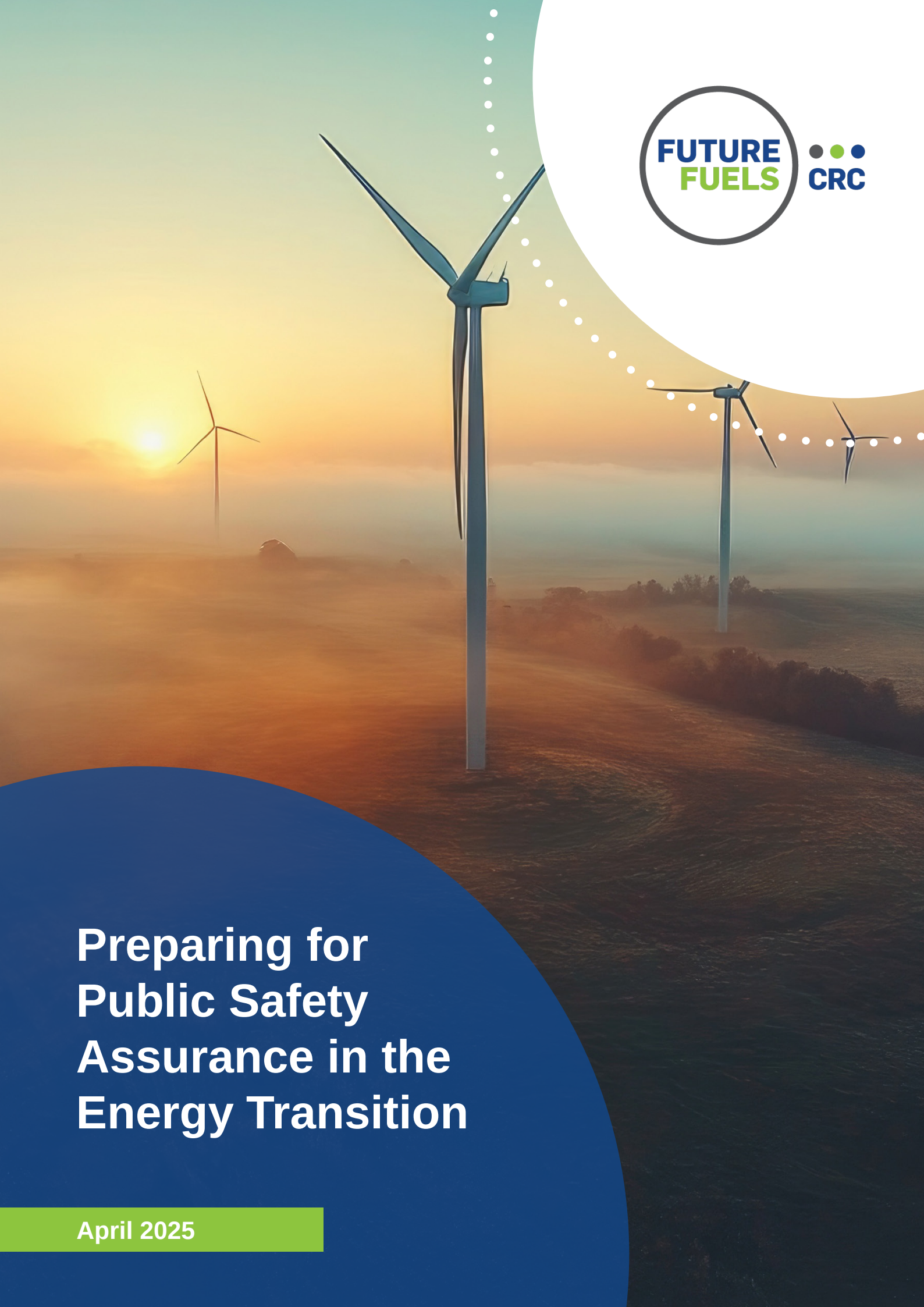


FUTURE FUELS CRC

Preparing for Public Safety Assurance in the Energy Transition

April 2025

Foreword

Craig Clarke
Manager Infrastructure Transformation, Energy Solutions APA

The Critical Need for Industry to Recognize and Address Sociotechnical Risk in the Energy Transition

The energy industry is in a period of transformation, shifting from fossil fuels to sustainable alternatives. This transition presents complex challenges that extend beyond technology. This booklet emphasizes the critical need for the industry to recognize and address the sociotechnical risks inherent in this shift.

