8 Aug 2022

Key Findings from Intervention Plans

–

Process Safety
Electrical Control & Instrumentation
Mechanical Integrity

(For Circulation)

Please note that this publication is part of MHD Annual Report 2022, which shares the insights of the Safety Case Regime in Singapore.

Introduction

Since implementing the Safety Case regime in September 2017, key findings from Intervention Plan (IP[1]) items issued to MHIs are summarised in three focus areas:

a) Process Safety,
b) Electrical, Controls & Instrumentation, and
c) Mechanical.

These key findings are meant to serve as a guidance, for MHIs to demonstrate the effectiveness and reliability of protective measures that have been put in place. While the focus starts with Safety Critical Events (SCEs), MHIs should extend the scope to Major Accident Scenarios (MASs) on a proportionate basis, with possible leverage on systemic implementation via existing Safety and Health Management Systems.

Process Safety

MHD assessors observed that MHIs could better demonstrate the requirements in Process Safety criteria 5.2.1.5[2] and 5.2.1.7[3] of the Safety Case Assessment Guide:

a) Demonstrate the adequacy and sufficiency of their pressure relief arrangement for a given vessel, equipment, or system (criteria 5.2.1.5 & 5.2.1.7).
b) Demonstrate the safety of reaction chemistries and the basis of safety relied upon to ensure safety for a given reactor (criterion 5.2.1.7).

a) Demonstrate the adequacy and sufficiency of their pressure relief arrangement for a given vessel, equipment, or system

Pressure relief devices such as pressure relief valves (PRV) protect a process vessel or reactor from pressure excursions or overpressures. As it is often the last line of defence when other systems such as process cooling and control systems have failed, it is imperative that pressure relief devices are sized adequately for worst-case credible[4] scenarios. Otherwise, potentially serious consequences could ensue.

A desirable demonstration of an MHI's pressure relief arrangement would entail a demonstration of the MHI's overpressure protection philosophy and PRV design basis. MHIs are advised to peruse *API 521 Pressure-relieving and Depressuring Systems*, which provides guidance on the following aspects:

- Hierarchy of protective measures
- Consideration of single/double jeopardy

[1] Intervention Plan refers to the items or topics which warrant further discussion in subsequent years before the next Safety Case submission.
[2] The Safety Case shall show that appropriate measures have been taken to prevent and effectively contain releases of dangerous substances.
[3] The Safety Case shall describe how adequate control measures have been provided to protect the plant against excursions beyond design conditions.
[4] Credible scenarios as indicated in PHA study conducted at site including HAZOP, What If or other PHA study methodologies.

- Role of instrumentation in overpressure protection
- Use of administrative controls and consideration of operator's actions.

When demonstrating the design basis of PRVs, MHIs are expected to provide reasons and evidence in response to:

- Are all the credible overpressure scenarios identified for the system of interest?
- How is the relief load and subsequently the required relief area for each applicable scenario determined for the purpose of sizing for the worst-case credible overpressure scenario (or controlling case)?

A focused systematic analysis could be done to identify all credible overpressure scenarios, or MHI could reference relevant PHA studies to obtain the credible overpressure scenarios. As a guide, API 521 lists some common occurrences that require overpressure protection as shown in Table 1. Plant managers, process engineers, and other relevant personnel should deploy engineering judgement to carefully assess site-specific hazards or uncommon factors that might also constitute an overpressure source. Justifications should be provided for an overpressure scenario's inclusion or exclusion (applicable to situation where overpressure scenario deemed credible but judged to be excluded from consideration) from the design basis consideration. [Examples: (1) distillation process without any reactive hazard – no justification needed if "chemical reaction" scenario was not considered, (2) for a full vapour system with no liquids, no justification is needed for an "overfilling" scenario.]

Table 1. Causes of overpressure (non-exhaustive list).

Common occurrences of overpressure	
• Blocked outlets • Cooling or reflux failure • Absorbent flow failure • Accumulation of non-condensable • Entrance of volatile material • Overfilling • Failure of automatic controls • Abnormal process heat or vapour input	• Internal explosions or transient pressure surges • Chemical reaction • Hydraulic expansion • External fires • Heat transfer equipment failure • Power failure • Maintenance

Demonstrating a PRV's design basis with respect to overpressure scenarios could include a coherent combination of the following:

- Equipment details: Relief valve identification numbers and set pressure, corresponding equipment tag and service type, P&ID reference etc.
- List of all possible credible scenarios: e.g. external fire, blocked outlet, air fan failure, power failure, cooling water loss, instrument air failure, failure of critical valves
- For each credible scenario, the details of the release: vapour rate, molecular weight, liquid rate, density, temperature etc.
- Other considerations: e.g. emergency depressurisation rate, emergency response procedures.

