Government of South Australia

Department for Energy and Mining

Energy Regulatory Guidelines

007

Process safety management framework for assessing compliance

Department for Energy and Mining
Level 4, 11 Waymouth Street, Adelaide SA 5000
GPO Box 618, Adelaide SA 5001

Phone +61 8 8463 3000
Email DEM.Engineering@sa.gov.au

www.energymining.sa.gov.au/industry/energy-resources

South Australian Resources Information Gateway (SARIG)
map.sarig.sa.gov.au

Energy Regulatory Guidelines 007

Cover. Moomba, Cooper Basin. (Courtesy of Santos Ltd; photo 043361)

Preferred way to cite this publication. Department for Energy and Mining 2024. *Process safety management framework for assessing compliance,* Energy Regulatory Guidelines 007. Department for Energy and Mining, South Australia, Adelaide.

Revision history

Date	Comment
September 2019	First published
February 2020	Table 1 functional competency elements updated to include their corresponding metrics.
August 2024	Updated for the Energy Resources Act 2000

Contents

Purpose

This guideline outlines the process safety management philosophy adopted by the Energy Regulation Branch within the Department for Energy and Mining (DEM) regarding its assessments of submissions made under relevant requirements of the Energy Resources Act 2000 and Energy Resources Regulations 2013. In particular, regulations 16A (management system elements), 30 (fitness-for-purpose assessments) and 32 (incident reports).

It makes clear how the outcomes from these assessments and other sources inform DEM's ongoing surveillance of regulated activities for compliance with the relevant statement of environmental objectives.

Context

Under section 87 of the Act, a licensee must carry out regulated activities in accordance with good practice as recognised in the relevant industry, and with due care for:

- the health and safety of persons who may be affected by those activities; and
- the environment; and
- the need to ensure, in a case where interruption of natural gas supply could cause significant social disruption, that the facilities for processing and transporting natural gas are designed, constructed and managed and operated on a prudential basis so as to provide a reliable and adequate supply of natural gas.

Licensees must also comply with the statement of environmental objectives relevant to the regulated activities that they are undertaking.

The Act and Regulations include mandatory requirements for assessment and reporting of compliance against these objectives, which inform DEM's surveillance. This guideline focuses on:

- Classification of activities to be conducted under licence (s. 74 and r. 17) which require an assessment of a licensee's management system (detailed in r. 16A) to determine whether a licensee can be classified as requiring low-level official surveillance. Specifically relevant is the licensee's adoption and implementation of an effective management system for identifying and maintaining effective controls for both the prevention of and mitigation of the consequences of potential hazardous events. See also *Guidelines on criteria used to classify level of licensee surveillance required*, Energy Regulatory Guidelines (ERG) 010 (PDF 1.7 MB).
- Fitness-for-purpose assessment (s. 86A and r. 30) which require licensees to

The Act defines the environment to include the natural environment; buildings, structures and cultural artefacts; productive capacity or potential; the external manifestations of social and economic life; and the amenity values of an area.

undertake an assessment of and submit a report on the fitness for purpose of their facilities and the associated management systems.

Namely, assessment of the fitness for purpose of the controls in place for both the prevention of and mitigation of the consequences of potential hazardous events. See also *Fitness-for-purpose assessment reporting guidelines*, ERG 008 (PDF 273 KB).

- Reporting on certain incidents (s. 85 and r. 32) which require reporting and investigation of reportable and immediately reportable incidents, as classified under the Act, including determination of the root causes of such incidents. This requires an assessment of the systemic causes resulting in the impairment of the controls in place. See also *Incident reporting guidance*, ERG 006 (PDF 3.6 MB).

To aid assessment of submissions and the development of DEM's surveillance strategies, in addition to other checklists in use, DEM has adopted the principles of process safety management. Bowtie methodology is being used to visualise line of sight between threat, event and consequence, together with associated controls in place for prevention and mitigation.

Process safety management

The interrelated elements of process safety management are summarised in Table 1. All these elements are essential to achieve successful process safety management, bringing together effective design, operational and technical integrity and the key interfaces of people, processes, and systems.

