Demonstration of Adequacy A Practical Guide

Raymond Wright

FSE Global Pte Ltd

Safety Case Symposium 2018 Singapore

Overview

- Purpose of Safety Case
- Purpose of Demonstration
- How to Demonstrate
- Demonstration by Example

Purpose of Safety Case - WSH (MHI) Regulations: Third Schedule, Part 1

To demonstrate that:

1. *A Major Accident Prevention Policy and a Safety & Health Management System have been established and implemented.*
2. *All Major Accident Hazards have been identified and Major Accident risks eliminated or reduced to ALARP.*
3. *Adequate measures have been incorporated into the design and construction and the operation and maintenance of the Major Hazard Installation.*
4. *An emergency response plan takes the necessary measures in the event of a Major Accident.*

Purpose of Demonstration

To provide assurance to all stakeholders how safe operation is achieved and maintained over the life of the MHI by providing evidence that the facility SMS has the necessary elements that work together to ensure:

- MA scenarios have been identified and assessed, and MA risk is ALARP.
- Safe Design and Construction.
- Safe Operation and Maintenance of the facility.
- An Emergency Response is available should risk control measures fail.

How to Demonstrate

Provide evidence to show a clear understanding and use of the SMS elements that drive all the activities undertaken by

- Providing a detailed description of all risk management activities undertaken
- Describing the processes used, and how decision are made for each activity, and linking each activity to specific SMS elements.
- Describe how other systems of work, such as Asset Management, Action Tracking, Training, MOC, PTW, LOTO, etc. are used in conjunction with these activities.
- Provide worked examples using selected high-risk MAs.

MA Prevention Policy

Est. Requirement	Examples of Evidence
Available	It is has an assigned document number.

Imp. Requirement	Examples of Evidence
In Use	Provide links between the Policy requirements and SMS elements to show that the Policy was used as the basis for the framework of the SMS.
Maintained	Review/revise requirement up-to-date.

Safety Management System

Est. Requirement	Examples of Evidence
Available	Each SMS element has an assigned document number.

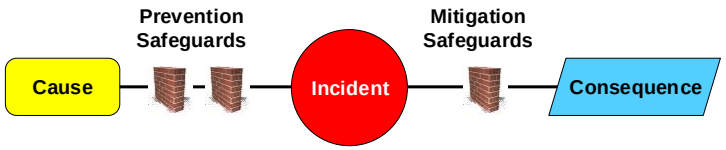
Imp. Requirement	Examples of Evidence
In Use	Reports, documents generated from using the SMS elements.
Comprehensive	It covers the requirements of the MA Prevention Policy.
People Trained	Included in documented training programs; training records.
Effective	KPIs assigned and monitored through reviews and audits.
Maintained	Assigned owner with periodic review/revise and audit records.

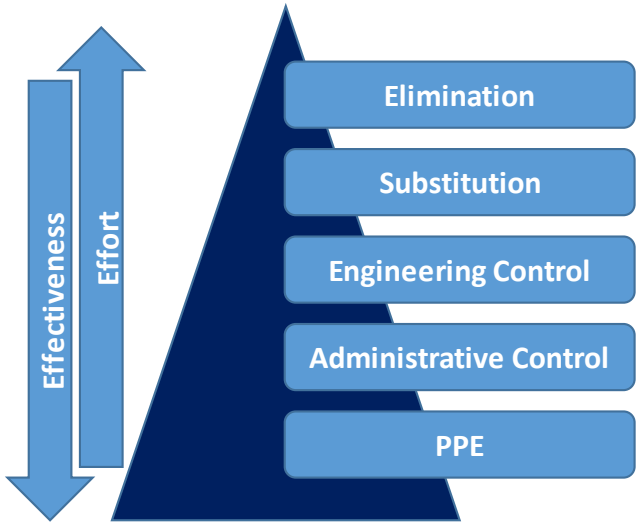
MA Hazards Identified

Requirement	Examples of Evidence
All MA Hazards Identified	The use of robust, systematic hazard identification process that is established, implemented and documented. E.g. HAZOP, that ▪ Examined all activities at the facility. ▪ Considered external threats, including neighbouring facilities. ▪ Considered incidents and data from similar facilities in industry. ▪ Provided justification for the rejection of potential MA scenarios. ▪ Comprehensively documented results.

