Safety case Electrical, Control & Instrumentation (EC&I) aspects

Safety Case Assessment Guide

1. Must MHIs append samples of calculations, studies, inspection records etc. in the safety case? Some of this information is confidential. Could we provide the information for viewing in our office instead of including them in the safety case report?

   Adequate details and information supporting the demonstration of control measures will need to be provided in the safety case. By virtue of section 45 of the WSH Act, all information received will be treated as confidential.

2. What is the level of detail expected in the safety case? Most of the information would be better demonstrated during on-site verification than in documentation. Do MHIs need to share detailed particulars of personnel involved in safety case e.g. Certificate of LEW, NRIC, etc.

   Companies are generally not required to provide detailed personnel particulars in safety case documentation. MHD will focus on the system and procedural levels for safety case assessment. At a minimum, the safety case should include relevant P&IDs of the SCEs to assist in the demonstration of control measures and to facilitate MHD's understanding of the processes.

3. Safety Case Assessment Guide requires MHIs to demonstrate competency in SIL level determination, SIS design and maintenance of EC&I systems. Does competency refer to specific functional safety competencies e.g. functional safety certifications, functional safety? Or would competence gained through on-the-job-training and work experience in relevant areas such as operation / maintenance / process safety and design be acceptable?

   Relevant staff must have good understanding of the EC&I systems in order to implement the requirements and maintain the systems.

   To demonstrate this, MHIs could use a Training – Core Competency Matrix, which matches training and experience to competencies needed for SIL implementation, SIF design, installation and maintenance. The demonstration should include how the MHI determined the level of understanding, training and education needed to perform those tasks.

   Functional safety certification is not a requirement but would be useful for the demonstration of EC & I competency.

4. Can third parties be engaged for EC&I activities?
   What proof/documentation is required in the safety case to demonstrate that the third party is competent to do the work, especially for past projects?

Yes, third parties can be engaged.

The MHI will need to demonstrate competency for third parties e.g. relevant competencies and experience in proof testing and SIS maintenance; basic understanding and training in functional safety, especially in requirements for record keeping and SIS proof test procedure.

5. What proof/documentation is required in the safety case to demonstrate survivability of critical utilities and adequacy of backup e.g. UPS?
   - Are there standards/guidelines for utilities?
   - Is an instrument designed to fail safe on loss of utilities good enough?
   - Can MHIs adopt in-house guidelines instead of IEC61511?

There are a range of codes, standards, good engineering practices and guidelines for the design/maintenance of utilities that MHIs can take reference from.

Examples of critical utilities that could impact on safety are compressed air, N_2, steam etc. In the safety case, MHIs should describe the utilities, their sources, how loss of utility is detected and actions taken upon loss detection. Information on utility specifications (e.g. compressor capacity), availability of backup systems, utility recovery, maintenance, inspection and testing should be provided. Documentation such as test records and diagrams would support demonstration in the safety case.

Designing fail-safe instruments is good engineering practice and enhances reliability. However, the use of fail-safe design does not remove the need for utility survivability. Instead, it should be seen as a complement to utility design. The SIS should comply with IEC61511.

MHIs that adopt in-house guidelines for non-SIL control must demonstrate that in-house guidelines are comparable to good industry engineering practices and guidelines.

6. Does Safety Case require MHI to apply IEC61511 to:
   - relay based systems, PLC and DCS with loops used for safety protection
   - general alarm systems and Priority 1 Alarm systems used for safety protection

All systems deemed to be SIS and SIL-rated should adhere to IEC61511. For alarm management, refer to EEMUA 191.

Beyond the scope covered by these standards, good engineering practices shall apply. For example, selection and placement of detectors should be considered and could be addressed by detector mapping.

7. What proof/documentation is required in the safety case to demonstrate adequacy of non SIL-rated system?

   The safety case should include the identification of SIFs, SRSs, inspection records etc. MHIs can refer to HSE's Operational Guidance on "Management of instrumented systems providing safety functions of low / undefined safety integrity".

