PRIMATECH WHITE PAPER

CHANGES IN THE SECOND EDITION OF IEC 61511: A PROCESS SAFETY PERSPECTIVE

Summary

From the perspective of process safety, the most notable change is the addition of requirements for a security risk assessment. Also, requirements for competence have been increased and they apply to process safety practitioners supporting functional safety. Such practitioners should be aware of a number of other pertinent changes.

Introduction

The IEC 61511 standard on functional safety addresses the part of process safety that relates to the correct functioning of safety instrumented systems (SISs) and other protection layers for the process industries.

Two clauses in the standard, Hazard and Risk Assessment, and Allocation of Safety Functions to Protection Layers, typically fall under the purview of process safety practitioners to support functional safety. Specifically, process hazard analysis (PHA) and safety integrity level (SIL) determination using techniques such as layers of protection analysis (LOPA) and risk graphs fall under these clauses. They are the only clauses in IEC 61511 for which detailed requirements deliberately are not provided in the standard.

This white paper identifies changes in the second edition of IEC 61511 that may impact process safety practitioners in supporting functional safety studies.

Inherently Safer Technology

The first edition stated that, in most situations, safety is best achieved by an inherently safe process design. The second edition qualifies this statement by adding, “However, in some instances this is not possible or not practical”.

Scope

The first edition stated that it applies to a wide variety of industries within the process sector and listed chemical, oil refining, oil and gas production, pulp and paper, and non-nuclear power generation as examples. The second edition adds pharmaceuticals and food and beverage to the list.

A figure in the first edition split a demand mode safety instrumented function (SIF) into prevention and mitigation types. The second edition removes this distinction.

Both low and high demand mode are recognized by the second edition. Low demand mode is where the frequency of demands is no greater than one per year while high demand mode is where the frequency of demands is greater than one per year.

Terminology

Some new definitions are provided, some previous definitions have been changed, and some previous definitions have been deleted. Of note to process safety practitioners are the following changes.

Newly defined terms include:

> *Hazardous event*: Event that can cause harm.
>
> This definition derives from ISO/IEC Guide 51:2014.
>
> *Hazardous situation*: Circumstance in which people, property or the environment are exposed to one or more hazards.
>
> This definition derives from ISO/IEC Guide 51:2014.
>
> *Harmful event*: Hazardous event which has caused harm.
>
> The standard notes that whether or not a hazardous event results in harm depends on whether people, property, or the environment are exposed to the hazardous situation and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred.
>
> *Process safety time*: Time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed.
>
> The standard notes that this is a property of the process only and that the SIF has to detect the failure and complete its action soon enough to prevent the hazardous event taking into account any process lag (e.g. cooling of a vessel).

The term *hazardous event* is a key concept in the IEC 61511 standard. However, surprisingly, it was not defined or explained in the first edition. In addition to the new definitions, the second edition also provides a figure that illustrates the relationship between hazardous event, hazardous situation, and harmful event (in Annex A to Part 3 of the standard). Unfortunately, hazardous events cannot be defined in a unique way

which creates difficulties in assessing their risks and determining SILs for SIFs.

Common cause failures and common mode failures have been redefined. They are now more understandable to process safety practitioners:

> *Common cause failures*: Concurrent failures of different devices, resulting from a single event, where these failures are not consequences of each other.
>
> *Common mode failures*: Concurrent failures of different devices characterized by the same failure mode (i.e., identical faults).

Risk is now defined as the combination of the probability, rather than frequency, of occurrence of harm and the severity of that harm. The standard notes that the probability of occurrence includes the exposure to a hazardous situation, the occurrence of a hazardous event, and the possibility to avoid or limit the harm. This definition derives from ISO/IEC Guide 51:2014. Frequencies can be viewed as probabilities per unit time, usually annual. Therefore, this change has no material effect on process safety studies.

The following definitions were deleted and the terms are not used in the second edition:

> *External risk reduction facilities:* Measures to reduce or mitigate the risks, which are separate and distinct from the SIS, e.g. a fire wall or bund / dike.
>
> *Other technology safety related systems*: Safety related systems that are based on a technology other than electrical, electronic, or programmable electronic, e.g. a relief valve.

These terms were never in use by process safety practitioners and they were hardly used in IEC 61511. Therefore, their removal is logical and of little consequence.

The second edition has substituted *hazardous event* for *hazard* in guidelines for PHRA which is consistent with process safety usage. Also, *levels of performance* has been replaced by *target failure measures* and *safety layers* by *protection layers*.

Process Safety Competence

The standard contains requirements for the management of functional safety. It states that persons, departments or organizations involved in SIS safety life-cycle activities shall be competent to carry out the activities for which they are accountable.

The standard lists various items that shall be addressed and documented when considering the competence of persons, departments, organizations or other units involved in SIS safety life-cycle activities. They include appropriate engineering

knowledge, training, and experience, and also safety engineering knowledge. Process safety analysis is given as an example of safety engineering.

The requirement for documentation of competence was introduced in the second edition, as were specific requirements for knowledge of the legal and regulatory functional safety requirements and adequate management and leadership skills appropriate to their role in the SIS safety life-cycle activities.

Notably, the second edition specifies that a procedure shall be in place to manage competence of all those involved in the SIS life cycle and that periodic assessments shall be carried out to document the competence of individuals against the activities they are performing and on change of an individual within a role.

Hazard and risk assessment are key parts of the SIS life cycle. Consequently, practitioners of hazard and risk assessments that support functional safety are covered by the competence requirements of the standard. In particular, practitioners of process hazard analysis (PHA) and risk assessment methods such as layers of protection analysis (LOPA) must be demonstrably competent.

Grandfather Clause

The U.S. standard, ISA-84.00.01-2004, which is the equivalent of IEC 61511-2004, contains the “grandfather clause” that derives from the U.S. Occupational Safety and Health Administration’s process safety management (PSM) standard:

> For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issue of this standard, the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.

A similar statement has been added to the second edition of IEC 61511 under Management of Functional Safety.

The intent of the grandfather clause is to recognize prior good engineering practices and to allow their continued use with regard to existing SISs. The grandfather clause releases the user from the design and construction requirements of the standard for existing installations, if the user can demonstrate compliance with the grandfather clause. The International Society for Automation (ISA) has addressed the applicability of the grandfather clause in the technical report, ISA-TR84.00.04-2005, *Guidelines for the Implementation of ANSI/ISA-84.00.01-2004*.

Management of Change

A management of change requirement has been added. The second edition states that management of change procedures shall be in place that identify changes that will affect the requirements on the SIS (e.g., re-design of a BPCS, changes to manning in a certain area).

Also, an elaboration was provided for the term *replacement in kind* beyond the previous "like for like" which was extended by adding "an exact duplicate of an element or an approved substitution that does not require modification to the SIS as installed".

Process Hazard and Risk Assessment (PHRA)

The process hazard and risk assessment is carried out to enable specifications to be derived for SISs. The requirements now specify that the PHRA be carried out on materials in addition to the process and equipment. This addition should have no effect on how PHRAs already are carried out.

The requirement for allocation of the safety functions to layers of protection has been deleted, no doubt because it replicates existing requirements in the clause, Allocation of Safety Functions to Protection Layers.

Initiators of hazardous events are now referred to as *initiating sources*.

PHRA Guidelines

The PHRA guidelines in the second edition now state that consideration should be given to past incidents, including the causes, system failures, and lessons learned to prevent reoccurrence. This is consistent with current practices.

The second edition now notes that successful activations of protection layers should be considered in the analysis. This guidance means that hazard scenarios involving the successful operation of process safeguards may need to be addressed.

The first edition referenced IEC 60300-3-9:1995 for the identification of hazardous events for more complex or new processes. This reference has been replaced by IEC/ISO 31010:2009, Risk management - Risk assessment techniques.

In discussing the judgement that should be made on when to include operator errors as initiating causes of hazardous events, the first edition states that operator error could often be excluded if the action is subject to permit procedures or lock-off facilities are provided to prevent inadvertent action. This practice would be hard to justify and the statement has been deleted from the second edition. Indeed, the second edition now states that a human reliability analysis should be performed when greater than a factor

of 10 credit is taken for an operator action.

Additional guidance has been provided on requirements for the design of alarm systems when used as means of risk reduction by reducing the demand rate on the SIS, or as a separate protection layer safety function reducing the overall risk of a scenario.

Also, it is now stated that periodic revalidations of the PHRA should be conducted and documented to ensure that assumptions match actual operational experience and that prompt follow-up and satisfactory resolution of recommendations arising from SIS life-cycle activities has occurred.

Security Risk Assessment

A new requirement has been added for a security risk assessment (SRA) to be carried out to identify the security vulnerabilities of the SIS. The SRA identifies threats that could exploit vulnerabilities and result in security events, including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error. Also, it identifies the potential consequences resulting from the security events and the likelihood of the events occurring. Requirements for additional risk reduction are determined.

The standard notes that the SRA can range in focus from an individual SIF to all SISs within a company and that the SRA can be included in an overall process automation SRA.