MA Risk Eliminated

Requirement	Examples of Evidence
Risk of each MA Scenario Assessed	The results of a robust risk assessment process are available and show the consistent use of an appropriate risk assessment methodology.
Controls for each MA scenario identified.	Preventative and mitigative control measures have been documented for each MA scenario.
Hierarchy of controls has been considered	The rationale for selecting/rejecting risk control measures have been provided and documented.





MA Risk Reduced ALARP

Requirement	Examples of Evidence
Risk of each MA scenario reduced to ALARP	▪ Existing controls have been improved where practicable. ▪ Alternative/additional controls have been considered. ▪ A documented rationale for the rejection of any improved, alternative, or additional risk control measures. ▪ The improvements and/or additions have reduced risk to ALARP; or the effort and cost of reducing risk further is disproportionate to the benefit gained in risk reduction. ▪ Where improved, alternative, or additional risk control measures have been identified and accepted, but not yet implemented, a prioritised action plan is in place.

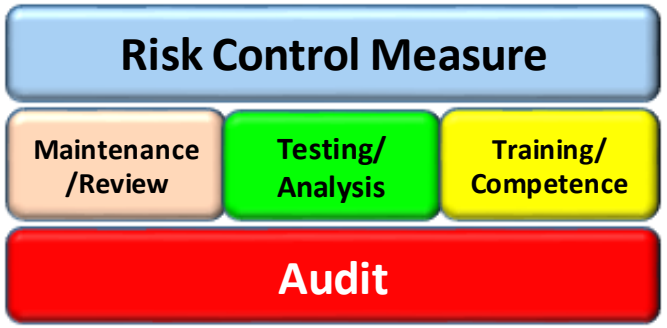
Safe and Reliable Design and Construction

Requirement	Examples of Evidence
Safe Design Safe Construction	▪ Applicable national and international codes and standards used as the minimum requirement. ▪ Revisions to codes and standards have been considered at the facility ▪ Requirements of codes and standards compared against the requirements of the facility. (Ethylene Oxide example)

Safe and Reliable Operation

Requirement	Examples of Evidence
Safe Operation Reliable Operation	▪ Operations personnel are trained and competent. ▪ Operational logs indicate the facility is operated within documented acceptable process limits. ▪ Results of investigations into any cases where the acceptable process limits have been breached. ▪ Historical data has been analysed for trends and to highlight potential weaknesses - alarms silenced and ignored, operator visual checks missed, shift logs incomplete, safety functions left in bypass, changing trip points without going through an MOC process.

Safe and Reliable Maintenance

Requirement	Examples of Evidence
Safe Maintenance Reliable Maintenance 	▪ Maintenance personnel are trained and competent. ▪ SMS elements drive maintenance activities. ▪ The type and frequency of maintenance (equipment), and the requirement for review (procedures and systems of work) must be documented and followed. ▪ The type and frequency of testing must be documented, and the results fully documented and analysed for trends.

Emergency Response Plan (ERP)

Requirement	Examples of Evidence
ERP Drawn Up	▪ ERP is available, and has an assigned document number.
ERP Takes Necessary Measures	▪ Covers all MA scenarios and considers manning levels and available equipment. ▪ Firefighting infrastructure is based on a comprehensive fire study. ▪ External threats (bombs, terrorists) are included. ▪ Emergency services are included in the planning and testing.

Demonstration by Example

Provide the demonstration by using one or more high-risk examples taken from the identified MA scenarios.

It is recommended that the examples be provided in a separate section of the SC

The body of the SC should already contains a detailed, but general description of each activity, and provide references to associated procedures and systems of work.

Having the examples in a separate section provides a better information flow in both the body of the SC and the demonstrations, and allows easier updates in future SCs.

What to Include in each Example

Each example should provide a flow from one activity to the next, by describing how the output from each activity is used in other activities, and together lead to the risk of the MA being reduced to ALARP.

For each activity:

- Provide a reference to the specific part of the procedure that states the requirements relevant to the example
- Highlight every decision point and rule set used in making the decision, and the outcome for the specific example.
- Provide a specific reference to the documented outcomes of each activity.

Example: Fuel Terminal – Storage Tank Overflow

SMS References

- Fictitious Risk Assessment Guide used in the example.
- All activities are linked to the specific requirements in the SMS element used.

Risk Assessment Team

- The most experienced personnel were used on the team.
- The name, discipline and position of team members listed in table.