IEC 61511

8. Do MHIs need to adhere to all requirements in IEC 61511?

   MHIs could determine and implement the relevant requirements. However, if the MHI claims to comply with IEC61511, all requirements in the standard will need to be complied with.

   MHIs adopting alternative standards will need to provide justifications.

9. IEC 61511, Section 8.2.4 calls for "A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS". Security risk assessment is new for the process industries in Singapore. What is the timeline for MHIs to complete the assessment?

   Safety case covers industrial risks that could lead to major accidents. Although security is beyond the scope of SCAG, MHIs should ensure that their systems are secure and safe from cyber attacks. Currently, demonstrations of security and cyber attack prevention are not required in safety case.

10. Fire and Gas detection has been taken out of the scope of IEC 61511. The general understanding is that the PFD for detectors can be influenced by external environmental conditions (e.g. wind direction), thus, SIL rating of detectors would not be sufficient. Would it be acceptable to use detector mapping to demonstrate sufficient coverage by detectors of a SIF, as part of SIL verification?

    F&G systems is within the scope of IEC61511. Detector mapping is good practice to demonstrate sufficient detection coverage.

Safety Instrumented Function & Safety Integrity Level

11. The assessment of EC&I is skewed to the assessment of Safety Instrumented Function/System (SIF/SIS) and Safety Integrity Level (SIL). However, not all companies have introduced SIF/SIS/SIL into their management system.

    In our MHI, the process safety functions are executed by control logics in Distributed Control Systems (DCS), i.e. when certain process conditions are met, safety interlocks will be activated to bring the process to a predetermined safe state. The analysis of these interlocks is done in the process safety section.

    Often, the design of safety interlocks and additional safety functions (e.g. safety relief valves, pressure balancing lines) in processes are based on PHA/HAZOP as there are no international standards.

    Could MOM provide guidance on how MHIs not using SIF/SIS/SIL can demonstrate that they have met the EC & I criteria?

    Refer to HSE's Operational Guidance on "Management of instrumented systems providing safety functions of low / undefined safety integrity". Good engineering practices should be applied to instrumented protection systems.

    There should not be shared components between BPCS and SIS. The BPCS shall be designed to meet SIL capability. Otherwise, the SIS is expected to be only as good as a BPCS.

SCAG Appendix F – 'Electrical, Control & Instrumentation Assessment Criteria and Guidance'

Clarifications on Technical Criterion 7.1.1.2

7.1.1.2 (a): Are there standards for air compressor system design?

Refer to UK HSE's HSG 39 "Compressed air safety" or other equivalent.

7.1.1.2 (c): Does this refer to supplies for operations in safe mode or normal mode?

Both. MHIs need to demonstrate that electrical and instrument air supplies are suitable and adequate for both modes. MHIs need to describe supply sources, how they work, how loss of utilities is detected, actions to be taken upon loss detection and plans for inspection, maintenance, testing etc.

The reliability of fail-safe systems needs to be demonstrated, e.g. to consider whether there are excessive demands placed on the system which could change the demand mode.

7.1.1.2 (d): What is an example of integrity requirement?

For a SIL 1 capable SIS, the integrity requirements should cover the utility supply and its backup systems. It is also good practice for a SIS to be designed to fail safe on loss of utility.

7.1.1.2 (k): Please elaborate on this requirement?

Suitably rated equipment should be used for electrical power generation, distribution and use. The equipment should be rated to safely handle the **calculated maximum short circuit current** at the rated voltage of the system under consideration. Switchgears and transformers should be designed based on this as well.

7.1.1.2 (m): Please elaborate on this requirement?

Excessive electrical stress should be avoided by adopting relevant good practices for the design of electrical systems. Appropriate voltage and current protection systems should be used and electrical systems should be suitably rated. Procedures and authorization required for handling high voltage equipment, overcurrent/undercurrent protection etc. should be described.

