NOPSEMA
Australia's offshore energy regulator

INFORMATION PAPER

Risk migration

Document No: N-06300-IP1771 A599510

Date: 27/05/2022

Key messages

- Learning from accidents and other hazardous events (e.g. near misses) has historically been a focus of safety improvement efforts.
- There has been increasing attention paid to the idea of learning from successes as a means of improving safety outcomes.
- Accident and hazardous event investigations often identify individual actions as causal factors, particularly when those actions are contrary to procedures. However, those same actions are often ones that may enable work to succeed in meeting productivity and economic goals. Breaches of procedures may be seen by individuals as justified, particularly if there are no immediate and visible adverse safety consequences.
- By understanding how people adapt to local and temporal factors to balance competing goals, organisations can guide adaptations in a way that maintains rather than erodes safety margins.
- A case study is presented to explore these concepts.

Table of Contents

Key definitions for this information paper

The following are some useful definitions for terms used in this information paper. They are a suggested starting point only and are not prescriptively defined, unless otherwise indicated.

Decrementalism	A negative shift away from an established safe standard through incremental steps.
Hazardous event	A collective term encompassing safety, integrity, and environmental incidents, used for readability purposes within this information paper.
Human error	Failure of a planned action to achieve a desired outcome.
Incubation period	The accumulation of an unnoticed set of events which are at odds with the accepted beliefs about hazards and the norms for their avoidance (Turner & Pidgeon, 1997).
Risk migration	An unseen increase in risk related to a hazard over time due to operational decisions that attempt to balance safety, economic and workload goals
Sociotechnical work systems	Hierarchies of interconnected levels, where individual decisions and actions dynamically influence and impact an entire system through controls and feedback (Rasmussen, 1997)
Weak signals	Small anomalies that appear innocuous but may be indicative of impending problems. They are easily dismissed and may be so subtle that their significance becomes apparent only in hindsight.

Abbreviations

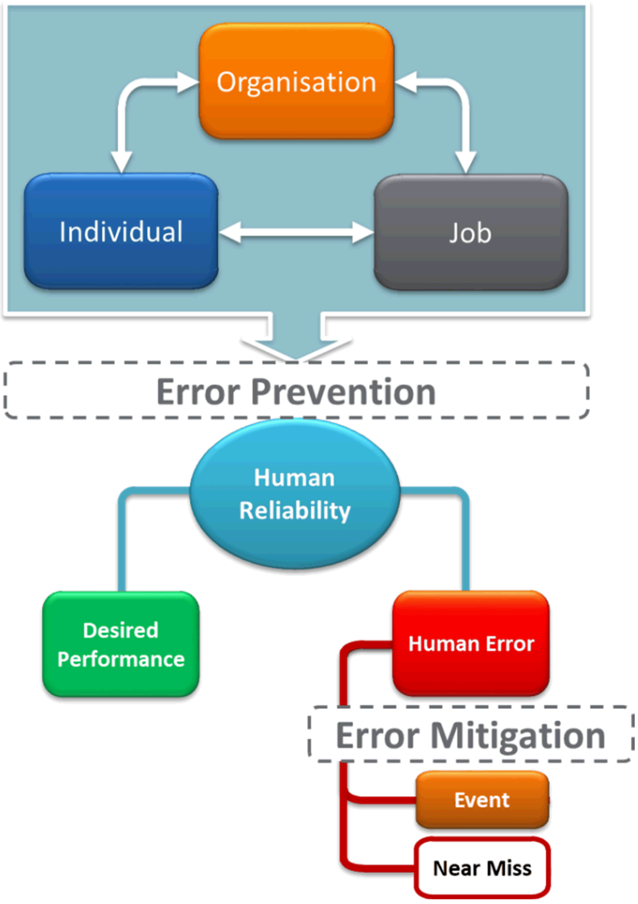
ALARP	As Low as Reasonably Practicable
HAZID	Hazard Identification study
HAZOP	Hazard and Operability study
MAE	Major Accident Event
MODU	Mobile Offshore Drilling Unit
NOPSEMA	National Offshore Petroleum Safety and Environmental Management Authority
P&ID	Piping and Instrumentation Diagram
SMS	Safety Management System

1. Introduction to the human factors information paper series

Human error has long been identified as a contributing factor to incident causation. Commonly cited statistics claim that human error is responsible for anywhere between 70-100% of incidents (e.g. Rasmussen, 1997). It may seem logical, therefore, to blame incidents on individuals or small groups of people and to focus remedial actions at the individual level (e.g. training, disciplinary action, etc.). However, by taking this approach in addressing human error, organisations ignore the latent conditions in their work systems that contribute to human error across the workforce. Rather, human error should be recognised as an outcome of combined factors, instead of the root cause of an incident. Organisational, job, and individual factors all interact to influence human reliability, that is, the likelihood that an individual will perform their task effectively or experience error.