- **Sociotechnical risks are multifaceted:** They involve social, organizational, technical, epistemic, and cultural factors that can impact the safety and success of the energy transition.
- **Proactive risk management is essential:** Strategies to identify and mitigate these risks are crucial for a smooth and safe transition.
- **SOTEC framework as a key tool:** The SOTEC framework provides a structured approach to identify, assess, and manage sociotechnical risks, ensuring a holistic and effective risk management process.

The industry must not neglect existing infrastructure. Condition uncertainties in existing facilities can lead to significant problems when repurposing them for new energy solutions.

The energy transition is a sociotechnical undertaking that demands a holistic approach. By recognizing and addressing the multifaceted risks involved, and by implementing frameworks such as SOTEC, the industry can ensure a safe, efficient, and publicly accepted transition to a sustainable energy future.

Foreword

Michael Malavazos
Director Energy Regulation
Department for Energy and Mining

History tells us that the potential for unforeseen hazards and consequences remains a challenge in a pursuit to adopt new technologies without careful testing and responsible management at the deployment stage. This research is a timely reminder of this, analysing experiences from other industries such as Chernobyl, the Titan submersible and space shuttle Challenger. The report draws some social, institutional, organizational and systemic parallels faced in a new world of energy transition, particularly large-scale hydrogen production, storage and transport – and possibly nuclear. Skills and technology are often argued to be transferable between existing and emerging industries, however, this research suggests to me that this could be a convenient assumption blinded by social, political and organizational demands to appease a real or perceived pressing urgency. The reality is that existing expertise is a great starting point, but new skills and knowledge must also be cultivated. Equally, new technologies can bring pre-existing latent systemic weaknesses to the fore in unexpected ways. In the risk based/ safety case regulatory regime under which Australia operates, regulatory focus is on the organizational and systemic factors that create the operational conditions to ensure the safe and competent deployment of technology and good recognized practices. Hence, an understanding of the sources of sociotechnical risk outlined in this research is an essential element of such a regulatory focus.

Table of Contents


Swagelok
INCREASE (+)
DECREASE (-)
Hydrogen

How to use this guide

This guide on preparing for public safety assurance in the energy transition is designed for the gas sector to use in preparing for a safe transition to decarbonised energy production and delivery. It is presented in two parts.

The first part of the guide introduces the SOTEC framework which integrates structural, organizational, technological, epistemic, and cultural sources of risk in the energy transition. This way of thinking about risk encourages companies and regulators to go beyond the technical in considering public safety risk in the energy transition. A successful transition requires decision makers to consider people and technology together, i.e., the entire sociotechnical system.

The second part of the guide describes five major accidents that have occurred as a result of sociotechnical failures in technology transitions. Our focus here is on the risks that existed in those systems prior to disaster occurring. Users of the guide are invited to consider whether their organizational systems could be subject to some of the same weaknesses that will need to be addressed for a safe energy transition.

The guide applies to both operating companies and regulators. It aims to improve the performance of all participants involved in the emerging future fuels industry for delivery of safe and reliable new infrastructure and technologies.

The guide focuses on risk awareness and identification of risks, rather than providing detailed prescriptive advice regarding how best to manage sociotechnical risks. There are two reasons for this. In general, failures happen because people can't imagine them. This guide promotes reflection on what risks may be present in any given sociotechnical system. Once risks have been identified, risk mitigation/control is the next step. We expect that more work on tools for risk identification and strategies for risk mitigation will be the next phase of our research in this area. Anyone with an interest in this work is invited to get in touch with us.

We would like to acknowledge support from our FFCRC project steering committee and production assistance from Viet Hoang in preparation of this booklet. We would also like to acknowledge Carl Macrae's work on the SOTEC framework in the context of autonomous vehicles, which inspired our work.