Clarifications on Technical Criterion 7.1.1.4

7.1.1.4 (aii): What is an example of machinery safety systems?

Rotating equipment vibration monitoring systems

7.1.1.4 (d): Please elaborate on how this requirement can be met?

MHIs can refer to guidance available for legacy systems, such as 61508.org's "Legacy Systems: Principles for Safety" and HSE's Operational Guidance on "Management of instrumented systems providing safety functions of low / undefined safety integrity"

Clarifications on Technical Criterion 7.1.1.5

7.1.1.5 (b): Any example on how to address this requirement?

IEC 62305 part 2 – risk assessment covers both lightning protection systems and surge protection systems, and focuses on sensitive and critical equipment.

7.1.1.3 (c) What is lightning protection level? How is it applied?

IEC 62305 Part 1 gives 4 lightning protection levels – range of currents associated with lightning strikes (1-low significant; 4-high significant). Other standards that can be referred to include API 2003 and API 545 "Protection Against Ignitions arising out of Static, Lightning and Stray Current". MHIs can also refer to SS 555 Part 1-4, which is equivalent to IEC 62305. For legacy sites, MHI should perform a gap analysis and bridge the gaps as far as reasonably practicable.

Clarifications on Technical Criterion 7.1.2

7.1.2 (b): Please elaborate how MHIs can meet this requirement. Is there a template for a typical inspection on Ex equipment? How should MHIs ensure that their maintenance crews have proper certification for EX equipment maintenance?

First, identify HAC zones. Designate relevant Ex equipment for use in each zone. Based on HAC zoning, MHIs should stipulate a testing framework including frequency, tests required, competency of personnel to conduct the testing etc. MHIs could refer to IEC 60079 Part 10 for HAC, Part 17 for maintenance and Part 14 for selection of equipment.

Typically, maintenance of EX equipment should be carried out by CompEX certified personnel. MHD, together with relevant agencies, will explore how to address the lack of competency certification in Singapore. MHD will consider if LEWs can double as competent personnel for maintenance of EX equipment.

Technical Criterion 7.1.4.1

7.1.4.1 (b) Please explain what this requirement means?

This requirement targets critical spares or spares for SIS. The Mean Time To Restoration affects PFD calculations, as the delivery/lead time of spares may exceed and affect expected PFD, especially for safety instrumented systems with higher integrity levels.

The expected turnaround duration for “immediate restoration” is less than 8hrs. MHIs will need to demonstrate this using examples if claiming “immediate restoration”.

Clarifications on Technical Criterion 7.2

Please elaborate on the expectations for 7.2 and performance standards.

This criterion applies to process safety performance indicators (PSPI) set by the MHI, which is not limited to EC&I. Refer to API 754 or HSG 254 on how to determine performance indicators.

References

Links to Guidance	Description
http://www.hse.gov.uk/eci/eci-delivery-guide.pdf	Inspection of EC&I Systems
http://www.hse.gov.uk/foi/internalops/og/og-00046.htm	Management of instrumented systems providing safety functions of low / undefined safety integrity
http://www.hse.gov.uk/foi/internalops/og/og-00047.htm	Operator Response within Safety Instrumented Systems
http://www.hse.gov.uk/foi/internalops/og/og-00054.htm	Proof Testing of Safety Instrumented Systems
http://www.hse.gov.uk/comah/sragtech/techmeasutilitie.htm	Reliability of Utilities
http://www.hse.gov.uk/pubns/books/hsg39.htm	Compressed air safety guidance
http://www.61508.org/images/downloads/Legacy-Systems-Basic-Principles-for-Safety-V-2.5-01.10.2009-Version-for-website1.pdf	Legacy Systems: Principles for Safety
http://www.hse.gov.uk/pubns/books/hsg254.htm	Developing Process Safety Performance Indicators