In summary, the four steps that DEM believes are necessary to deliver effective process safety management are:

1. Identify the potential hazardous events associated with one's activities.
2. Conduct a systematic risk assessment to ascertain the level of risk associated with such potential hazardous events (i.e. the likelihood of such hazardous events, and the potential consequences of any such events).
3. Identify and implement effective controls to reduce the likelihood of identified hazardous events and mitigate the severity of potential consequences of any such events.
4. Establish and implement an effective management system to maintain both the preventive and mitigative controls.

Underpinning these four steps is the need for a strong organisational culture, demonstrating leadership and responsibility that is essential for effective process safety management.

Table 1 *Functional competency elements of process safety*

Elements	Metrics
Knowledge and competence	Conformance with process safety related role competency requirement
Engineering and design	Deviations to safety critical elements (SCE)
	Short-term deviation to SCE
	Open management of change on SCEs
	Demand on SCE
	Barriers failing on demand
Systems and procedures	SCE inspections performed versus planned
	Barriers fail on test
	Damage to primary containment detected on test/inspection
	SCE maintenance deferrals (approved corrective maintenance deferrals following risk assessment)
	Temporary operating procedures open
	Permit to work checks performed to plan
	Permit to work non-conformance
	Number of process safety related emergency response drills to plan
Assurance	Number of process safety related audits to plan
	Number of non-conformances found in process safety audits
Human factors	Compliance with critical procedures by observation
	Critical alarms per operator hour (EEMUA 1999)
	Standing alarms (EEMUA 1999)
Culture	Open process safety items
	Number of process safety interactions that occur

Note: It could be argued that some of the metrics could be allocated to other elements as they cross over, however the table shows IChemE Safety Centre's consensus on the allocation.

EEMUA 1999. *191[1]: Alarm systems – A guide to design, management & procurement*. Engineering, Equipment and Materials Users Association, UK.

Source: IChemE 2015. *Lead process safety metrics – selecting, tracking and learning*, IChemE Safety Centre Guidance.

The bowtie method

Bowtie diagrams are widely regarded in industry as a useful visual tool to provide an overview of risk management practices, supplementing rather than replacing existing processes or systems. Given its applicability to a variety of processes and systems, the bowtie method is well suited to regulatory overview applications.

A bowtie diagram gives a visual summary of plausible accident scenarios that could exist around a certain hazard. By identifying control measures, the bowtie displays what is in place to control those scenarios.

Bowtie diagrams clearly display the links between the potential threats, prevention and mitigation controls and consequences of an unwanted event.

Figure 1 shows a simple bowtie diagram, where the hazard is 'operating oil and gas infrastructure' and the hazardous event is 'loss of containment'.

To the left of the hazardous event, threats are identified that could lead to this event occurring. Along this threat line, the controls (also known as barriers) in place to prevent the event are recognised. To the right of the hazardous event, potential consequences of the hazardous event are identified. Controls to mitigate these consequences are depicted along the relevant consequence lines.

However, controls are not always wholly effective and can be subject to escalation factors (also known as degradation factors or mechanisms). A more complex example of a threat depicted on a bowtie diagram is presented in the Appendix (corrosion under insulation).

