meets the required target SIL 1 integrity.

## <u>Hardware Fault Tolerance (HFT)</u>

Irrespective of the hardware reliability calculated ($PFD_{avg}$) for the design, the functional safety standard IEC 61511 specifies minimum levels of redundancy for each safety integrity level.
There are two approaches:

- Route $1_H$: Determination of HFT based on the calculated safe failure fraction (SFF);
- Route $2_H$: Determination of HFT based on field experience and field data (proven-in-use)

*Route1$_H$*

The Route1$_H$ approach uses SFF and the SIL target to determine the hardware fault tolerance. The SFF is defined as the sum of the potentially dangerous failures revealed by auto-test and those failures which result in a safe state, as a fraction of a total number of failures.

$$\text{SFF}= \frac{[dangerous\ detected\ failures(self\ test)+safe\ failures]}{Total\ failures}$$

The above is calculated for each element or subsystem, i.e., current transformer, thermal relay, and motor contactor). Two tables, Table 2 and Table 3, are provided in IEC 61508- Part 2. Table 2 is for “Type A” devices which are simple devices such as relays (no microprocessors and programming are involved), and Table 3 for “Type B” devices which are complex devices such as multifunction relays. Based on the SFF, device type, and the SIL target, the hardware fault tolerance is determined using **Table 2** and **Table 3**, which are reproduced from IEC 61508 Part 2 for reference.

### Table 2. Maximum allowable integrity level for a safety function carried out by a type A safety related element or subsystem

| **Safe failure fraction (SFF) of an element** | **Hardware fault tolerance (HFT)** | | |
|---|---|---|---|
| | **0** | **1** | **2** |
| **< 60%** | SIL 1 | SIL 2 | SIL 3 |
| **60% - < 90%** | SIL 2 | SIL 3 | SIL 4 |
| **90% - < 99%** | SIL 3 | SIL 4 | SIL 4 |
| **≥ 99%** | SIL 3 | SIL 4 | SIL 4 |

### Table 3. Maximum allowable integrity level for a safety function carried out by a type B safety related element or subsystem

| **Safe failure fraction (SFF) of an element** | **Hardware fault tolerance (HFT)** | | |
|---|---|---|---|
| | **0** | **1** | **2** |
| **< 60%** | Not allowed | SIL 1 | SIL 2 |
| **60% - < 90%** | SIL 1 | SIL 2 | SIL 3 |
| **90% - < 99%** | SIL 2 | SIL 3 | SIL 4 |
| **≥ 99%** | SIL 3 | SIL 4 | SIL 4 |

*Route$2_H$*

In Route $2_H$, the hardware fault tolerance is specified by the functional safety standard for each SIL target if the device is selected based on well documented and verified field based failure rate data with 90% statistical confidence. For low demand application (electrical faults are low demand mode of operation) with SIL 1 or SIL 2 target, there is no need for any redundancies (HFT=0), and SIL 3 requires one redundant element (HFT=1).

Unless the field failure data with 90% confidence levels are available, the Route $2_H$ cannot be justified. Many of the electrical components are reliable and field proven and, therefore, Route $2_H$ can be the best approach if a proper documentation of failure rate data for specific applications is available.

For microprocessor-based protection devices where sophisticated hardware and software are involved, the protection devices must be evaluated by competent organizations such as TUV, SIRA, FM, etc., to ensure compliance with IEC 61508- Part 2 (hardware) and IEC 61508- Part 3 (software). Route $1_H$ will be appropriate for microprocessor -based protection devices.

For electromechanical devices, there should be sufficient operating experience enabling the analyst to use historical failure rate data as part of the reliability analysis and Route $2_H$ for HFT evaluation.

All the elements of a subsystem must meet or exceed the hardware fault tolerance requirements for the specified target SIL. For the locked rotor example described above, the hardware fault tolerance is applied as per Route $1_H$ to illustrate the methodology, and the analysis is tabulated in **Table 4**.

## Table 4. Evaluation of HFT

| **Element or Subsystem** | **Device type per IEC 61508** | **SFF** | **Target SIL** | **Required HFT** | **Achieved HFT** | **Achieved SIL per HFT criteria** |
|---|---|---|---|---|---|---|
| Current Transformer | Type A | 61% | SIL 1 | 0 | 0 | SIL 2 |
| Thermal Relay | Type A | 89% | SIL 1 | 0 | 0 | SIL 2 |
| Motor Contactor | Type A | 89% | SIL 1 | 0 | 0 | SIL 2 |
| **Overall SIL Claimed per HFT** | | | | | | **SIL 2** |

From the above, the safety function provided by the thermal relay tripping the motor contactor meets SIL 1 as per $PFD_{avg}$ calculation and SIL 2 as per HFT criteria. Therefore, *the safety function meets SIL 1 integrity per the functional safety standard*.