This publication forms part of a series of information papers focusing on human factors. NOPSEMA defines human factors as "the ways in which the organisation, the job, and the individual interact to influence human reliability in hazardous event causation". Generally, reliable behaviour results in desired performance, while unreliable behaviour may result in human error, which can lead to hazardous events and dangerous occurrences (sometimes referred to as near misses). This interaction is represented in Figure 1.

Figure 1 - A model of human factors



The Human Factors Information Paper Series is designed to provide information about the ways in which organisational, individual, and job factors influence human reliability, and how organisations can minimise or optimise the effect of these factors to assist in the prevention and mitigation of hazardous events and drive continuous improvement in safety, integrity and environmental performance.

1.1. Intent and purpose of this information paper

There is a long history of learning from accidents and hazardous events in safety-critical industries including the offshore petroleum industry. However, there has also been increasing focus on understanding how work is performed successfully as an important means of improving safety outcomes. It has been suggested that retrospective accident and hazardous event investigation as a means of predicting future accidents is limited because systems are rarely, if ever, static (Leveson, 2011). Reliance on retrospective analysis has been found to contribute to accidents because the planning process relies on past failures to identify potential failures and is often unable to imagine failure pathways that have not happened before. This problem becomes increasingly relevant as new technologies are introduced into the sociotechnical work system. This does not mean that retrospective analysis is not useful, but it does suggest that proactive analysis will become increasingly important over time.

Within complex sociotechnical work systems, actions classified as "procedure non-compliance" contributing to accidents are often the same actions that usually enable work to succeed (Hollnagel, 2009). By understanding how people adapt to local and temporal factors to balance competing goals, organisations can attempt to guide adaptations in a way that maintains rather than erodes safety margins. This information paper uses a case study[1] as an example of an arguably successful operational adaptation that could have preceded a major accident event (MAE). A systems theory framework is used to provide possible explanations for the problem-solving decisions that were made in the case study. *These are possible explanations only and should not be taken as verified findings.*

Please note: Information papers provide information, background, and practices to foster continuous improvement within industry. NOPSEMA acknowledges that what is good practice, and what approaches are valid and viable, will vary according to the nature of different organisations, offshore facilities and their hazards.

2. Case Study – offshore personnel exposed to hydrocarbon gas

2.1. Information established by NOPSEMA

A Mobile Offshore Drilling Unit (MODU) operator was engaged by a titleholder for a well abandonment campaign. During an inspection, NOPSEMA inspectors (the inspectors) noted a controlled gas venting activity recorded on the operator's daily drilling report.

Subsequent discussions confirmed that hydrocarbon gas venting activities were conducted at the facility and that hydrocarbon gases had been discharged via the fluids handling package through the facility's overboard vent lines into areas that presented risks to personnel on board the facility, including in proximity to the engine room air intakes. This was notable because gas venting activities were not described in the facility safety case and this hydrocarbon gas venting had not been notified to NOPSEMA as a dangerous occurrence.

The drilling reports showed that hydrocarbon gas was discharged through the same venting arrangements on at least four well abandonments over a two-month period. The fluids handling package was then

[1] All of the findings described have been addressed in accordance with NOPSEMA's inspection and enforcement policies and procedures.

modified to divert through the mud gas separator vent line. The modification works were completed without safe work practices such as non-destructive testing of welds and pressure testing.

The fluids handling package had been specified assuming only minimal residual hydrocarbons in the wells. Potential new sources of hydrocarbon hazards for the campaign had been assessed as “not credible” during HAZOP and HAZID studies, leading to the classification of the activities related to the fluids handling package as non-hazardous area related and therefore there were no associated MAEs identified. Consequently, the fluids handling package was not deemed “safety-critical” and was therefore excluded from the scope of validation. Because of this, the modifications to the fluids handling package were not subject to adequate risk assessment or independent validation.

The titleholder had engaged a third-party equipment provider for the work campaign. The inspection found that periodic inspection, testing, and certification for the third-party equipment, as required by the relevant standards, had not been performed for some safety-critical third-party equipment including the surge tank, surface safety valve, high pressure hose, and high-pressure pipework. The titleholder’s personnel involved in the quality assurance of the equipment had recognised that these requirements had not been met and had applied a dispensation to avoid delays in the equipment load-out and campaign process.