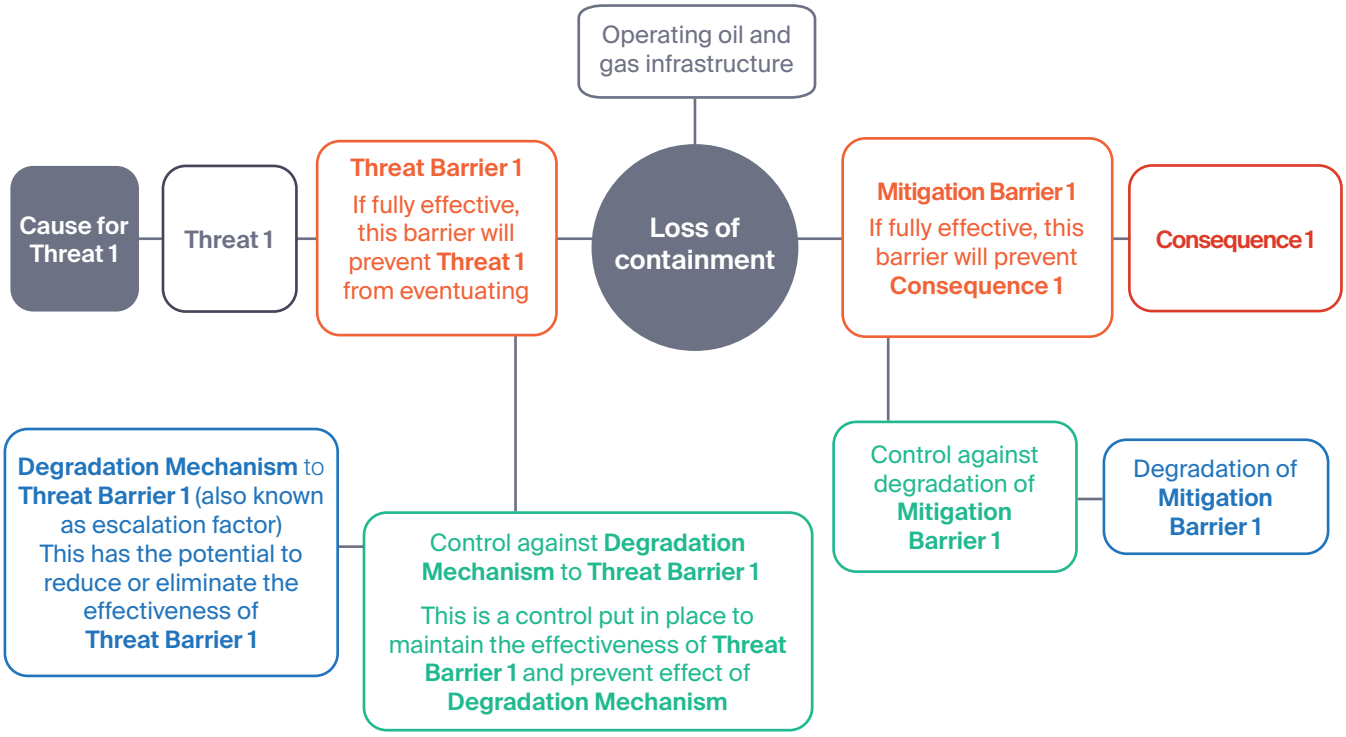


Figure 2 *Generic bowtie showing one threat line.*

Application of bowties to DEM's surveillance

To undertake effective, targeted surveillance, DEM focuses on controls critical to ensuring the achievement of compliance with the Act and the relevant statement of environmental objectives. When developing inspection programs, bowtie risk assessments can be used to identify which controls should be considered as critical.

DEM aims to ensure a clear line of sight between:

- threat being controlled
- relevant controls in place to prevent or avoid a hazardous event
- controls in place to mitigate the severity of the potential consequences of such an event.

Once the critical controls have been identified, DEM seeks evidence that associated performance standards are demonstrably articulated in accordance with recognised industry practice, namely:

- performance objective of the critical controls in question
- requirements of the critical control to deliver its objective
- how these requirements will be assured and verified.

Performance standards provide essential line of sight in demonstrating management of the effectiveness of critical controls, and hence the risk of hazardous events. Performance standards should have clear acceptance criteria and stated responsibilities in the event that a critical control is found not to be meeting this criteria.

Assessment of the performance of critical controls must also include a close examination of the systems, processes, procedures and personnel competencies that underpin the fitness for purpose of such controls.

Fitness-for-purpose assessments (s. 86A and r. 30)

Section 86A of the Act and regulation 30 require licensees to carry out a fitness-for-purpose assessment of their facilities at five-yearly intervals to assess the risks imposed by the facilities on public health and safety, the environment and the security of production or supply of natural gas. Section 86A(6) requires that any identified risks are eliminated or reduced so far as is reasonably practicable, and any remedial actions identified must be promptly carried out.

The fitness-for-purpose report should consider all credible threats to the design, operation and technical integrity of the asset. The report must be clear that these threats have been identified, recorded and are continuously being effectively managed.For additional guidance refer to *Fitness-for-purpose assessment reporting guidelines*, ERG 008 (PDF 273 kB).

