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;

Corrections à la version française:

3.2.39.1
SIF en mode sollicitation

Remplacer les notes à l'article de 3.2.39.1 par les suivantes:

Note 1 à l'article: Dans l'éventualité d'une défaillance dangereuse de la SIF, un événement dangereux ne peut se produire que:

– si la défaillance n'est pas détectée et qu'une sollicitation survient avant l'essai périodique suivant;

– si la défaillance est détectée par les essais de diagnostic, mais que le processus concerné et ses équipements associés n'ont pas basculé dans un état de sécurité avant qu'une sollicitation ne survienne.

Note 2 à l'article: En mode à sollicitation élevée, il sera normalement approprié d'utiliser les critères du mode continu.

Note 3 à l'article: Les niveaux d'intégrité de sécurité des SIF fonctionnant en mode sollicitation sont définis au Tableau 4 et au Tableau 5.

3.2.75.2
langage de variabilité limitée
LVL

Remplacer la définition 3.2.75.2 par la suivante:

langage de programmation destiné aux automates programmables industriels du commerce dont les capacités sont limitées à leur mise en oeuvre, telle que définie par le manuel de sécurité associé. La notation de ce langage peut être textuelle, graphique ou présenter les caractéristiques des deux.

Note 1 à l'article: Ce type de langage est conçu pour être aisément compris par les utilisateurs du secteur des industries de transformation, et permet de combiner des fonctions de bibliothèque, prédéfinies, spécifiques à une application, pour mettre en œuvre les SRS. Les LVL fournissent une correspondance fonctionnelle étroite avec les fonctions exigées pour réaliser l'application.

Note 2 à l'article: L'IEC 61511 part du principe que les contraintes nécessaires à l'obtention des propriétés de sécurité sont le résultat de la combinaison du manuel de sécurité, de la proximité de la notation avec les fonctions dont le programmateur d'application a besoin pour définir les algorithmes de commande de processus et du temps de compilation et des vérifications d'exécution que le fournisseur de l'unité logique intègre dans le logiciel de base de l'unité logique et son environnement de développement. Les contraintes identifiées dans le rapport de certification et le manuel de sécurité peuvent garantir que les exigences de l'IEC 61508-3:2010 sont satisfaites.

Note 3 à l'article: Le LVL est le langage le plus fréquemment utilisé lorsque la série IEC 61511 fait référence au terme "programme d'application".

Note 4 à l'article: L'abréviation "LVL" est dérivée du terme anglais développé correspondant "limited variability language".

9.2.5 *Remplacer le Paragraphe 9.2.5 par le suivant:*

9.2.5 Si le processus d'allocation donne une exigence de réduction de risque > 10 000 ou une fréquence moyenne de défaillance dangereuse < 10^{-8} par heure pour un ou plusieurs SIS conjointement avec une couche de protection BPCS, l'application (p. ex.: processus, autres couches de protection) doit être reconsidérée afin de déterminer si l'un des paramètres de risque peut être modifié de manière à éviter l'exigence de réduction de risque de > 10 000 ou de fréquence moyenne de défaillance dangereuse < 10^{-8} par heure. La revue doit notamment considérer si:

– le processus ou les cuves/tuyauteries peuvent être modifiés pour éliminer ou diminuer les dangers à la source;

– des systèmes relatifs à la sécurité complémentaires ou d'autres moyens de réduction de risque (non basés sur l'instrumentation) peuvent être introduits;

– la gravité de la conséquence peut être réduite, par exemple en réduisant la quantité de substances dangereuses;

– la probabilité d'occurrence de la conséquence indiquée peut être réduite, par exemple en diminuant la probabilité d'occurrence de la source initiatrice de l'événement dangereux.

NOTE Les applications exigeant l'utilisation d'une seule SIF avec une exigence de réduction de risque > 10 000 ou une fréquence moyenne de défaillance dangereuse < 10^{-8} par heure nécessitent d'être évitées compte tenu de la difficulté à réaliser et maintenir de tels niveaux élevés de performance tout au long du cycle de vie de sécurité du SIS. L'exigence de réduction de risque > 10 000 ou la fréquence moyenne de défaillance dangereuse < 10^{-8} par heure peut exiger des niveaux élevés de compétence et des niveaux élevés de couverture pour tous les essais de réception en usine, essais périodiques, vérification et activités de validation.