Professor Jan Hayes

RMIT University

jan.hayes2@rmit.edu.au

Professor Sarah Maslen

RMIT University

sarah.maslen@rmit.edu.au

April 2025

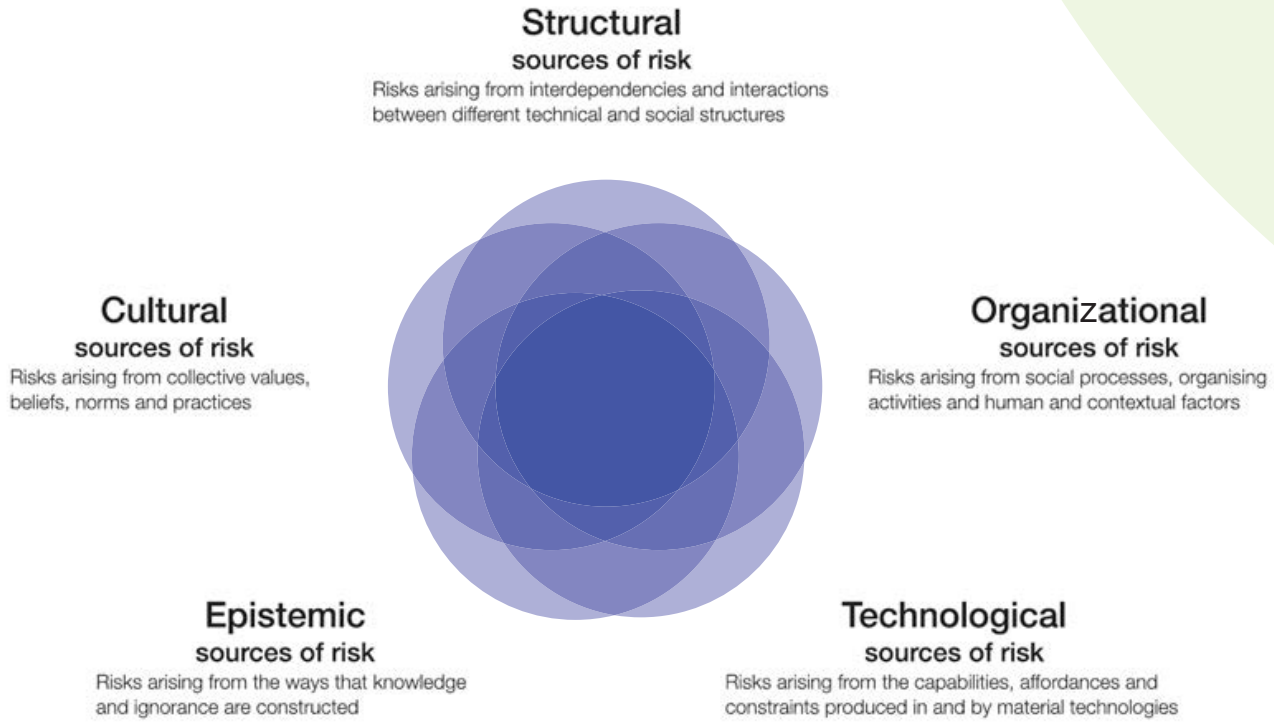
Introducing the SOTEC Framework

Engineers are used to looking at risk from a technical perspective, where failures occur for technical reasons like fatigue and corrosion and can be mitigated by technical methods such as monitoring and inspection. A different view of risk focuses on the people who are involved in every aspect of selecting, governing, designing, constructing, operating and maintaining technological systems. Together, the people and the technology comprise what can be called a sociotechnical system.

To think about sociotechnical risk in the context of new technologies, we adopted Macrae's SOTEC framework. This was based on a review of autonomous vehicles and has since been applied in the context of AI use in healthcare and robotics. The framework integrates structural, organizational, technological, epistemic, and cultural sources of risk. In the SOTEC framework:

- Structural sources of risk arise from interdependencies and interactions between different parts of the technical and social structures.
- Organizational sources of risk arise from the social processes, organizing activities, and human and contextual factors that underpin new technologies.
- Technological sources of risk arise from the capabilities, affordances, and constraints inscribed into and produced by new material technologies.
- Epistemic sources of risk arise from the ways that knowledge and ignorance are constructed in relation to, and within, the new technology.
- Cultural sources of risk arise from the collective values, beliefs, norms, and practices that surround and shape the technology.

These sources of risk are not independent, with different sources of risk amplifying, reinforcing, interacting and overlapping with one another.