API 521 also provides general considerations and specific guidelines for the various overpressure scenarios listed in Table 1. Good engineering judgement, rather than blind adherence to these

guidelines, should be followed in each case. For relief area sizing, MHIs could peruse *API 520 Sizing, Selection, and Installation of Pressure-relieving Devices Part 1* for sizing procedures and methods.

b) Demonstrate the safety of reaction chemistries and the basis of safety relied upon to ensure safety for a given reactor

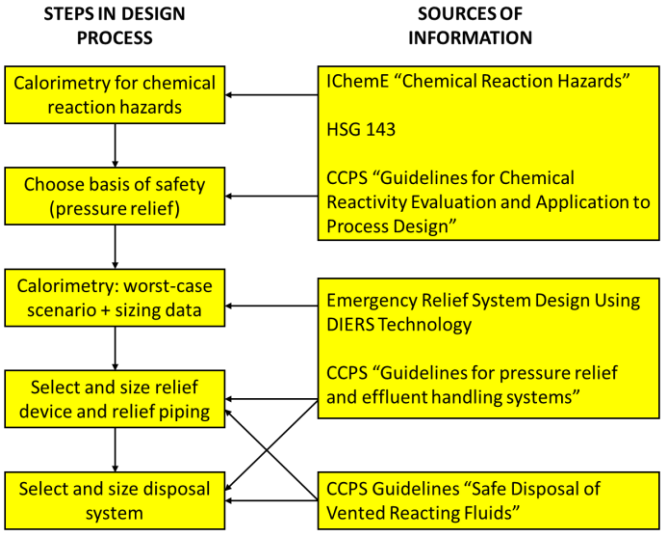

Figure 2. Runaway Reaction Case – Steps in design process and sources of information

Figure 2 shows the typical steps in the design process and possible sources of information for a case of runaway reaction. The basis of safety for a reactor is the combination of measures (e.g. hardware, protective systems, and procedures) that are deemed safety critical, with direct references to the chemical reaction. The basis of safety can only be selected once all foreseeable hazards have been systematically identified and evaluated. Hence, it is crucial to show the pathways or deviations that could lead to a runaway in the Safety Case, for example:

- Cooling failure
- Incorrect charging sequence
- Agitator failure or restart of agitator after failure
- Contamination of reaction mixture
- Fast/slow addition of reactants
- High/low temperature
- Different reactant concentration
- Removal or omission of volatile diluents
- More/less catalyst

Based on information obtained from the reaction hazard assessment, the basis of safety for the reactor is selected with the intent of implementing barriers necessary for runaway pathways or process deviations. Table 2 shows some examples of measures that could be included as part of a reactor's basis of safety.

Table 2. Examples of preventive and protective measures used as part of an overall basis of safety for a reactor.

Preventive Measures	Protective Measures
Basic process control system (BPCS) Safety interlock Emergency shutdown system Procedural controls	Emergency relief system Emergency dumping system Total containment within reactor Emergency cooling Reaction inhibition Quenching or drown-out

Using the example of an emergency relief system as part of an overall basis of safety, understanding chemical processes through reaction hazard assessments must be exhibited in the Safety Case, with identification of all credible conditions that could lead to a runaway.

As the emergency relief system is the last line of defence, the design of the emergency relief system must be adequate and sufficient for the worst-case credible scenario. The worst-case credible scenario is identified by the maloperation that gives rise to the largest relief size required. Kinetic data (e.g. rate of temperature/pressure rise) is required for the purpose of sizing reactive relief systems and such data are usually obtained through calorimetry tests.

In addition, all credible maloperations that could lead to runaway reactions but are not considered further in the relief sizing design basis should be properly justified.

MHIs are advised to refer to *Emergency Relief System Design Using DIERS Technology*, *CCPS Guidelines for pressure relief and effluent handling systems* or other similar sources for more information on sizing of reactive relief system.

The evaluation of chemical reaction hazards should be undertaken by technically qualified and experienced personnel[4]. Operations personnel are strongly recommended to be involved in the assessment for enhanced understanding of the measures and barriers implemented. Reaction hazard assessments typically include desktop screening methods, small-scale screening tests, and reaction calorimetry tests. MHIs are advised to refer to *HSG 143 Designing and operating safe chemical reaction processes* and *CCPS Guidelines for Chemical Reactivity Evaluation and Application to Process Design* for further guidance. MHIs are also advised to seek expert help, where available, from their corporate HQ, catalyst vendor/technology licensors, or competent laboratories or institutes specialising in reaction hazard assessments.

