Journal of Loss Prevention in the Process Industries 56 (2018) 155–161

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

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

Janardhanan Kallambettu P.Eng., Principal Engineer-Control Systems,
Venkatesh Viswanathan P.Eng., Senior Electrical Engineer*

Bechtel, TX, USA

A B S T R A C T

In process industries, the application of functional safety in preventing major incidents is a well-established practice. The functional safety standard IEC 61511 (IEC, 2016) 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.

1. 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 (HSE and UK, 2017):

- 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*" (Energy Institute and UK, 2006) 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

* Corresponding author.
E-mail addresses: jkallamb@bechtel.com (J. Kallambettu), vviswana@bechtel.com, venky.viswanathan@worleyparsons.com (V. Viswanathan).

https://doi.org/10.1016/j.jlp.2018.07.009
Received 6 February 2018; Received in revised form 1 July 2018; Accepted 12 July 2018
0950-4230/

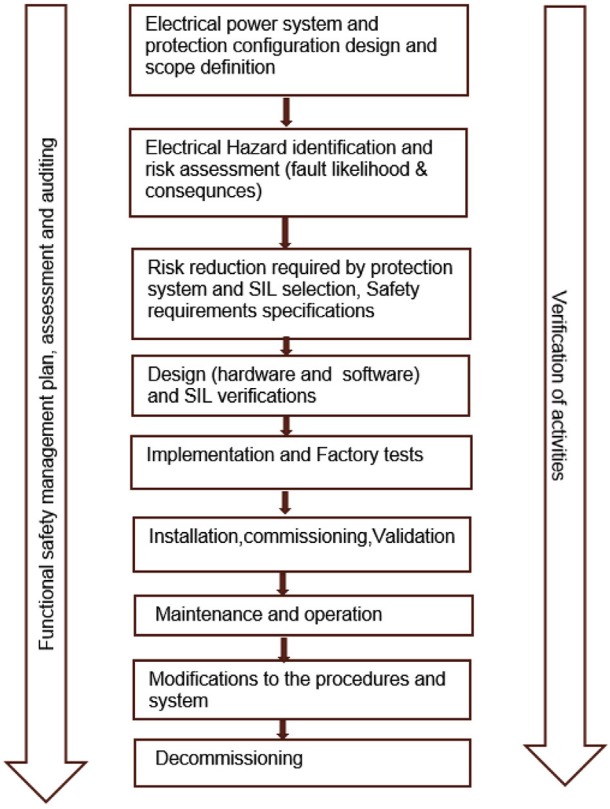

Fig. 1. Electrical protection systems -safety life cycle.

verification, and other safety life cycle activities relevant to the electrical protection systems.

2. 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 Fig. 1.

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

3. 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.

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.

4. 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 Fig. 2 is considered to illustrate the SIL selection process.

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

Initiating event (IE) locked rotor
IE frequency 0.01/year (Energy Institute and UK, 2006)
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