The inspection found that hydrocarbon gases in quantities significantly greater than had been described in the safety case (and analysed in the formal safety assessment) had been discharged into areas that presented risks to personnel. Risks associated with these gas venting activities had not been identified or analysed as an MAE risk within the formal safety assessment, and adequate risk controls had not been put in place. The inspectors concluded that senior facility supervisors and operations personnel failed to recognise:

- the risk posed by venting the gas into areas in proximity to the engine room air intakes
- the significant change in risk profile from the first well where this equipment was utilised
- the need to stop work and re-assess the risk.

2.2. Why was NOPSEMA concerned?

The case study above describes a series of decisions and actions that served to degrade the layered defences established to protect personnel working at the facility. However, from a traditional lagging indicator perspective, *nothing went wrong*. There were no deaths or injuries. There was no ignition or damage to equipment. The problem-solving actions taken by senior facility supervisors and operations personnel could be argued to have worked, evidenced by the absence of adverse safety consequences and achievement of operational milestone targets. Had the regulator not intervened, the campaign may have been deemed a success and the problem-solving actions commended and reinforced within the titleholder’s and operator’s organisations.

Despite the absence of adverse safety consequence, this case study is representative of a precursor event. Critical control measures had failed before the campaign had commenced, in particular the HAZOP and HAZID studies that set the foundations for how risk would be managed throughout the campaign, and the quality assurance processes involved in accepting the third-party equipment. Then, during the campaign, defined operational boundaries were exceeded when the volume of hydrocarbons was found to be significantly greater than predicted. These boundaries were set by the operator and described in the facility safety case, yet the facility leadership team involved in the problem-solving process did not appear to recognise that the boundaries had been exceeded. These findings can be viewed as indicators of systematic erosion of the layered defences established through the safety management system.

3. Risk migration

Sociotechnical systems perspectives view accidents as the result of complex interactions between elements or components of the total system. Theory development and research in this field has been progressing for the past 40 years, and while a range of accident causation models have emerged, they all have ideas in common. The case study summarised above will be discussed in relation to relevant systems thinking tenets (Grant et al. 2018) to describe the concept of risk migration. As mentioned above, this discussion provides *possible* explanations for the decisions that were made in the case study, using a systems theory framework. These possible explanations should not be taken as verified findings.

3.1. Constraints

Offshore petroleum organisations operate in a competitive global commercial environment with limited resources. Within this environment, economic, workload, and safety constraints create boundaries to productivity. Drivers to improve productivity place pressure on economic, workload and safety constraints, creating incompatible goals (e.g. "faster, cheaper, better").

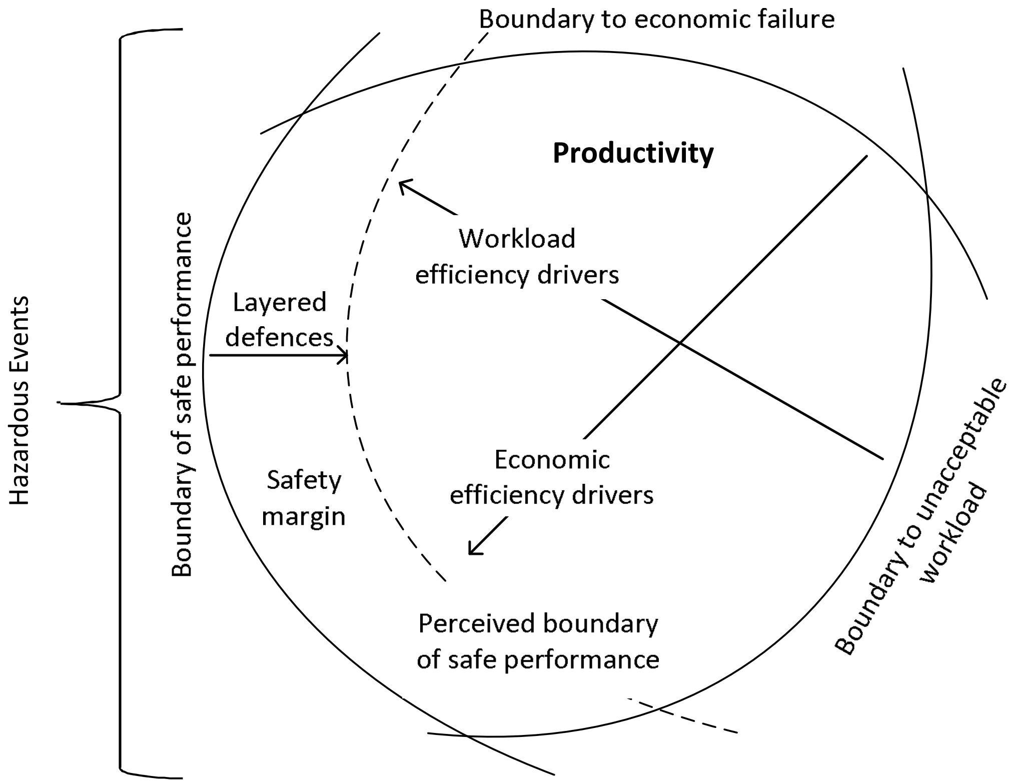
Economic and workload constraints may have influenced the decision to proceed despite the significant increase in risk. Stopping the campaign to undertake appropriate assessment and remediation activities would have a certain, immediate, and measurable impact on the campaign timeline and costs associated with drilling contractor and third-party equipment provider rates. An extension to the duration of the campaign may have delayed commencement of future campaigns for both the drilling contractor and the provider of the fluids handling package, which could result in reputational damage and financial losses or penalties for either or both parties. For the titleholder, delays to the well abandonment campaign would increase expenditure with no potential to recoup any losses.