Whilst provision of bowties from licensees is not mandatory in the fitness-for-purpose report, it is encouraged, and DEM will use the information provided to establish a line of sight through a bowtie analysis of the controls in place. This will also involve developing an understanding of the escalating factors (e.g. pressure safety valves becoming out of calibration, lack of training in the use of a critical procedure, excursions outside of the safe operating envelope) and the assurance or verification in place to ensure these controls will perform and continue to perform as required. The findings are used to inform ongoing surveillance conducted by DEM.

Management systems r. 16A

From a process safety management perspective, the requirements of the regulation 16 operator assessment factors are to demonstrate the effectiveness of the licensee's management systems for identifying and maintaining effective controls for both the prevention of and mitigation of the consequences of potential hazardous events.

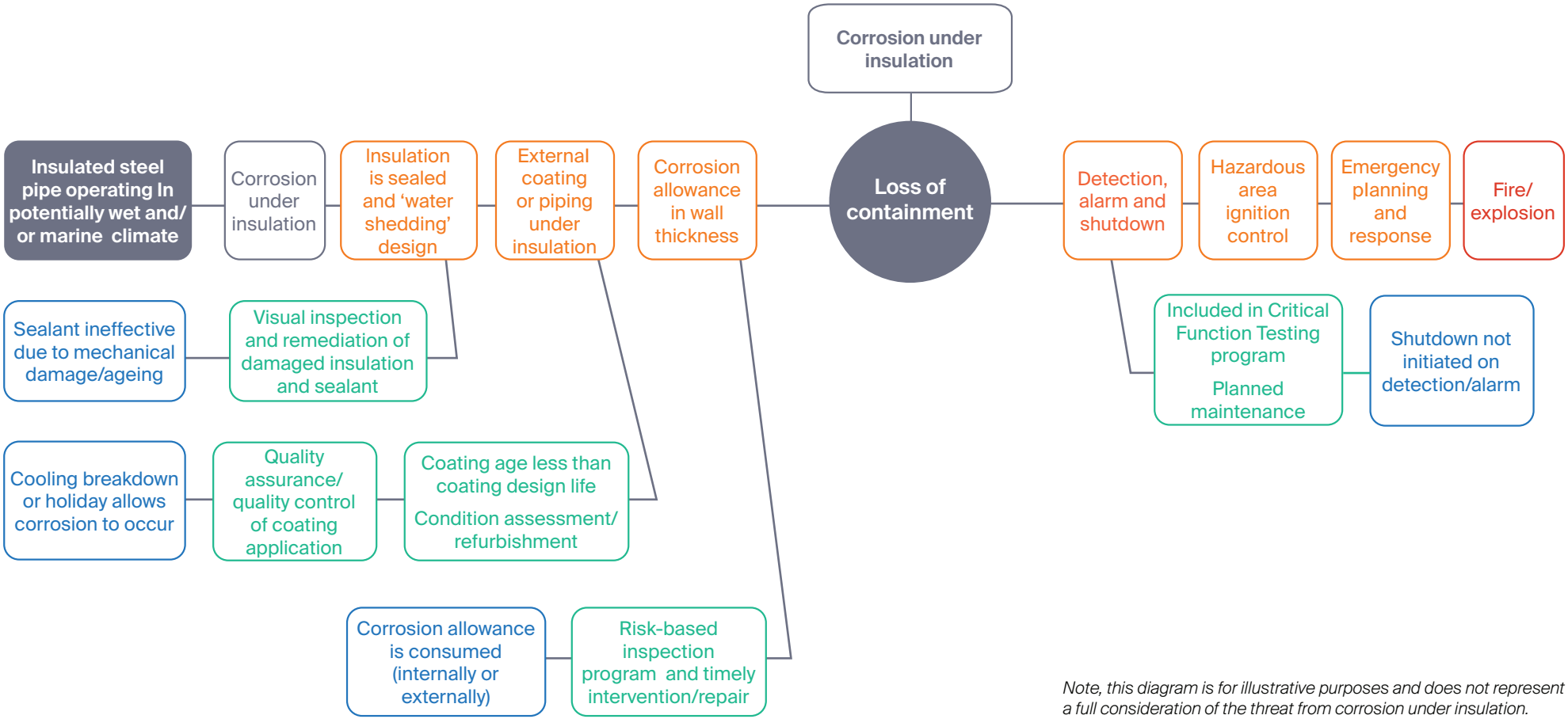
DEM uses the information provided in these submissions to establish a line of sight between the controls and the systems in place for maintaining the effectiveness of these controls. This is then used to inform follow up surveillance conducted by DEM.