### Factory acceptance testing (FAT)

Factory testing of the complete protection system as per the testing procedures should be carried out and the reports should be available. Factory testing should include primary current injection and secondary current injection testing. If primary current injection cannot be adequately achieved at the manufacturer's location then, the protection system manufacturer should provide the site testing methodology including the checking sequences.

### Installation and Commissioning

The protection system must be installed as per the installation drawings, safety manuals, and manufacturer's recommendation. Any deviations must be subject to safety review process before performing any site modifications.  Before energizing the equipment, the following must be carried out as part of the commissioning to ensure the protection function(s) will perform as intended:

- Checking of the protection settings per protection setting study report;
- Additional testing which has not been performed during the FAT;
- Re-checks of primary and secondary current injection testing where major components of the system are reassembled at site;

### Inspection and testing

Operation and maintenance are the longest periods in the safety life cycle. The functional safety standards require continuous performance monitoring, including demand rates, failure modes and failure rates of various components. The actual performance must be compared with the predicted performance to identify any gaps so that remedial measures can be provided with appropriate safety review.

The protective functions must be inspected and tested at the intervals as determined per SIL verification calculations. In the above example, the test interval is five years. The inspection and testing procedures shall comply with the manufacturer's recommendations. If the devices of protective functions are not tested as per the test intervals considered in the SIL verification calculations and as per the manufacturer's recommendations then, the functional safety is not achieved for the specified protective functions. The records of testing shall be maintained. Any performance degradation must be analyzed and if required revise the testing periods to sustain the required SIL.

The failure rates considered in the calculations are applicable only during the useful life of the devices. Therefore, it is important to check the useful life and replace the components as required.

## Auditing and Assessments

The risk assessment, SIL selection and other life cycle activities, work processes and application of procedures must be periodically audited.  Also, auditing shall take place whenever modifications are under taken.

## Management of change (MOC)

In any process facility, making changes to the protective system, equipment and procedures are inevitable.  Modifications are required for a variety of reasons due to evolution of the technology, equipment malfunctions, and obsoleteness.

Many regulations require employers to establish and implement written procedures to manage changes, except 'replacements in kind.'  A robust management of modifications procedures shall be in place to initiate, document, review, implement and approve changes to protective functions other than replacements in kind. A robust change management process will ensure protective function integrity throughout the operation and maintenance phase of the safety life cycle.

## Competency

The personnel undertaking the safety life cycle activities must be competent in performing the activities. The competency must be managed to ensure systematic errors are minimized. Any deficiencies must be analyzed, and appropriate training shall be provided, or other control measures must be in place.

## Conclusion

Electrical power supply and distribution systems generate, store and transmit large amounts of energy and the faults in the system may lead to catastrophic incidents in any process facility, like process and process equipment failures.  A risk based robust management system helps to assess the risk and to specify, design, install, operate, and maintain the electrical protection systems. The principles of performance based functional safety standard IEC 61511 provide a frame work to establish an effective management system.  Electrical protection systems designed, operated and maintained per functional safety standards meet the regulatory requirements and helps to sustain the integrity throughout the life cycle of the electrical supply and distribution systems.

## References

1. IEC. IEC 61511 Functional Safety: Safety Instrumented Systems for the Process Industry Sector- Part 1-3, Edition 2, Geneva, 2016.

2 HSE, UK. SPC/TECH/OSD/31, Safety instrumented systems for the overpressure protection of pipeline risers, Available at http://www.hse.gov.uk/eci/electrical.htm, accessed on July 24, 2017.

3. Energy Institute, UK. Publication "*Guidance on Assessing the Safety Integrity of Electrical Supply Protection*," London, 2006.

4. Dr. D. J. Smith, Reliability, Maintainability and Risk, 8th Edition, Butterworth-Heinemann, Waltham, MA, 2011.

5. IEEE publication, Gold Book, 493 - "IEEE *Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems,*" 3 Park Avenue, New York, NY 10016-5997, USA.

6. IEEE publication, IEEE Std. C37.2-2008 IEEE Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations.