INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

IEC 61511-1
Edition 2.0 2016-02

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 1: Framework, definitions, system, hardware and application programming requirements

IEC 61511-1
Édition 2.0 2016-02

SECURITE FONCTIONNELLE – SYSTEMES INSTRUMENTES DE SECURITE POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION –

Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

CORRIGENDUM 1

Corrections to the French version appear after the English text.

Les corrections à la version française sont données après le texte anglais.

3.2.39.1
demand mode SIF

Replace 3.2.39.1 notes to entry with the following:

Note 1 to entry: In the event of a dangerous failure of the SIF, a hazardous event can only occur

– if the failure is undetected and a demand occurs before the next proof test;
– if the failure is detected by the diagnostic tests but the related process and its associated equipment has not been moved to a safe state before a demand occurs.

Note 2 to entry: In high demand mode, it will normally be appropriate to use the continuous mode criteria.

Note 3 to entry: The safety integrity levels for SIF operating in demand mode are defined in Tables 4 and 5.

3.2.75.2
limited variability language
LVL

Replace definition 3.2.75.2 with the following:

programming language for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application as defined by the associated safety manual. The notation of this language may be textual or graphical or have characteristics of both.

Note 1 to entry: This type of language is designed to be easily understood by process sector users, and provides the capability to combine predefined, application specific, library functions to implement the SRS. LVL provides a close functional correspondence with the functions required to achieve the application.

IEC 61511-1:2016-02/COR1:2016-09(en-fr)

Note 2 to entry: IEC 61511 assumes that the constraints necessary to achieve the safety properties are achieved by the combination of the safety manual, the closeness of the language notations to the functions the application programmer needs to define the process control algorithms, and the compile time and run time checks which the logic solver provider embeds into the logic solver system program and the logic solver development environment. The constraints identified in the certification report and safety manual can ensure the relevant requirements of IEC 61508-3:2010 are satisfied.

Note 3 to entry: LVL is the most commonly used language when the IEC 61511 series refers to “application program”.

9.2.5 *Replace Subclause 9.2.5 with the following:*

9.2.5 In cases where the allocation process results in a risk reduction requirement of >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour for a single SIS or multiple SISs or SIS in conjunction with a BPCS protection layer, there shall be a reconsideration of the application (e.g., process, other protection layers) to determine if any of the risk parameters can be modified so that the risk reduction requirement of >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour is avoided. The review shall consider whether:

– the process or vessels/pipe work can be modified to remove or reduce hazards at the source;
– additional safety-related systems or other risk reduction means, not based on instrumentation, can be introduced;
– the severity of the consequence can be reduced, e.g., reducing the amount of hazardous material;
– the likelihood of the specified consequence can be reduced e.g., reducing the likelihood of the initiating source of the hazardous event.

NOTE Applications which require the use of a single SIF with a risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour need to be avoided because of the difficulty of achieving and maintaining such high levels of performance throughout the SIS safety life-cycle. Risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour can require high levels of competence and high levels of coverage for all factory acceptance testing, proof testing, verification, and validation activities.

9.2.6 *Replace Subclause 9.2.6 with the following:*

9.2.6 If after further consideration of the application and confirmation that a risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour is still required, then consideration should be given to achieving the safety integrity requirement using a number of protection layers (e.g., SIS or BPCS) with lower risk reduction requirements. If the risk reduction is allocated to multiple protection layers then such protection layers shall be independent from each other or the lack of independence shall be assessed and shown to be sufficiently low compared to the risk reduction requirements. The following factors shall be considered during this assessment:

– common cause of failure of SIS and the cause of demand;

NOTE 1 The extent of the common cause can be assessed by considering the diversity of all devices where failure could cause a demand and all devices of the BPCS protection layer and/or the SIS used for risk reduction.

NOTE 2 An example of common cause between the SIS and the cause of demand is if loss of process control through sensor fault or failure can cause a demand and the sensor used for control is of the same type as the sensor used for the SIS.

– common cause of failure with other protection layers providing risk reduction;

NOTE 3 The extent of the common cause can be assessed by considering the diversity of all devices of the BPCS protection layer and/or the SIS used to achieve the risk reduction requirements.

NOTE 4 An example of common cause between SISs providing risk reduction is when two separate and independent SISs with diverse measurements and diverse logic solvers are used but the final actuation devices are two shut off valves of similar types or a single shut off valve actuated by both SISs.

– any dependencies that may be introduced by common operations, maintenance, inspection or test activities or by common proof test procedures and proof test times;

NOTE 5 Even if the protective layers are diverse then synchronous proof testing will reduce the overall risk reduction achieved and this can be a significant factor impeding achievement of the necessary risk reduction for the hazardous event.

NOTE 6 When high levels of risk reduction are required and proof tests are desynchronised according to Note 5 then the dominant factor is normally common cause failure even if multiple independent protection layers are used to reduce risk. Dependency within and between protection layers providing risk reduction for the same hazardous event can be assessed and shown to be sufficiently low.

9.2.7 *Replace Subclause 9.2.7 with the following:*

9.2.7 If a risk reduction requirement >10 000 or average frequency of dangerous failures $<10^{-8}$ per hour is to be implemented, whether allocated to a single SIS or multiple SIS or SIS in conjunction with a BPCS protection layer, then a further risk assessment shall be carried out using a quantitative methodology to confirm that the safety integrity requirements are achieved. The methodology shall take into consideration dependency and common cause failures between the SIS and:

– any other protection layer whose failure would place a demand on it;
– any other SIS reducing the likelihood of the hazardous event;
– any other risk reduction means that reduce the likelihood of the hazardous event (e.g., safety alarms).

Table 6 – Minimum HFT requirements according to SIL

Replace Table 6 with the following:

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

15.2.2 *Replace Subclause 15.2.2 third bullet with the following:*

- in accordance with the preceding bullet, the measures (techniques) and procedures that will be used for confirming that each SIF conforms with the specified safety requirements and the specified SIL;