For operations to proceed, individuals at all levels of the organisation engage in a constant, often subconscious, process of negotiation and trade-off between economic, workload, and safety goals. These trade-off decisions are also known as performance variability.

3.2. Performance variability

This process of ongoing trade-offs can lead to an erosion of safety margins, as illustrated in Figure 2, where gradients associated with drivers of workload and economic efficiencies create a systematic migration towards the boundary of safe performance, beyond which a hazardous event may occur.

Figure 2 - Migration model



Adapted from Rasmussen (1997)

Layered defences create the safety margin between the actual and perceived boundaries of safe performance. The layered approach is used to ensure that a single failure of a control measure does not lead to a hazardous event. However, the existence of these layered defences also means that deterioration of individual control measures may have no immediate or obvious effect and may not be visible to people operating within the system.

Personnel engaged in the campaign work at the facility may not have known that the periodic inspection, testing, and certification of some of the third-party equipment had not been conducted. Their decision to use the fluid handling package to discharge the excess hydrocarbons may have been made under the assumption that the equipment had been tested and certified and was therefore able to contain the pressure introduced by the excess hydrocarbons.

Trade-offs are necessarily made between costs, returns and risks to ensure the survival of the commercial endeavour. However, a feedback imbalance exists between these trade-offs. The economic or workload consequences of a trade-off decision are measurable, relatively immediate, and tangible. The safety consequences of such decisions, however, are not always obvious or measurable, particularly if there is no immediate observable effect.

Thus, over time layered defences can experience systematic degradation, as individual decisions meet workload and economic drivers with no observable impact on safety boundaries. In this manner, the safety margin is gradually encroached upon during what is known as an *incubation period*, and organisations move closer to the boundary of safe performance. This migration often occurs so gradually that it is difficult for members of the organisation to identify and reflects a pattern of decision-making known as *decrementalism*.

3.3. Decrementalism

Decrementalism refers to a shift away from an established safe standard through incremental steps. Personnel engage in continuous internal negotiation between incompatible goals, making trade-offs between costs, values, and risks. Such trade-offs are made in the face of uncertainty, risk, and constrained resources, in the knowledge that there is no risk-free option. This process is known as the efficiency-thoroughness trade-off principle (Hollnagel, 2009). When a slight departure from an established safe standard is 'successful' (i.e. an economic or workload goal is met without an obvious impact to safety), a new norm is created and used as the basis from which to depart slightly again. The incremental nature of each departure makes it unremarkable and unreportable at the time and so, over time, the distance between the original established safe standard and the current 'safe' norm increases, and safety margins are eroded. Signs of potential danger are acknowledged and then rationalised and normalised, allowing continued operation under degraded conditions that have been re-classified as 'safe'. This process is repeated in the face of worsening signs of danger, resulting in incremental steps toward greater risk.

