# IEC 61508: COMPATIBILITY, APPLICATION AND REQUIREMENTS IN CANADIAN NUCLEAR INDUSTRY

**Elyad Zahedi**[1]
[1] University of Toronto, Ontario, Canada

## Abstract

The renaissance of nuclear industry in Canada and worldwide comes with increasing safety concerns, requirements and regulations. This paper focuses on the study and analysis of IEC 61508 safety standard and its applications in Canadian nuclear industries. Identifying and detailed analysis of the IEC 61508 safety standard in this paper enables a clear mapping of the standard guidelines and Canadian safety requirements.

The main purpose of this paper is to enable the nuclear industries in Canada to gain a nuclear-specific scope and understanding of the standard in order to better apply this standard in their industrial procedures.

## 1. Introduction

The rapidly increasing need for cleaner and more efficient energy in the world has created a blooming season for nuclear industry in Canada and around the world. The increased demand and fast growing activities in nuclear world comes in the era of evolving modern technologies; Technologies that have increase the performance, reliability and naturally expectations from many different industries including nuclear industry. The increased expectations, especially the safety requirements come with increasing need for a systematic method of compliance. Safety standards such as IEC 61508 are developed for such purposes and are widely used in many safety-critical industries.

Compliance to international safety standards has an important effect in processing of commissioning procedures in Canadian nuclear industry. This effect has persuaded the nuclear industries around Canada to take serious measures toward compatibility to these standards. Nevertheless, the specific applications of each standard and their relativity to Canadian nuclear industry stay unclear in many aspects.

In addition to relevance of each standard to Canadian nuclear industry, the evolvement of each standard over a period of time and the flexibility of nuclear industry to comply with the changes are some of the main challenges faced in applying such standards to nuclear applications.

## 2. IEC 61508: Functional safety of electrical, electronic, programmable electronic safety-related systems

IEC 61508, Functional safety of electrical, electronic, programmable electronic safety-related systems (E/E/PES) is an international safety standard applicable to a wide range of indistries including safety-critical industries. Functional Safety in IEC 61508 is defines as: “part of the overall safety relating to the Equipment Under Control (EUC) and the EUC control system which depends

on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities."

Although sector-specific standards can be developed by interpretation of the generate standard, the standard covers the complete safety life cycle for a generic safety case of process control industry.

The safety life cycle can be divided to 3 main categories:

1. Analysis

2. Realization

3. Operation

The Analysis section of the life cycle constitutes the phase 1 through 5 of the standard. Realization is phase 6 through 13 of the standard and finally Operation contains the phases 14-16 of IEC 61508.

IEC 61508 contains two major parts: The first part is definition and explanation of the requirements and the second part is intended as a general guideline for safe practice of control applications and also includes several industrial examples as references.

The risk is a function of frequency of the hazardous events and the event consequence severities. The risk is reduced to a tolerable level by applying safety functions that may consist of E/E/PES. While other technologies may be employed in reducing the risk, only those safety functions relying on E/E/PES are covered by the detailed requirements of IEC 61508.

IEC 61508 covers all safety-related systems that are electrotechnical in nature (i.e. electromechanical systems, solid-state electronic systems and computer-based systems). The standard consists of the following parts:

Part 0: Functional safety and IEC 61508
Part 1: General requirements
Part 2: Requirements for E/E/PE safety-related systems
Part 3: Software requirements
Part 4: Definitions and abbreviations
Part 5: Examples of methods for the determination of safety integrity levels
Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
Part 7: Overview of techniques and measures

In order to fully understand the application of IEC 61508 in nuclear industry, the main concepts behind this standard should be explained:

## 2.1 Functional safety

Based on the definition of *safety* which is "the freedom from unacceptable risk of physical injury or of damage to the health of people as a result of damage to property or to the environment", *Functional safety* is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs and all possible accidents.

For example, an over-temperature protection device, using a thermal sensor in the windings of an electric motor to de-energize the motor before they can overheat, is an instance of functional safety. But providing specialized insulation to withstand high temperatures is not an instance of functional safety. This clearly is an application of functional safety that can be closely applied in nuclear industry. However, the additional regulations of nuclear industry should be addressed in order to satisfy the commissioning of the components for nuclear-grade applications.

### 2.2 Safety functions and safety-related systems

In addition to inherent safety design, which is the key factor in developing a safe environment, the necessity of executing functional safety requirements should be examined and evaluated based on individual applications.

"The term *safety-related* is used to describe systems that are required to perform a specific function or functions to ensure risks are kept at an accepted level. Such functions are, by definition, *safety functions*."

In addition to evaluation of the definition and role of the functional safety, the likelihood of the satisfactory performance of the function also needs to be taken into account.

Safety-related systems consist of any technology which performs safety functions. In the latter case, the equipment control system will be a safety-related system. In order to achieve an acceptable safety integrity level, a sold and well documented test plans and performance supervision is required.

## 3. Functional Safety Issues in Canada

Some of the key challenges of performing supervision in functional safety in Canada are analyzed in this section. The safety systems are mostly complicated, making it very challenging in practice to examine failure modes.

The main functionality of such standards is to primarily eliminate the possibility of hazardous and also to minimize the effect of such hazards should they happen.

Canadian history of industrial operation has shown the following to be the most common reasons for hazardous situations:

1. electromagnetic, temperature, mechanical phenomena and other environmental conditions
2. software errors
3. common cause failures
4. hardware or software lacking of system specifications
5. incomplete application of safety functions and requirements
6. random hardware failure mechanisms
7. systematic hardware failure mechanisms;
8. human error

## 4. Safety Integrity levels

IEC 61508 categorizes safety functions in 4 levels: System Integrity Level 1, 2, 3 and 4. The safety integrity levels (SILs) are ordered in increasing fashion in their integrity.

The applications of each level are limited in Canada and are specific to the industries and their risk assessments. For safety critical industries such as nuclear industry a safety level of SIL3 is most common. Industries with less severity in their hazardous situations are required to achieve SIL 1 or SIL2. Canadian industries are usually not required or awarded SIL4 for their performance as the requirements for this level of Safety integrity is very high and not easily achievable by most of the current instrumentations used in Canadian industries. For the industries with different functionalities which naturally will result in more that one required safety level, the highest of all the safety levels required will be needed to be applied to the entire plant.

## 5. References

[1] Functional safety and IEC 61508, *International Electrotechnical Commission*, September 2005, IEC, Geneva, Switzerland

[2] Furness, Harry. (1994). *Digital Communications Provides...* Control Engineering, January, 23–25.

[3] M. A. Hennell1, J. C. P. Woodcock2 and M. R. Woodward, *THE SAFETY INTEGRITY LEVELS OF IEC 61508 AND A REVISED PROPOSAL*, Department of Computer Science, University of Liverpool

[4] David J. Smith and Kenneth G. L. Simpson, Functional Safety, *Second Edition: A Straightforward Guide to Applying IEC 61508 and Related Standards*, Elsevier Butterworth-Heinemann