Discipline	Name	Position
Facilitator		
Process		Senior Engineer
Operations		Supervisor
Maintenance		Supervisor
Health & Safety		H&S Representative

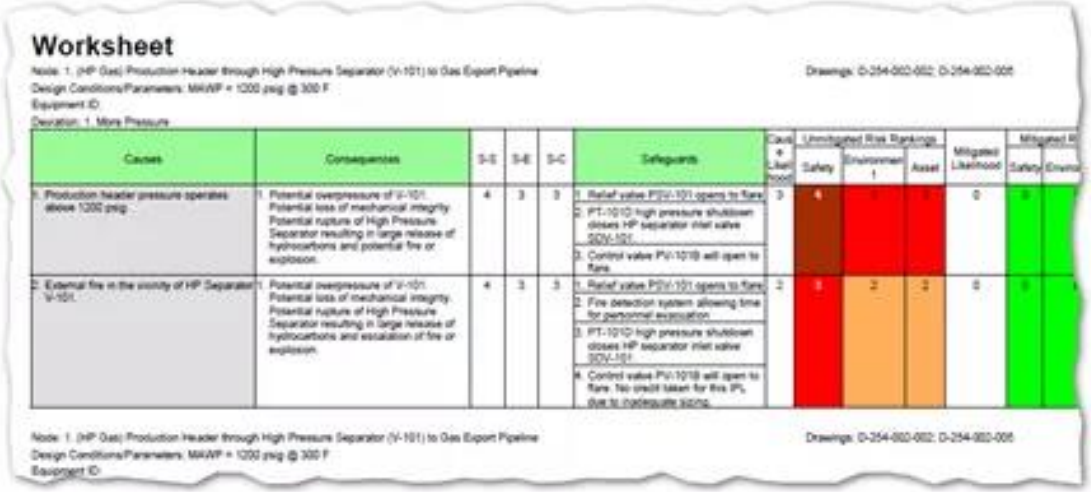
Example: Fuel Terminal – Storage Tank Overflow

HAZID/HAZOP

- The HAZOP results identified the overflow scenario with various causes.
- Considered facility knowledge, and industry information. Buncefield.

Bowtie

- The scenario was represented visually as a bowtie, showing causes, consequences and safeguards.
- Select scenario for storage tank overflow caused by level control failure



Worksheet

Node: 1. (HP Gas) Production Header through High Pressure Separator (V-101) to Gas Export Pipeline

Drawings: D-254-002-002; D-254-002-005

Design Conditions/Parameters: MAWP = 1200 psig @ 300 F

Equipment ID:

Deviation: 1. More Pressure

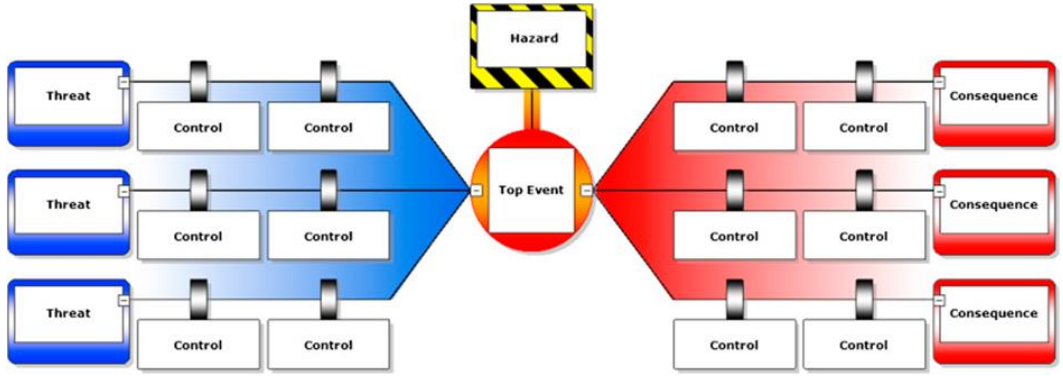
Causes	Consequences	S-E	S-E	S-C	Safeguards	Caus + Likelihood	Unmitigated Risk Rankings: Safety	Environment	Asset	Mitigated Likelihood	Mitigated R: Safety	Enviro
1. Production header pressure operates above 1200 psig	1. Potential overpressure of V-101. Potential loss of mechanical integrity. Potential rupture of High Pressure Separator resulting in large release of hydrocarbons and potential fire or explosion.	4	3	3	1. Relief valve PSV-101 opens to flare; 2. PT-1010 high pressure shutdown closes HP separator inlet valve SDV-101; 3. Control valve PV-1010 will open to flare	3	4	[illegible]	[illegible]	0	[illegible]	[illegible]
2. External fire in the vicinity of HP Separator V-101.	1. Potential overpressure of V-101. Potential loss of mechanical integrity. Potential rupture of High Pressure Separator resulting in large release of hydrocarbons and escalation of fire or explosion.	4	3	3	1. Relief valve PSV-101 opens to flare; 2. Fire detection system allowing time for personnel evacuation; 3. PT-1010 high pressure shutdown closes HP separator inlet valve SDV-101; 4. Control valve PV-1010 will open to flare. No credit taken for this IPL due to inadequate sizing	2	[illegible]	2	2	0	[illegible]	[illegible]