For further detail on submission requirements for operator assessment factors refer to *Operator assessment factor reporting guidelines for high-level official surveillance activity notifications*, ERG 009 (PDF 2.0 MB) and *Guidelines on criteria used to classify level of licensee surveillance required*, ERG 010 (PDF 1.7 MB).

Incident reports (r. 32)

As outlined in regulation 32, the incident investigation must include an assessment of the effectiveness of the design, procedures and management systems that were in place to prevent the incident occurring. In the context of this guideline, using bowtie analysis for incident investigation is an effective means for establishing line of sight between the controls and the escalating factors which impaired those controls within which the root causal factors can be found. For a more detailed description of the use of root causal analysis for this purpose see Appendix 1 in DEM's *Incident reporting guidance note,* ERG 006 (PDF 3.6 MB).

APPENDIX Demonstration of corrosion under insulation on a bowtie diagram



Note, this diagram is for illustrative purposes and does not represent a full consideration of the threat from corrosion under insulation.

Shortened forms

DEM Department for Energy and Mining

Glossary

Definitions of key terms for the purpose of this document.

Consequence. An effect on people, the environment or security of supply as a result of a hazardous event occurring. It is the ultimate credible harm that may occur as a result of a hazardous event.

Control. Prevent or reduce the probability of a threat from causing an event (left hand side of the bowtie) and limit the extent of, or provide immediate recovery from the consequences (right hand side of the bowtie). A control may be hardware, procedural or system, human intervention, or a combination of these.

Critical control. Crucial to preventing a hazardous event or mitigating the consequences of a hazardous event. The absence or failure of a critical control would significantly increase the risk despite the existence of the other controls. Each critical control should have an associated performance standard.

Environment. The *Energy Resources Act 2000* defines the environment to include—

(a) land, air water (including both surface and underground water and sea water), organisms, ecosystems, flora, and fauna; and
(b) buildings, structures and other forms of infrastructure and cultural artefacts; and
(c) existing and potential land use; and
(d) public health, safety, or amenity; and
(e) the heritage, aesthetic, or cultural values of an area; and
(f) the economic or social impact on an area

Escalation factors. Situations, conditions or circumstances that defeat, degrade, impair or reduce the effectiveness of a control.

Hazard. An activity with the potential to result in a hazardous event.

Hazardous event. An event that has the potential to result in:

- one or more fatalities or severe injuries
- extensive damage to structure, installation or plant
- large-scale, severe and/or persistent impact on the environment
- interruption of natural gas supply.

Human factors. All the interactions of individuals with each other, with facilities and equipment, and with management systems used in their working environment.

Management system elements. Underlying processes and practices designed to prevent hazardous events and mitigate any potential consequences of such events. Management system elements support controls.

Performance standard. Measurable criteria, expressed in qualitative or quantitative terms, of the performance required of a system, equipment item, person or procedure that may be part or all of a control.

Process safety management. Focuses on the management of high-consequence, low-probability events by maintaining the integrity of plant, equipment and operating systems through the application of inherently safe design principles and safe operating practices.

Threat. The occurrence (condition, situation, phenomenon or event) which will, if left unmanaged, cause a hazardous event.

Verification. The process of checking the extent to which the performance requirements set for a control are being met in practice. Verification activities may include audit, review and monitoring.

ACKNOWLEDGEMENT OF COUNTRY

As guests on Aboriginal land, the Department for Energy and Mining (DEM) acknowledges everything this department does impacts on Aboriginal country, the sea, the sky, its people, and the spiritual and cultural connections which have existed since the first sunrise. Our responsibility is to share our collective knowledge, recognise a difficult history, respect the relationships made over time, and create a stronger future. We are ready to walk, learn and work together.

FURTHER INFORMATION

Department for Energy and Mining
Level 4, 11 Waymouth Street, Adelaide
GPO Box 618, Adelaide SA 5001
T **+61 8 8463 3000**
E **DEM.Engineering@sa.gov.au**
www.energymining.sa.gov.au

SOUTH AUSTRALIA

Government of South Australia
Department for Energy and Mining

16/08/2024-205237