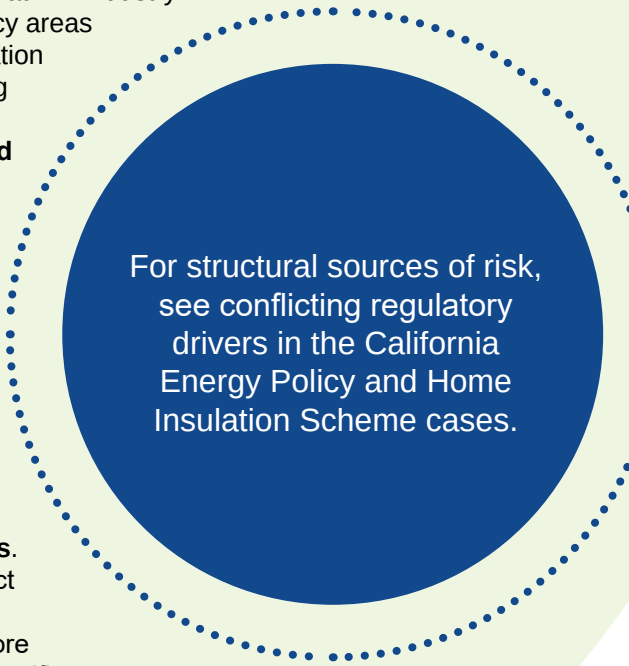
Structural Sources of Risk

Structures act as sources of risk by amplifying or transmitting local sources of failure. There are two sets of intraorganizational structures that are particularly relevant to sociotechnical risk in the energy transition.

Regulatory Structures

There is a long debate about the relative merits of goal-based and prescriptive regulation. The Australian gas pipeline industry operates under goal-based regulation which requires companies to understand risks and demonstrate that they are adequately managed. To date, the assumption has been that existing regulatory frameworks are appropriate for emerging technology in future fuels. However, **the impact of different regulatory approaches in the case of an emerging hazardous technology remains untested**. It is essential that regulatory decisions continue to be based on the best evidence available and the effectiveness of the regulatory regime is scrutinized.

Regulation of industrial safety is only one aspect of the structures that link industry and government. Structural separation of safety and economic policy areas of government has long been seen as best practice in safety regulation but is not always achieved in practice. Decarbonization is prompting major regulatory change in many areas that impact the gas sector. **Unless the impact of multiple conflicting objectives is managed mindfully, unintended consequences are very likely to result.**



Supply Chain Structures

The energy transition by its very nature will involve a significant program of capital works. **The way in which capital works are executed has a significant impact on safety** in operations, as the accident record demonstrates. Procurement failures often stem from viewing interconnectivity along the supply chain as a series of one-way transactions aimed at shifting risk. **Facilitating reciprocity and collaboration among system actors promotes transparency and knowledge sharing, reduces costs, and minimizes delays, ultimately leading to better project outcomes**. Making use of suppliers' expertise and adopting collaborative project delivery arrangements, such as early contractor involvement, can enhance project performance and safety. These factors become more prominent in the future fuels environment, where epistemic risk is significant.

Organizational Sources of Risk

When things go wrong, the temptation is often to look to the workers directly involved. There is now an extensive body of research detailing how we can only appreciate the actions of individuals in light of their local and organizational conditions. As described in James Reason's well-known Swiss Cheese model, for any individual error to lead to a major accident, a set of organizational defences must fail. As such, **improving organizational factors is the best way to make the overall system more robust**. Organizational factors refer to processes and procedures - are they seen as things to support people to do the best work possible or something used to constrain people and punish them if they don't comply? - also, reporting lines, incentive schemes and roles / responsibilities. We've identified three main organizational sources of risk.

Planning Major Projects

Particularly relevant to the energy transition are the organizational risks associated with delivery of major projects. The front end is expensive and time consuming, so people are tempted to take shortcuts that backfire later. Projects with a lot of bespoke engineering are very prone to this as they are less forgiving of change. **A focus on planning can counter the tendency for cascading failures**. Good planning requires a good range and depth of questions and rigorous but imaginative answers. Researchers in this area recommend learning at a small scale (cheap, quick and where failure is not dangerous) before going full scale. An experienced project manager and team is also vital. Inexperienced teams tend to lead to problem projects because they make the mistake of making decisions using "what you see is all there is" thinking rather than hard analysis.

