Guidelines on Safety Instrumented Systems in Major Hazards Installations

Revision 0 Oct 2020

About this set of Guidelines:

Instrumented Protective Systems[1] (IPSs) are commonly used in the process industries to implement safety functions, such as process safety interlocks and emergency shutdowns, in order to achieve or maintain a process in a safe state with respect to a specific hazardous event. These safety functions typically provide risk reduction of ≤10, and are referred to as Instrumented Protective Functions[2] (IPFs) in this document.

Safety functions meeting higher levels of functional safety performance providing risk reduction of >10, i.e. of Safety Integrity Level[3] (SIL) 1 or higher, are termed as Safety Instrumented Functions[2] (SIFs). The application and requirements of SIFs in the process industries and the corresponding Safety Instrumented Systems[1] (SISs) implementing them are further addressed through the IEC 61511 standards[4] (*Functional safety – Safety instrumented systems for the process industry sector*).

This document, "Guidelines on Safety Instrumented Systems in Major Hazards Installations", is intended to provide guidance on:

- The approach for hazard and risk assessment to evaluate the required functional safety performance of IPFs and SIFs.
- The considerations for implementing IPFs and SIFs for further risk reduction, to as low as reasonably practicable ("ALARP").
- The principles and requirements for managing, operating and maintaining existing IPSs and SISs.

[1] **IPSs** / **SISs**: Refers to the instrumented system, composing of any combination of sensor(s), logic solver(s) and final element(s), that implements one or more of the corresponding IPFs / SIFs.

[2] **IPFs** / **SIFs**: Refers to the safety function, implemented by the corresponding IPS / SIS, that is intended to achieve or maintain a process in a safe state, with respect to a specific hazardous event.

[3] **SIL**: Refers to the level of functional safety performance to be achieved. A SIF meeting the requirements of SIL 1 can achieve a risk reduction of > 10 to ≤ 100.

[4] The latest edition of IEC 61511 should be applied. References to specific clauses in this document was based on the 2nd edition (2016), should it be updated, the equivalent clause in the updated standard should instead be applied.

Guidelines on Safety Instrumented Systems in Major Hazards Installations

1. Objective

1.1 Instrumented Protective Systems (IPSs) are commonly used in the process industries to implement safety functions, such as process safety interlocks and emergency shutdowns, in order to achieve or maintain a process in a safe state with respect to a specific hazardous event. These safety functions typically provide risk reduction of ≤10, and are referred to as Instrumented Protective Functions (IPFs) in this document. For IPSs to be effective in reducing risk, it is essential that its designed functional safety performance be met.

1.2 Safety functions meeting higher levels of functional safety performance providing risk reduction of >10, i.e. of Safety Integrity Level (SIL) 1 or higher, are termed as Safety Instrumented Functions (SIFs). The application and requirements of SIFs in the process industries and the corresponding Safety Instrumented Systems (SISs) implementing them are addressed through the IEC 61511 standards (*Functional safety – Safety instrumented systems for the process industry sector*). The standard covers the entire SIS life-cycle, from initial concept, design, implementation, operation and maintenance through to decommissioning.