MHI to consult MHD for further action in cases where despite best efforts, the MHI is still not able to obtain reaction chemistry details for the basis of relief valve sizing. These efforts include exploring with MHI's corporate headquarters, technology suppliers, catalyst vendors (wherever applicable), and other relevant technical resources.

[4] Could also refer to a team consisting of various disciplines/functions with knowledge of reaction chemistry, plant operation, process hazards, risk assessment.

Electrical, Controls & Instrumentation

Most MHIs faced challenges in fulfilling the requirements outlined in Safety Case Assessment Guide Electrical, Controls & Instrumentation (EC&I) criteria 7.1[5], 7.1.1.4[6] and 7.1.4.1[7].

MHIs could enhance Safety Cases to:

a) Demonstrate how necessary instrumented safety functions are identified and the required integrity level is determined (criterion 7.1).
b) Demonstrate the management of functional safety system is in accordance with current relevant good practice (criteria 7.1.1 4 and 7.1.4.1).
c) Demonstrate the adequacy of maintenance regime for safety critical EC&I systems to prevent major accidents or reduce the loss of containment in event of such accidents (criterion 7.1.4.1).

a) Demonstrate how necessary instrumented safety functions are identified and the required integrity level is determined.

The first activity of the IEC 61511 safety life-cycle model calls for a process Hazard and Risk Assessment (H&RA) to identify and determine the performance requirements of the instrumented safety functions (i.e. safety integrity level, SIL). Most MHIs used a qualitative process hazard analysis (PHA) such as HAZOP as the basis of assessment for identifying safeguards required to prevent and mitigate risk. Such qualitative methods are however not suitable, for major accident scenarios (MAS) and safety critical events (SCE), to demonstrate that the safeguards are independent and sufficient with adequate safety integrity to reduce the risk to as low as reasonably practicable (ALARP). As a minimum, semi-quantitative analysis such as Layer of Protection Analysis (LOPA) or other sound engineering methods such as Fault Tree Analysis (FTA) should be used to assess MAS and minimally keep the risk level to the tolerable region through the implementation of safeguards. MHIs should ensure that the depth of the H&RA is commensurate to the risk.

A good H&RA would help MHIs correctly assess the adequacy of existing safeguards and determine the required integrity of the safety functions for further risk reduction, to ALARP. MHIs can refer to the CCPS publication[8] for additional LOPA guidance and MHD's ALARP demonstration guidelines[9].

[5] Criterion 7.1: The safety case shall show a clear link between the measures taken and the SCEs described.
[6] Criterion 7.1.1.4: The safety case shall show how safety-related control systems have been designed to ensure safety and reliability.
[7] Criterion 7.1.4.1: The safety case shall show that an appropriate maintenance regime is established for plant and systems to prevent major accidents or reduce the LOC in the event of such accidents.
[8] Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, 2015. ISBN 978-0-470-34385-2
[9] ALARP Demonstration Guidelines: Single Scenario Risk Tolerability Target and Adequacy of Barriers, 2020. https://www.mom.gov.sg/-/media/mom/documents/safety-health/mhi/alarp-demo-guidelines.pdf

Common LOPA pitfalls observed include:

- Initiating events of higher risk scenarios that were identified in bow ties did not have corresponding LOPA studies.
- Qualitative assessments tended to underestimate the consequences of LOPA scenarios.
- Failure to identify the common mode of failure within the same layer. (e.g. BPCS, alarm layer, operators)
- Assumption that operators always have time to react to an alarm, including actions to be taken, without justification.
- Overestimation of the reliability of safeguards (probability of failure on demand values), as established literature basis or proper justifications were lacking.

b) Demonstrate the management of functional safety system is in accordance with current relevant good practice.