Changing Roles and Responsibilities

Functional changes to organizational priorities in the energy transition will result in significant changes in reporting lines, role definitions and role responsibilities. **Structured methods for review of proposed organizational changes should be adopted as a key mitigation strategy** for risks of this kind. These can be linked to organizational management of change processes that formally review reporting lines, functions and competencies to ensure that a proposed change (such as reorganization of functions, creation of new business areas or disestablishment of a function) does not create any gap in safety responsibilities or lines of communication.

Organizational sources of risk are present in Chernobyl and Challenger. Major design decisions were not inherently safe, and testing was minimal.

Latent Failures

Failures in transition to a new technology can emerge due to pre-existing systemic weaknesses. Such latent problems may only become obvious when systems are called on to act as part of the technology change. They can manifest as a gap or weakness in processes, such as failing to apply concepts of inherent safety in design even when they are well known in an organization. Another example from the accident record is foregoing inspection and testing of new designs in the rush to go into operations. **A strong training program in safe design principles, an organizational commitment to these and ongoing audits against such principles could provide an effective mitigation strategy for these risks**. Other latent failures may be physical faults in the system that lead to major failure when operating conditions change.

Technological Sources of Risk

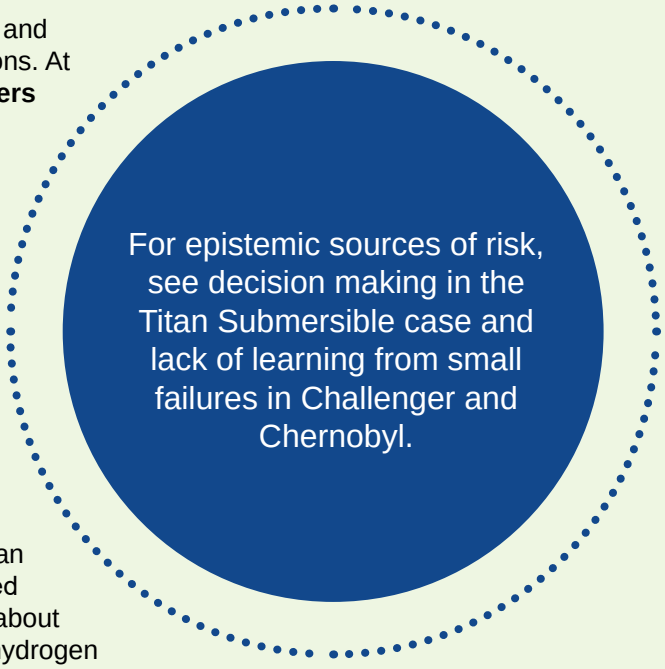
Technical processes for managing pure technological risks are well established in the gas sector and are not canvassed here in detail. Rather, we have listed some broad qualities of the technological system that may pose risks and noted how these change with the energy transition.

Current and future gas sector orientations towards technology

Quality	Existing orientation	Future orientation re: future fuels
Similarity/difference	Remotely operated pipelines containing high and lower pressure flammable gas. Some companies are also experienced with process plant/unit operations.	The nature of the facilities is unchanged although different unit operations will be used. Future fuels have similar properties to natural gas, although some possible future fuels are toxic.
Maturity	Mature technologies with incremental innovation.	Immature technologies still in the development phase.
Availability	Well established supply chains and experienced vendors with decades of experience and a large pool of resources.	Competing in a tight global market with a limited pool of highly stretched suppliers.
Location	Pipelines are a highly distributed system but operationally largely passive.	Distributed hydrogen production and injection facilities could mean a substantial dispersed asset base of a type that requires more frequent on-site presence.
Familiarity	Very familiar. Decades of operating experience to draw on. Experienced pool of suppliers and contractors available to support existing facilities.	Very unfamiliar. Only pilot scale facilities in existence. Many industry players have no specific experience of operating or maintaining these facilities.
Complexity	Gas pipelines and associated facilities are moderately challenging to design and operate.	New facilities will have a similar level of technical complexity to existing facilities.
Coupling	The consequences of major safety decisions manifest slowly meaning that there is time to respond if necessary.	New facilities will have a similar relatively low level of technical coupling to existing facilities.
Uncertainty	Physical details of existing buried infrastructure may be uncertain due to lack of accurate records. The inherent uncertainty at a materials level is low for steel pipelines transporting gas.	Uncertainty of physical details may still be high for repurposed facilities, but accurate records of newly constructed facilities should be available. Some material properties are uncertain (e.g. the impact of hydrogen on fracture propagation).
Variability	Variability in the transported fluid is minimal. Systems transporting natural gas suitable for end users generally have a single service for their design life.	Blended fuels may change specifications over time as user needs / requirements change. Pipeline systems may need to be designed and constructed for a wider operating envelope.