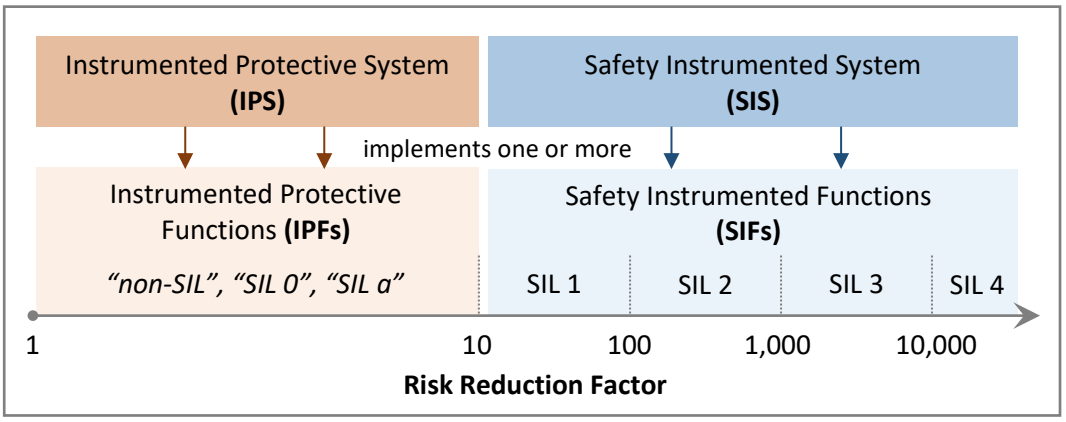

Figure 1: Illustration of terminology used in this document

1.3 This document aims to provide guidance to Major Hazards Installations (MHIs) on the application of IEC 61511 in their facilities, including evaluation of the required performance of IPFs and SIFs; implementation of IPFs and SIFs for further risk reduction; and management, operation and maintenance of existing IPSs and SISs.

2. Scope

2.1 This document is primarily intended for existing facilities[5]. MHIs planning greenfield facilities or new expansions / modifications to brownfield sites should perform the necessary hazard & risk assessments and implement identified IPFs and/or SIFs in

[5] Existing facilities – Any facility where the first cycle Safety Case was submitted before 1 January 2022

compliance with IEC 61511 in its design. MHIs could approach the Major Hazards Department (MHD) for consultation if there are difficulties in doing so.

2.2 The extent of current implementation of IPFs and SIFs and compliance to IEC 61511 varies across existing MHIs due to differences in the age of the facility, knowledge on SISs, etc. MHIs are to refer to the flow chart in Figure 2 on the applicability of the various sections in this document.