The management of functional safety system begins with determination of instrumented safety functions (SIFs) and requirements. Functional safety systems such as the safety instrumented system (SIS) should be managed in a manner that fulfils the requirements stipulated in IEC 61511 standards (*Functional safety – Safety instrumented systems for the process industry sector*) as part of ALARP demonstration, to assure the required functional safety performance of the SIS throughout its lifecycle. MHD assessors noted the varying extent of compliance to IEC 61511-1 across MHIs due to differences in the age of the facility, knowledge on SISs, etc. Some examples include:

- Inadequate understanding of the SIF's required performance with respect to the Safety Requirement Specifications (SRS), and the SIS verification and validation's intent in accordance with the standards. Most MHIs had left this initial part of the SIS activities to the Engineering, Procurement and Construction (EPC) or project team, and the knowledge or ownership of the SIS design was not properly passed down to the Operations and Maintenance team. MHI should understand the objective /significance of each activity and the key information available from the output of each phase.
- Lack of competent persons to oversee the overall functional safety system and its full compliance to standards. MHIs could appoint an in-house technical coordinator who is familiar with SIS life-cycle requirements, to coordinate all engineering activities related to SISs and ensure adequate documentation and records are maintained. The technical coordinator could also contribute to the development or review of the MHI's competence management system, to ensure persons involved in each SIS activity have the right competency to perform the task.
- Inadequate inspection and maintenance regime. *(Refer to (c) for further discussion)*
- IEC 61511-1 requirements for Functional Safety Assessment (FSA) and auditing were not carried out. MHIs should review their functional safety management programme with reference to IEC 61511, and thereafter develop implementation plans to address identified deficiencies to move towards full compliance with the SIS life-cycle requirements in the longer term.

MHIs can refer to MHD's Guidelines on Safety Instrumented Systems in Major Hazards Installations, and IEC 61511-2 for more details on the application of IEC 61511-1.

c) Demonstrate the adequacy of maintenance regime for safety critical EC&I systems to prevent major accidents or reduce the loss of containment in event of such accidents.

Implementing an effective maintenance regime is as important as safety critical EC&I equipment design, to prevent and mitigate major accidents. MHIs are to identify from risk assessments, the safety critical EC&I equipment and implement an appropriate maintenance regime. Typical safety critical EC&I equipment include:

- Basic Process Control System (BPCS)
- Electrical power system and its backup power system (e.g. Uninterruptible Power Supply (UPS), emergency diesel generator)
- Lightning protection system
- Gas detection system
- SIS.

A robust maintenance regime increases the reliability and availability of the equipment through periodic testing and inspections by competent persons. The scope of testing, inspection and servicing requirements are to be demonstrated in accordance with relevant industry codes and standards or vendor recommendations, allowing MHIs to uncover potential undetected failures relevant to the equipment. In some cases, MHD assessors noticed that the SIS inspections and proof tests' coverages were insufficient to fully validate the performance requirements of the safety functions as specified in the SRS, such as:

- Insufficient proof test coverage, as partial loop tests were carried out and did not constitute a complete full loop test for the given SIF.
- Failure modes applicable to the SIFs (i.e. response time, backup arrangements) were not tested.

MHIs are advised to refer to IEC 61511-1 Clause 16 and the UK Health and Safety Executive publication "Principles for proof testing of safety instrumented systems in the chemical industry"[10] for guidance on maintenance and proof testing of SIS.

[10] Principles for proof testing of safety instrumented systems in the chemical industry: https://www.hse.gov.uk/research/crr_pdf/2002/crr02428.pdf

Mechanical Aspect

Based on 422 Mechanical IP items generated, 44.5% of the IP items were targeted at the Maintenance Regime implemented in MHIs:

a) Criterion 6.1.3.1 – The Safety Case shall show that an appropriate maintenance regime is established for plant and systems to prevent major accidents or reduce the LOC in the event of such accidents.
b) 6.1.3.3 – The Safety Case shall show that systems are in place to ensure that safety critical equipment and systems are examined at appropriate intervals by a competent person.

a) Demonstrate an appropriate maintenance regime is established for plant and systems to prevent major accidents or reduce the LOC in the event of such accidents.

A maintenance master plan facilitates the capture of all mechanical/ECI equipment with the corresponding planned inspection dates. This master plan should also include a risk ranking filter for prioritisation purposes. From the list of equipment, MHIs are then required to define what is deemed as safety critical equipment in Safety Cases. [Refer to a(ii)]

The following key points are expected in an MHI's Safety Case.