When the unexpected volume of hydrocarbon gas was first discovered, there were very clear schedule goals that would be significantly impacted should work be stopped. However, if the campaign were to continue, operations would move beyond the perceived boundary of safe performance (see Figure 2*). This goal conflict was negotiated and resolved in a trade-off decision to close the engine room air intakes and choke the gas to minimise the volume released. This strategy, having resulted in no adverse consequence, appears to have been considered successful and was then repeated on four other wells during the campaign, suggesting that a new informal norm for safe operation had been created.*

However, trade-off decisions are not limited to operational activities. Trade-off decisions made during planning and risk assessment activities may occur years before they have an operational impact and may only become apparent through their interactions with other trade-off decisions. As layered defences become more complex, the safety system also becomes more opaque, obscuring the line-of-sight to operational hazard control.

3.4. Contribution of the protective structure

The process of reducing risk to a level that is ALARP involves the creation of a protective structure whose function is to prevent failure. In the offshore petroleum industry, as in most high-hazard industries, the primary framework for the protective structure is the safety management system (SMS) as required by the regulations, and as described in the safety case. The elements of the SMS are subject to interactions and interdependencies with operations. These interactions and interdependencies are often unexpected and unplanned, poorly understood, difficult to monitor, and impossible to fully control, to such an extent that the protective structure can actively facilitate risk migration. Being aware of the potential for risk migration during the application of risk assessment and management of change processes will minimise undermining of the protective structure.

During project planning, assumptions were made about the volume of hydrocarbons likely to be present in the wells. The actual volume present in the wells was significantly greater than the HAZOP and HAZID studies had anticipated, while the possibility of this eventuality had been considered and assessed as "not credible". The assumptions about likely hydrocarbon volumes drove the design of the fluids handling package, which was ultimately incapable of safely dealing with the volume of gas encountered within the wells. New information about the volume of hydrocarbons in the wells was an indicator of increased risk. However, decision-makers instead viewed the new information as a problem that could be solved using a relatively routine operation that would not disrupt the overall campaign. By responding to the increased volume of gas in this manner, decision-makers were able to retain their belief that the wells were understood and controllable, and that the campaign could continue safely.

After gas was observed in the sixth well of the campaign, a decision was made to modify the fluids handling package to divert the gas to the mud gas separator vent line. The project planning assumptions about gas volumes had justified the exclusion of the fluids handling package from the scope of validation. The exclusion from the scope of validation allowed modifications to the fluids handling package to proceed without independent oversight, without adequate risk assessment, and in the absence of critical safe work practices.

Protective structures were invoked to facilitate this decision, including a documented and approved Management of Change process, revisions to the P&ID, and HAZOP and HAZID studies. The use of these protective structures generated confidence in the solution proposed, while obscuring the risk posed by the poor-quality risk assessment, lack of independent validation, and inappropriate work practices undertaken during the modification works.

4. Toward safer trade-off decisions

Trade-off decisions are normal and adaptive. Variability is to be expected as individuals grapple with the goal conflicts confronting them daily. Variability becomes problematic when it occurs at the edge of, or beyond, the perceived boundary of safe performance (see Figure 2). Rather than focusing on the performance variability of an individual which happens to coincide with a hazardous event, organisations should seek to better understand and monitor trade-off decisions, identify where they are beneficial and where not, use them to drive learning and change within the sociotechnical system, and develop strategies to support safer adaptations.

4.1. Guided adaptability

Guided adaptability (Provan, et al., 2020) provides a model by which organisations can maintain awareness of, and learn from, local variability and can provide support and facilitation to guide variability in a safer direction. Organisations seeking to create guided adaptability for safety should develop their capacity for anticipation, readiness to respond, synchronisation, and proactive learning.

Anticipation creates foresight about possible future conditions and applies that foresight to review models of risk and approaches to control. To guide adaptability in a safer direction, the organisation needs to be able to anticipate potential failure paths and use those predictions to inform trade-off decisions. Such scenario planning involves the identification and monitoring of conditions or threats that have the potential to contribute to adverse scenarios, and the development of appropriate responses to those conditions and threats when they emerge.

Readiness to respond involves reserving resources that can be rapidly deployed in response to demand. Following on from anticipation, recognising that additional foreseen and unforeseen circumstances or demands can arise, the organisation should maintain flexibility in its capacities and resources. This flexibility allows for adaptation in response to local conditions, absorbing or dampening the impact of disruptions by relaxing efficiency drivers in favour of risk reduction, when operations are approaching the boundary of safe performance.