Node: 1. (HP Gas) Production Header through High Pressure Separator (V-101) to Gas Export Pipeline

Drawings: D-254-002-002; D-254-002-005

Design Conditions/Parameters: MAWP = 1200 psig @ 300 F

Equipment ID:



Safety Case Symposium 2018 Singapore

Example: Fuel Terminal – Storage Tank Overflow

Risk Ranking

- Risk ranking was determined by determining the consequence and likelihood. The results are shown on the risk matrix.

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Likelihood	Rare	Low	Low	Low	Medium	High
	Unlikely	Low	Low	Medium	Medium	High
	Moderate	Low	Medium	Medium	High	High
	Likely	Medium	Medium	High	High	High
	Very Likely	Medium	Medium	High	High	High

Identify MA Scenario

- Any risk ranking of **High**, or **Major** or **Extreme** consequence that involves Scheduled Materials is considered an MA, and further analysis is required.

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Likelihood	Rare	Low	Low	Low	Medium	High
	Unlikely	Low	Low	Medium	Medium	High
	Moderate	Low	Medium	Medium	High	High
	Likely	Medium	Medium	High	High	High
	Very Likely	Medium	Medium	High	High	High

Example: Fuel Terminal – Storage Tank Overflow

LOPA (further analysis)

- The LOPA study identified valid controls, and their performance.
- Achieved tolerable risk.

1	2	3	4	5	6	7	8	9	10	11
Impact Event	Severity Level	Initiating Event	Initiating Event Freq/year	Existing Layers of Protection (PFD)				Intermediate Event Likelihood	Tolerable Risk Likelihood	Risk Reduction Factor
				BPCS	Alarm & Operator Response	Other IPLs	Mitigation Measures			
Storage tank overflows and potential fire	High (fatality) Risk Ranking L: Likely C: Extreme	Level Control Failure	0.1	Failed 1.0	Independent High-Level Alarm 0.1	Independent High-High -Level Shutdown 0.01	Fire & Gas Detection plus Firewater System	1E-4	1E-4	0

ALARP

- Improved, alternate, and additional controls were considered. Reasons why they were accepted or rejected provided.
- Cost/Benefit analysis
- Controls not yet implemented were included in facility Action Plan.

Risk Control ID	Description	Accept/Reject	Comments
RCM #011	Improve performance of existing risk control measure (describe)	Accepted	Implemented under MOC (specific reference)
RCM #052	New high-high level control. Identified in Buncefield report.	Accepted	Listed as high priority in the facility Action Plan (specific reference)
	Additional risk control measure (describe)	Rejected	Not cost effective. See Cost/benefit Analysis in ALARP report (specific reference).
	Additional risk control measure (describe)	Rejected	Not feasible due to engineering restraints. See Engineering Analysis in ALARP report (specific reference).

Example: Fuel Terminal – Storage Tank Overflow

ERP

- The ERP includes the specific response to the example MA scenario. (If there is a generic response, the describe why the response is adequate for the MA Scenario).

Conclusion

- Summarise how the SMS elements worked together to identify MA scenarios, reduce risk to ALARP and maintain controls

Summary

- The best demonstration is evidence.
- Describe risk management activities in detail, and link to the relevant SMS elements.
- Make sure decision points and rule sets are explained.
- Provide worked examples of high-risk MA scenarios.

Demonstration of Adequacy

A Practical Guide

Raymond Wright

FSE Global Pte Ltd

Safety Case Symposium 2018 Singapore

www.SafetyCaseSymposium.com