Epistemic Sources of Risk

Epistemic sources of risk arise from the ways that knowledge and ignorance are constructed both for individuals and organizations. At an individual level, **specialist knowledge about safety matters informs decision making.** This includes technical discipline knowledge, which is why professionals are exhorted to work only within their specific areas of professional competence. It also includes non-technical capabilities like an ability to use long-term foresighted reasoning, to understand norms and values that inform actions, to think systematically and understand interconnectedness, to collaborate with and draw on the experience of others, to ground decisions in reality and to advocate for action and take responsibility.



Lack of Expertise

In the transition, one of the primary challenges that the industry faces is limited expertise in designing and operating systems with future fuels. While hydrogen is in some senses an "old" fuel that some members of the industry have encountered earlier in their careers, the industry is facing many questions about the physical properties, behaviour and management of pure hydrogen and hydrogen/methane blends, particularly at high pressure. The question then is: **how do people know when they are at the edges of what is operationally safe and so when there is the need for new approaches**? This applies to both companies and regulators, and across the supply chain. Mitigation of this risk relies on activities such as secondments, networking, and setting up advisory arrangements to give Australian engineers as much exposure to as many new facilities as possible.

Confident Ignorance

In the context of non-technical pressures, whether economic or political, people working with emerging technologies may be overly confident about their expertise in an area where they actually don't have depth of experience. **Confident ignorance refers to a psychological state in which an individual demonstrates a high degree of confidence in their knowledge or abilities, despite lacking a sufficient or accurate understanding of the subject.** This trait often leads to poor decision making and overestimation of one's competence. In the extreme, even when faced with technical or scientific information that contradicts their beliefs or goals, these individuals may dismiss it, assuming that their unique vision or capabilities will allow them to overcome challenges. This leads to a mindset where risks are downplayed and solutions are sought through personal determination rather than informed decision making.

Learning from Small Faults and Failures

Absence of disaster is not absence of risk therefore small anomalies, faults and errors are a potential source of valuable insights into system health. Maintaining corporate memory of small failures facilitates ongoing organizational learning. Small faults and failures also have an important social function in giving regular reminders of the potential for major disaster and every individual's role in prevention. **An effective industry-wide system for collecting, analyzing and sharing information about early design and operational problems is the key** mitigation here. If all organizations commit to this, it could be an extremely beneficial tool for the industry. Regulators may have a role to play here in ensuring that lessons are heard across the sector.

Cultural Sources of Risk

In day-to-day organizational life, shared values and beliefs focus attention on some issues which then become organizational priorities while other issues are ignored and eventually go unnoticed. **When it comes to safety, a key cultural characteristic for organizational success is safety imagination** – an ability of all workers to see the link between their day-to-day activities and the potential for disaster, which then becomes a natural area of focus as they go about their work. Over time, such shared norms can deviate or drift from what was originally understood to be a safe way of working. Senior management is critical here as illustrated by the old aphorism 'what interests my boss fascinates me'. If management focuses strongly on increasing production, reducing cost or working faster, ways of working that are bad for safety can become embedded in work practices. Via such mechanisms, cultural risks arise, contributing to the likelihood of a major disaster.

The Need for Speed

Particularly relevant to the energy transition are attitudes towards time that make it more difficult for public safety-related decisions to be made with the long term in mind. The nature of capital project work always emphasizes the need to complete work quickly, but the energy transition is aiming to proceed at an even more accelerated pace than usual. **Placing such a premium on meeting deadlines means that speed is sometimes celebrated as a synonym of good**. In reality, if projects are not organized appropriately, they tend to move quickly at the beginning and then slow down (and overshoot schedule milestones) when the inevitable rework is required.