- Maintenance Administration System
  - Online? Manual?
  - How are maintenance activities contracted out, coordinated and managed?
- Maintenance Regime/Strategy
  - Overarching principles
  - Run-to-fail? Preventive Maintenance? Grading system?
- Prioritisation of maintenance activities
  - Safety critical assets identified in system
  - Re-prioritisation of overdue works
- Structure of Maintenance Department
  - Available resources? Roles and responsibilities?

i. Maintenance strategy / regime

- Underlying basic policy: Plant assets shall be maintained as required by law, standards and codes and acceptable engineering practices to ensure safe operation, high reliability, and availability of plants.
- Preventive/Predictive Maintenance (PM) Programme: Based on equipment criticality as identified during design and the monitored reliability, categorised into time-based and condition-based. PM for safety critical barriers including relief valves, SIS, critical alarms and process control loops, critical check valves, critical pumps and compressors, turbine overspeed trip tests, toxic gas and LEL detectors/ analysers etc., are required in the Safety Case. A system is required to track job tasks as determined in the PM Programme, based on stipulated PM frequency for each specific equipment. Some MHIs' systems were observed to automatically generate work orders when the equipment was due for PM – e.g. inspections

were scheduled to be in-line with planned shutdowns and turnarounds, unless the equipment could be taken out of service onstream.

- Condition-based Maintenance: For example, operators in an MHI were equipped with handheld devices to collect and log in critical equipment condition data, for rotating equipment and general valves. Other conditions monitored included lubrication oil levels, pump seal leaks, abnormal temperatures, noise, and vibrations, etc. For high criticality equipment, online condition monitoring systems conducted real-time diagnostic and performance monitoring. Pre-alarms were also setup for early warning to identify and diagnose the problem before deterioration and failure of equipment. All data collected were coherently used and appropriately linked back to the maintenance programme, specific to the equipment or group of equipment.
- Corrective Maintenance: e.g. For onstream breakdown of equipment and instruments, corrective work orders were raised by Operations team to alert the Maintenance team. The Maintenance team of engineers/technicians/technical assistants would then carry out the asset maintenance, repair and calibration based on daily planning of work. Daily planning of work was carried out by maintenance planning engineers or supervisors. Depending on the criticality assessment and nature of problem observed, the equipment/plant may even be stopped for immediate rectification.

ii. Prioritisation of assets and maintenance activities

When prioritising assets, the basis should include safety critical equipment, equipment history/reliability, consequential loss, and most suitable maintenance method. Other factors of consideration include impacts on safety, environmental and production. Criticality ranking should be conducted by a cross-functional team consisting of Operations, Maintenance, Process Engineering, Process Safety, and Reliability (fixed assets and rotating) personnel.

After categorising and risk ranking of the equipment, Safety Cases are expected to explain how work priority is determined using equipment and job criticality levels. Criticality levels could be based on immediate threats to safety of people and plant, significant production impacts or equipment redundancy. The highest work order priority should include immediate actions taken on the asset and the rescheduling of other maintenance activities.

b) Demonstrate that systems are in place to ensure that safety critical equipment and systems are examined at appropriate intervals by a competent person. The Safety Case shall also show that there is a system in place to ensure the continued safety of the installations based on the results of periodic examinations and maintenance.

Safety Case should include the following factors for every safety critical equipment:

- Examination by a competent person[11]
- Examination at appropriate intervals
- Assessment of results

The following should be considered for continuing mechanical integrity of safety critical equipment via Risk-Based Inspections, Written Schemes of Examination, Equipment Strategies, Examination Reports, or Maintenance Assessments:

- Was there a Risk-Based Inspection study carried out?
- Who developed the study?
- What scope of examination does it specify?
- What are the foreseeable degradation mechanisms for this asset?
- What is the examination interval? How was this justified?
- What arrangements are in place to postpose an examination if needed?
- Does the scope of the examination carry out match that in the RBI/ WSE, etc.? If not, why not?
- Who assesses the results of examination (including remaining thickness and any corrosion allowance) to decide if the asset is fit for continued service?
- Where the corrosion allowance has been exceeded, were more detailed "fitness for service" demonstrations carried out?
- Does the report specify any defects or remedial actions? Any evidence that these remedial works were actually carried out?

Common References

- API 510 Pressure Vessel Inspection Code: In-service Inspection, Rating, Repair, and Alteration
- API RP 571 Damage Mechanisms Affecting Fixed Equipment in the Refining Industry
- API 653 Tank Inspection, Repair, Alteration, and Reconstruction

[11] By definition, a designated competent person to perform specified duties is based on his/her training (e.g. API-certified), knowledge, and experience. For example, could be an MHI to showcase its competent inspection engineer via an API-Certified Inspector for Pressure Vessels and Piping Tankage, who has an AWS-Certified Senior Welding Inspector with 14 years of experience in inspections, of which 10 years as Plant Inspector in Oil & Petrochemical industry.