Synchronisation is a coordinated flow of information and action across the sociotechnical system. Where synchronisation is established, information exchange occurs freely within the organisation (between internal organisational silos) and between the organisation and external parties such as suppliers, contractors, and regulators. This information exchange allows for efficient and effective identification of, and response to, emerging issues.

Proactive learning involves active searching for brittle systems of work, gaps in knowledge, trade-off decisions, and changing priorities. Organisations monitor adaptive cycles of work when they engage in an ongoing iterative process of understanding and then improving how work is performed. Through the process of understanding how work is performed, organisations can recognise brittle operations and identify where action is required to maintain safety margins. This process builds a system that supports successful frontline adaptation.

4.1.1. Guided adaptability applied to the case study

How might 'guided adaptability' practices have altered the events of the case study?

The potential for new sources of hydrocarbon was considered during HAZOP and HAZID studies. Although assessed as "not credible" during the studies, this is understood to be relatively common during well abandonment and therefore a plausible threat.

An organisation practicing ***anticipation*** *may have considered new sources of hydrocarbon as a potential failure path and planned a response should excess hydrocarbons be identified.*

An organisation practicing ***synchronisation*** *may have prioritised involvement of the titleholder, drilling contractor, and third-party equipment provider during the HAZOP & HAZID studies. Such involvement would likely have generated a more accurate assessment of the hydrocarbon hazard and influenced the subsequent rating of the fluids handling package. This may have led the operator to generate comprehensive contingency plans describing how operations would respond to various unexpected but possible scenarios.*

Upon identification of excess hydrocarbons, a ***synchronised*** *organisation could have communicated with the regulator to assist in determining whether their operations and proposed solutions were outside of the safety margin defined in the safety case. While an adaptive response decision was made by field-based leaders, the sacrifice judgement was made in a way that maintained the efficiency drivers and relaxed the safety constraints so that operations were proceeding at the boundary of safe performance.*

An organisation practicing ***readiness to respond*** *may have assigned field-based safety personnel to guide adaptive response decisions. When it became clear that an adaptation was necessary, the field safety function could provide oversight to ensure that the adaptation decisions did not push operations past the boundary of safe performance and could have instead given preference to adaptations that maintain the safety margin. The effectiveness of this type of safety function would in most cases require a reporting line that is independent of operations.*

After the first well was found to contain excess hydrocarbons, an organisation engaged in ***proactive learning*** *in their monitoring of field-based adaptations may have recognised that the adaptation taken at the time, while successful from a lagging indicator perspective, was encroaching on safety margins. Steps could have been taken to facilitate an inquiry with the front line to understand what needs to be learned and changed within the sociotechnical system, including HAZOP and HAZID assumptions, third party equipment design decisions, and campaign timelines.*

References, acknowledgments & notes

Grant, E., Salmon, P., Stevens, N. J., Goode, N., & Read, G. J. (2018). Back to the future: What do accident causation models tell us about accident prediction? *Safety Science, 104*, 99-109. Retrieved from: **https://www.researchgate.net/publication/322537216_Back_to_the_future_What_do_accident_causation_models_tell_us_about_accident_prediction**

Hollnagel, E. (2009). The ETTO principle: Efficiency-thoroughness trade-off. Why things that go right sometimes go wrong. Farnham, UK: Ashgate.

n Leveson, N. G. (2011). Applying systems thinking to analyse and learn from events. *Safety Science, 49*, 55-64. Retrieved from: **https://dspace.mit.edu/handle/1721.1/108102**

Provan, D. J., Woods, D. D., Dekker, S. W. A., & Rae, A. J. (2020). Safety II professionals: How resilience engineering can transform safety practice. *Reliability Engineering and System Safety, 195,* 106740. Retrieved from: **https://www.sciencedirect.com/science/article/pii/S0951832018309864?via%3Dihub**

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science, 27*(2), 183-213. Retrieved from: **http://sunnyday.mit.edu/16.863/rasmussen-safetyscience.pdf**

Turner, B. A. & Pidgeon, N. F. (1997). *Man Made Disasters (2nd Edition)*. Oxford: Butterworth Heinemann.

Note: All regulatory references contained within this Information Paper are from the Commonwealth *Offshore Petroleum and Greenhouse Gas Storage Act 2006* and the associated Commonwealth regulations. For facilities located in designated coastal waters, please refer to the relevant State or Northern Territory *Petroleum (Submerged Lands) Act 1982* and the associated regulations.

For more information regarding this information paper, contact the National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA):

- Telephone: +61 (0)8 6188 8700, or
- e-mail: information@nopsema.gov.au.