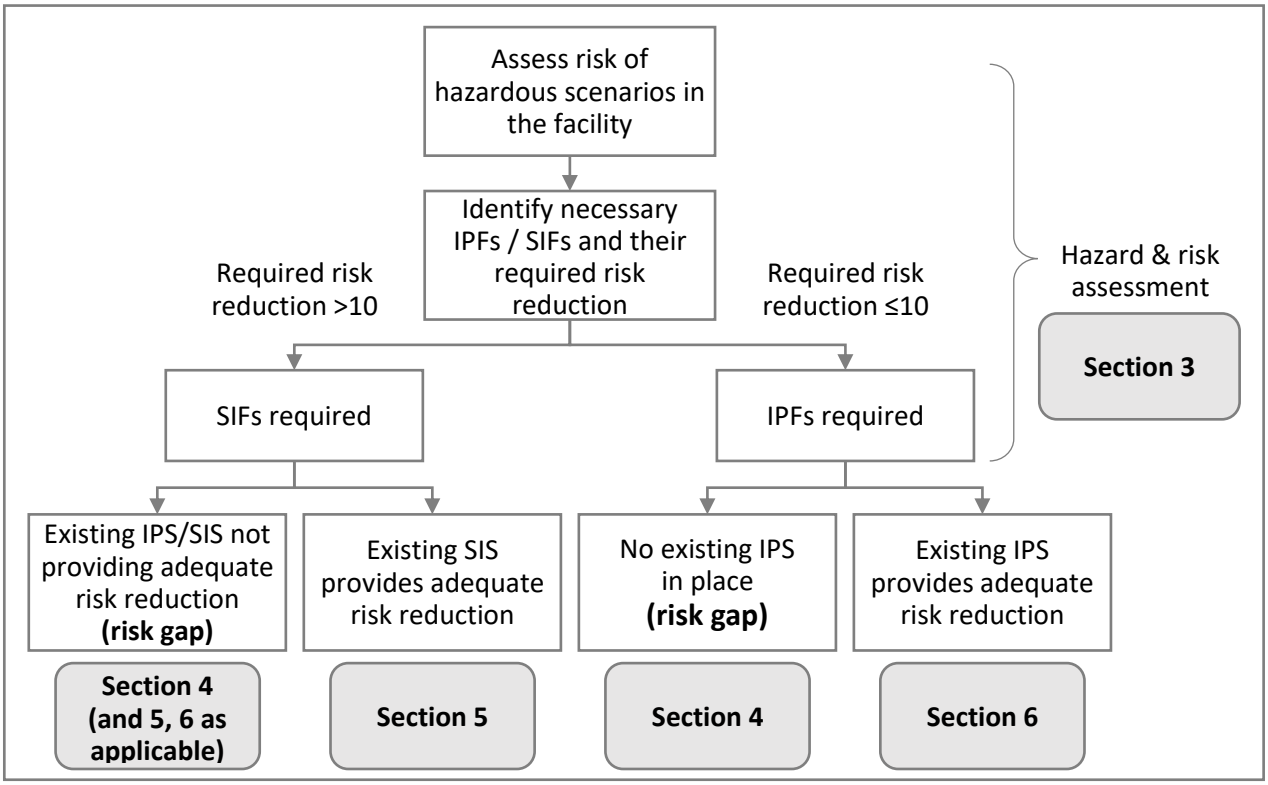

Figure 2. Flow chart for application of this document

2.3 **Section 3** provides the overall approach MHIs with identified IPFs and/or SIFs should take to assess their required functional safety performance, and to evaluate the adequacy of any existing instrumented systems.

2.4 Based on the assessment and the extent of existing IPFs and/or SIFs implementation, MHIs should then refer to Sections 4, 5 and/or 6 as appropriate for further guidance on:

i. Considerations for implementing additional IPFs and/or SIFs in accordance to IEC 61511 for further risk reduction **(Section 4)**.

ii. Requirements for operating and maintaining existing SISs to ensure safety and reliability **(Section 5)**.

iii. Principles for managing existing IPSs in line with industry good practices **(Section 6)**.

2.5 Lastly, **Section 7** provides additional guidance on the risk-based approach for applying and implementing the guidelines set out in this document.

3. Guidance on Hazard & Risk Assessment and Adequacy of Safety Systems

This section is applicable to MHIs that require IPFs and/or SIFs to achieve or maintain their process in a safe state with respect to a specific hazardous event.

3.1 The objective of the hazard & risk assessment is for MHIs to assess the risk from hazardous scenarios and identify existing safeguards, so as to determine the necessary IPFs and/or SIFs and their required functional safety performance.

3.2 Process Hazard Analysis (PHA) studies should form the basis of the assessment. MHIs should review if their existing PHA methodology has considered the key requirements in Clauses 8 and 9 of IEC 61511-1, such as ensuring independency of protection layers available while accounting for potential common cause failures. Additionally, the maximum risk reduction that could be claimed for Basic Process Control Systems (BPCS) in quantitative assessments should be ≤ 10, unless the system also complies with the requirements for higher functional safety performance in IEC 61511. Similarly, for safety functions implemented prior to publication of IEC 61511, risk reduction of >10 can be claimed if it had been assessed and verified that the system meets IEC 61511 requirements.

3.3 Examples of methods that can be used to establish the required functional safety performance, such as Layer of Protection Analysis (LOPA), are illustrated in IEC 61511-3. MHIs should also review the document *"ALARP Demonstration Guidelines: Single Scenario Risk Tolerability Target and Adequacy of Barriers"* for further guidance on LOPA methodology, and on the risk target that should be set. Any safety function requiring functional safety performance of SIL 1 or greater (risk reduction >10) should be implemented by a SIS conforming to IEC 61511, for effective risk reduction.