9.2.6 *Remplacer le Paragraphe 9.2.6 par le suivant:*

9.2.6 Si un examen approfondi de l'application confirme qu'une exigence de réduction de risque > 10 000 ou que la fréquence moyenne de défaillance dangereuse < 10^{-8} par heure est toujours exigée, il convient d'envisager la réalisation de l'exigence concernant l'intégrité de sécurité à l'aide de couches de protection multiples (p. ex.: SIS ou BPCS) faisant l'objet d'exigences de réduction de risque inférieures. Si la réduction de risque est allouée à plusieurs couches de protection, ces couches de protection doivent être indépendantes les unes des autres ou l'absence d'indépendance doit être évaluée et démontrée comme suffisamment faible par rapport aux exigences de réduction de risque. Les facteurs suivants doivent être étudiés lors de cette évaluation:

– la cause commune de défaillance du SIS et la cause de la sollicitation;

NOTE 1 L'étendue de la cause commune peut être évaluée en tenant compte de la diversité de tous les appareils dont la défaillance pourrait entraîner une sollicitation et de tous les appareils de la couche de protection BPCS et/ou du SIS utilisés pour réaliser la réduction de risque.

NOTE 2 Un exemple de cause commune entre le SIS et la cause de la sollicitation est la perte de commande du processus suite à une anomalie ou une défaillance du capteur, ce qui peut entraîner une sollicitation, le type de capteur utilisé pour la commande étant le même que celui du capteur utilisé pour le SIS.

– la cause commune de défaillance avec d'autres couches de protection fournissant la réduction de risque;

NOTE 3 L'étendue de la cause commune peut être évaluée en tenant compte de la diversité de tous les appareils de la couche de protection BPCS et/ou du SIS utilisés pour réaliser les exigences de réduction de risque.

NOTE 4 Un exemple de cause commune entre les SIS fournissant la réduction de risque est lorsque deux SIS indépendants et séparés caractérisés par des mesures diversifiées et des unités logiques diversifiées sont utilisés, mais que les appareils actionneurs terminaux sont deux vannes d'arrêt de type similaire ou une seule vanne d'arrêt commandée par les deux SIS.

– la ou les dépendances pouvant être introduites par des activités communes d'exploitation, de maintenance, d'inspection ou d'essai ou encore par des procédures d'essai périodique et des horaires d'essai périodique communs.

NOTE 5 Même si les couches de protection sont diversifiées, les essais périodiques synchrones atténueront la réduction globale de risque obtenue, ce qui peut constituer un facteur important empêchant d'atteindre la réduction de risque nécessaire pour l'événement dangereux.

NOTE 6 Si des niveaux de réduction de risque élevés sont exigés et que les essais périodiques sont désynchronisés selon la Note 5, le facteur dominant est en principe une défaillance de cause commune, même si plusieurs couches de protection indépendantes sont utilisées pour réduire le risque. La dépendance au sein et entre les couches de protection assurant la réduction de risque pour le même événement dangereux peut être évaluée et présentée comme étant suffisamment faible.

9.2.7 *Remplacer le Paragraphe 9.2.7 par le suivant:*

9.2.7 Si une exigence de réduction de risque > 10 000 ou si la fréquence moyenne de défaillance dangereuse < 10^{-8} par heure doit être mise en œuvre, qu'elle soit allouée à un ou plusieurs SIS ou à un SIS associé à une couche de protection BPCS, une autre évaluation du risque doit être réalisée par une méthodologie quantitative visant à confirmer que les exigences concernant l'intégrité de sécurité sont satisfaites. La méthodologie doit prendre en compte les défaillances dépendantes et les défaillances de cause commune entre le SIS et:

– une autre ou d'autres couches de protection dont la défaillance entraînerait une sollicitation de celle-ci;

– un autre ou d'autres SIS réduisant la probabilité d'occurrence de l'événement dangereux;

– un autre ou d'autres moyens de réduction de risque réduisant la probabilité d'occurrence de l'événement dangereux (p. ex.: alarmes de sécurité).

Tableau 6 – Exigences de HFT minimale en fonction du SIL

Remplacer le Tableau 6 par le suivant:

Tableau 6 – Exigences de HFT minimale en fonction du SIL

SIL	HFT minimale exigée
1 (n'importe quel mode)	0
2 (mode à faible sollicitation)	0
2 (mode à solicitation élévée ou continu)	1
3 (n'importe quel mode)	1
4 (n'importe quel mode)	2

15.2.2 *Remplacer la troisième puce du Paragraphe 15.2.2 par la suivante:*

- conformément au point ci-dessus, les mesures (techniques) et les procédures qui seront utilisées pour confirmer que chaque SIF est conforme aux exigences de sécurité spécifiées et au SIL spécifié;