The standard notes that guidance related to SIS security is provided in:

- ISA TR84.00.09, *Security Countermeasures Related to Safety Instrumented Systems*
- ISO/IEC 27001:2013, *Information technology - Security techniques - Information Security Management Systems -- Requirements*
- IEC 62443-2-1:2010, *Industrial communication networks - Network and System security - Part 2-1: Establishing an Industrial Automation and Control System Security Program*

Allocation of Safety Functions to Protection Layers

Requirements

The first edition of IEC 61511 specified that the allocation process shall result in “the allocation of safety functions to specific protection layers for the purpose of prevention, control or mitigation of hazards from the process and its associated equipment” while

the second edition states that it shall result in “the allocation of safety functions required to achieve the necessary risk reduction to specific protection layers”. This change removes an implied definition of the purpose of protection layers from the first edition.

A requirement was added to the allocation process that if the risk reduction required for a hazardous event is allocated to multiple SIFs in a single SIS, then the SIS shall meet the overall risk reduction requirement.

Also, the results of the allocation process must now be recorded so that the SIFs are described in terms of the functional needs of the process, such as the actions to be taken, etc. The standard suggests that this description can be referred to as the process requirements specification or the safety description. It is used as input information for the Safety Requirements Specification.

SIL 4 Requirements

The additional requirements for allocation of SIFs with safety integrity level 4 provided in the first edition have been removed. No doubt this reflects the prevailing view that SIL 4 SIFs should not be used in the process industries because the integrity level is too difficult to achieve and maintain.

Requirements on the Basic Process Control System as a Protection Layer

Additional requirements have been imposed on BPCSs. The second edition requires that the BPCS not only be designed but also be managed to IEC 61511 requirements if the risk reduction claimed for a BPCS protection layer is greater than 10.

Furthermore. If the BPCS is not intended to conform to IEC 61511 requirements, then:

- No more than one BPCS protection layer shall be claimed for the same sequence of events leading to the hazardous event when the BPCS is the initiating source for the demand on the protection layer; or

- No more than two BPCS protection layers shall be claimed for the same sequence of events leading to the hazardous event when the BPCS is not the initiating source of the demand.

In these cases, each BPCS protection layer must be independent and separate from the initiating source and from each other to the extent that the claimed risk reduction of each BPCS protection layer is not compromised. For example, a hot backup controller is not considered to be independent of the primary controller because it is subject to common cause failure.

Primatech Publications Relating to Functional Safety

P. Baybutt, Layers of Protection Analysis for Human Factors (LOPA-HF), Process Safety Progress, Vol. 21, No. 2, pages 119 - 129, June, 2002.

P. Baybutt, An improved risk graph approach for determination of safety integrity levels (SILs), Process Safety Progress, Vol. 26, No. 1, pages 66 - 76, March, 2007.

P. Baybutt, Risk tolerance criteria for layers of protection analysis, Process Safety Progress, Vol. 31, No. 2, pages 118–121, June, 2012.

P. Baybutt, Using layers of protection analysis to evaluate fire and gas systems, Process Safety Progress, Vol. 31, No. 3, pages 255–260, September, 2012.

P. Baybutt, Conducting process hazard analysis to facilitate layers of protection analysis, Process Safety Progress, Vol. 31, No. 3, pages 282–286, September, 2012.

P. Baybutt, Using risk tolerance criteria to determine safety integrity levels for safety instrumented functions, Journal of Loss Prevention in the Process Industries, 25 (6), pages 1000 - 1009, 2012.

P. Baybutt, Risk tolerance criteria and the IEC 61511/ISA 84 standard on safety instrumented systems, Process Safety Progress, Vol. 32, Issue 3, pages 307–310, September 2013.

P. Baybutt, The interface of functional safety with process safety and risk analysis, Process Safety Progress, Vol. 32, Issue 4, pages 346–350, December 2013.

P. Baybutt, The ALARP Principle in Process Safety, Process Safety Progress, Vol. 33, Issue 1, Pages: 36–40, March 2014.

P. Baybutt, The use of risk matrices and risk graphs for SIL determination, Process Safety Progress, Vol. 33, Issue 2, pages 179–182, June 2014.

P. Baybutt, Addressing enablers in layers of protection analysis, Process Safety Progress, Vol. 33, Issue 3, pages 221–226, September 2014.

P. Baybutt, Allocation of risk tolerance criteria, Process Safety Progress, Vol. 33, Issue 3, pages 227–230, September 2014.

P. Baybutt, Calibration of risk matrices for process safety, Journal of Loss Prevention in the Process Industries, Vol. 38, pages 163-168, 2015.

P. Baybutt, Designing Risk Matrices to Avoid Risk Ranking Reversal Errors, Process Safety Progress, Volume 35, Issue 1, pages 41–46, March 2016.

P. Baybutt, Setting multinational risk tolerance criteria, Process Safety Progress, Volume 35, Issue 2, pages 153–158, June 2016.

P. Baybutt, Addressing subjectivity and uncertainty in using risk matrices, Loss Prevention Bulletin, Issue 252, December, 2016.