3.4 MHIs should evaluate if existing systems implementing the identified safety functions provide sufficient functional safety performance, or if additional safeguards are required to reduce risk to ALARP, and refer to the subsequent Sections 4, 5, and/or 6 as appropriate.

3.5 It should be emphasised that the assessment should be proportionate to the risk, and an extensive, quantitative assessment is not always warranted, as qualitative PHA studies may be used for screening out less hazardous scenarios.

4. Guidance on Implementation of IPFs and/or SIFs for Further Risk Reduction

This section is applicable to MHIs with identified risk gaps that may need to be closed by implementing additional IPFs and/or SIFs, or by upgrading existing IPFs to SIFs in accordance with IEC 61511, to reduce risks to ALARP.

4.1 Where the risk gaps could be closed by implementation of identified IPFs, MHIs should generally do so at the earliest opportunity. Provision of IPSs to reduce risk of identified hazards is a common good practice in the process industries, and MHIs should do so without undue delay in order to demonstrate that risks are ALARP.

4.2 It is however recognised that implementation of SIFs in accordance with IEC 61511 requires extensive efforts and commitment. MHIs should carefully assess if such risk reduction measures are "reasonably practicable", and provide justification for the selected decision.

4.3 When determining "reasonable practicability", it is important that MHIs do not evaluate each decision in isolation, as there are often significant shared costs between multiple SIFs/SISs that would reduce their individual costs. The benefits arising from implementing the required functional safety management system would also extend beyond the SISs in consideration, and contribute to the overall functional and process safety at site.

4.4 In addition, where assessed to be "grossly disproportionate", further consideration should be given to examine all other means of reducing risk, so as to comply with the ALARP principles. Such measures could include improving means of monitoring and detecting hazards, or by increasing the testing frequency of the existing instrumented systems, or any other protection layers not related to instrumented functions.

4.5 In general, where implementation of SIFs is assessed to be reasonably practicable, MHIs should upgrade existing IPSs or install additional SISs in full compliance with IEC 61511. In particular, reference should be made to the requirements in Clauses 11–15, 17 of IEC 61511-1, pertaining to the design, engineering, installation, commissioning, validation and modification of SISs.

4.6 Partial measures, such as upgrading individual components without consideration for the overall SIS design, should be avoided to minimise unnecessary duplication of efforts later on to bring the system into full compliance.

5. Guidance on Management of Existing SISs

This section is applicable to MHIs with existing SISs.

5.1 These existing SISs should be managed in a manner that meets the full SIS life-cycle requirements of IEC 61511, failing which the required functional safety performance of the SISs cannot be assured, and may instead create a false sense of security.

5.2 MHIs with existing SISs should have a good understanding of the safety requirements of their SISs and define the required performance standards and specifications, so as to operate and maintain their SISs appropriately. MHIs should refer to Clauses 10 and 16 of IEC 61511-1 to assess the necessary requirements, and develop appropriate implementation plans as an immediate high priority.

5.3 MHIs should also review their functional safety management programme with reference to IEC 61511, and develop implementation plans to address identified deficiencies to move towards full compliance with the SIS life-cycle requirements in the longer term.

6. Guidance on Management of Existing IPSs

This section is applicable to MHIs with existing IPSs.

6.1 Depending on the outcome of the hazard & risk assessment, existing IPSs may or may not be adequate for the specified hazardous event. Section 4 of this guidance covers the considerations that should be made if existing IPSs were found to be inadequate.

6.2 Irrespective of the assessment, MHIs should ensure an appropriate standard of management for these IPSs, in line with industry good practices, are in place and applied throughout their operational life. This is also part of the requirements in criterion 7.1.1.4 of the Safety Case Assessment Guide.

6.3 The following should be taken into consideration in the management of existing IPSs to ensure their effectiveness and reliability:

i. competency of persons managing the instrumented systems;

ii. availability of clear specifications of the safety function with relevant engineering documentation;

iii. periodic inspection and maintenance, in line with manufacturers' recommendations and general good practice;

iv. periodic proof testing at appropriate intervals; and

v. proper management of change for the IPF.

6.4 MHIs should also refer to "Management of instrumented systems providing safety functions of low / undefined safety integrity" by the UK Health and Safety Executive, viewable at https://www.hse.gov.uk/foi/internalops/og/og-00046.htm, for further guidance.

7. Guidance on Risk-Based Approach for Implementation

7.1 In developing these guidelines, it is acknowledged that many MHIs would face significant challenges in implementing them, particularly for older facilities and for MHIs with lesser knowledge of SISs.

7.2 It is recommended that MHIs adopt a risk prioritisation approach in implementing these guidelines. The initial risk assessment and identification of IPFs and/or SIFs and their required functional safety performance should begin with known higher risk scenarios (for example, Safety Critical Events identified in Safety Cases). Timeline for the subsequent assessment could be aligned with the facility's existing PHA re-validation cycles to spread out resource requirements. MHD will engage individual MHIs through the safety case assessments to set appropriate implementation targets and timelines, based on the guidance set out in this document.

7.3 With respect to identified deficiencies in meeting the SIS life-cycle requirements of existing SISs, MHIs should consider giving higher priority to rectifying those relevant to operation and maintenance as described in Section 5. Efforts should also be made in

developing action plans to improve the competency of personnel and the company's functional safety management system while in transition to full compliance with IEC 61511.

7.4 Similarly, where existing instrumented systems have been assessed to be inadequate, MHIs should perform the relevant ALARP assessment beginning with the hazardous events with significant risk gaps (e.g. where the residual risks are found to be intolerable) to develop a prioritised improvement plan.

7.5 Proposed implementation plans can be discussed with MHD, together with any relevant follow-up items arising from the Safety Case assessment. Potential limitations and constraints should be highlighted, such that the overall plan could be suitably prioritised to consider these challenges.

8. List of References

8.1 The following publications provide further information on SISs, standards requirements, and guidance on management of SISs of low safety integrity:

International Electrotechnical Commission (IEC), 2016. *Functional Safety - Safety Instrumented Systems for Process Industry Sector.* IEC 61511

International Electrotechnical Commission (IEC), 2010. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.* IEC 61508

The 61508 Association, 2011. *Guidance for the Management of Legacy Safety Systems.* Retrieved from https://www.61508.org/images/downloads/Legacy_systems_-_Guidance_for_the_Managment_of_Legacy_Systems_V-1.1_27-4-11.pdf

Health and Safety Executive, 2014. *Management of instrumented systems providing safety functions of low / undefined safety integrity.* Retrieved from https://www.hse.gov.uk/foi/internalops/og/og-00046.htm

Acknowledgements

This guide was jointly developed by the Safety Case Workgroup (SCWG) comprising representatives from the Major Hazards Department (MHD) and industry members of the Singapore Chemical Industry Council (SCIC). MHD would like to express its appreciation to SCIC, industry members in the SCWG, as well as all stakeholders in the MHI industry for their feedback and support.

The SCWG consists of the following members:

	Name	Capacity
Co-Chair:	Mdm Jaime Lim	MHD
Co-Chair:	Mr Amit Bhatnagar	Singapore Refining Company Private Limited
Members:	Er. David Kan	Infineum Singapore Pte Ltd
	Mr Evert Klein	ExxonMobil Asia Pacific Pte Ltd
	Mr David Sugiman	Asahi Kasei Synthetic Rubber Singapore Pte Ltd
	Er. Gloria Wang	Shell Eastern Petroleum (Pte) Ltd
	Er. Jacqueline Liew	MHD
	Mr Wong Jianting	MHD
	Er. Lim Liang Hong	MHD
	Ms Jolyn Ho	MHD
Secretariat Support:	Ms Agmer Lee	Singapore Chemical Industry Council
	Ms Gina Ling	Singapore Chemical Industry Council