Lying at Work

Pressure on workers to achieve performance goals irrespective of the resources available to them creates conditions for lying at work. People create what they conceptualize as short cuts even though an external view might be that they are telling outright lies with potentially serious longer term consequences by reporting that work is done when it really has not been. Once such behaviours become established, it is very hard for anyone to change what is going on without external involvement. Organizational conditions in the energy transition requiring people to complete huge amounts of work in conditions of uncertainty with very tight deadlines means the environment is ripe for this kind of behaviour to occur. In fact, recent reports about faked research results regarding tests on hydrogen refuelling equipment at a South Korean research institute (Kitech) seem to be just such a case.

For cultural sources of risk, see the role of speed in decision making in the Challenger, Chernobyl and the Home Insulation Scheme.

A Changing Workforce

The excellent safety record of the Australian gas industry supports the conclusion that the culture of the industry places strong emphasis on achieving public safety. The sheer volume of work created by the energy transition will necessarily involve many new people moving into the sector. This could lead to competency gaps when it comes to process safety considerations and gaps in individual's cultural assumptions regarding safety and their work. This will need to be mitigated by **explicit communication of expectations regarding safety attitudes and performance reinforced by monitoring and feedback of actions to ensure that any early deviations from expectations are identified and addressed**. Conversely, people working on stranded assets can feel left out and anxious as they face the threat of their job disappearing and their expertise being no longer valued. Risks in this area are primarily mitigated by the actions of senior management in ensuring that those working on legacy assets feel that their work is significant to a successful energy transition.

Chernobyl Nuclear Power Plant

Reactor number 4 at the Chernobyl nuclear power generation plant suffered a meltdown in 1986. The accident caused 31 worker deaths and led to the permanent resettlement of 116,000 people. Estimates of excess deaths and injuries due to radiation impacts vary widely but are likely in the tens of thousands across impacted parts of the USSR and Europe (Higginbotham, 2019).

Construction of the Chernobyl nuclear power station began in February 1970. It was part of the USSR's crash program to build several new reactor complexes. The USSR had been the first to build a nuclear reactor to produce commercial power (in 1954) but since then had fallen well behind the US in commercial nuclear power technology and was short of electricity generation capacity, so there were both practical and political reasons to expand their nuclear power generation capacity.

The four reactors at Chernobyl were of the Soviet RBMK design. This design, which used graphite as the moderator and water as the cooling medium, was a direct descendent of Soviet military (plutonium producing) reactors. The same moderator/cooling medium combination was also used in reactors linked to the US Manhattan Project, but later US civilian reactors used boiling water as both a coolant and a moderator. This combination was chosen in the US due to a higher degree of inherent safety. The graphite/water combination had an inherent problem known as a 'positive void coefficient' whereby overheating of the water with the graphite moderator still in place could lead to a steam explosion and a runaway reaction.

The final design (including the graphite/water combination) was untested and immediately went into production in order to meet the ambitious goals set by government. It allowed the RBMK reactors to be built in existing factories previously making parts for tanks and tractors without specialist retooling. The design took advantage of economies of scale with the reactor having twenty times the volume of US reactors at the time.

The first commercial RBMK reactor was put into service in 1974 in Leningrad, and there were immediate problems. Apart from many quality issues with the plant itself, the sheer size made reactor control difficult as reactivity varied across the reactor core in unexpected ways. Also, the shutdown system operated too slowly to bring the reactor effectively and reliably to a subcritical state in the event of an emergency. After just over a year of operation, there was a runaway reaction and radiation was released over the Gulf of Finland. The subsequent inquiry reported that the cause was a construction fault, but in fact it was related to inherent safety issues with the design with the positive void effect in evidence, and operations were again not fully predictable or controllable. None of these problems were communicated to other sites operating RBMK reactors.

The first Chernobyl reactor came online in 1977 and proved to be as difficult to operate as the Leningrad reactors. A central study of all operating reactors in 1980 found nine major safety problems with the RBMK fleet, but this was not communicated to the operating plants. Instead, some tweaks to procedures were made, apparently without realising that the flawed construction and inherent operational problems meant that standard procedures were not being closely followed by people at site. Conversely, the people at site had no understanding that the modifications to procedures were safety critical.

In 1983, an emergency at another RBMK plant in Lithuania revealed a further design problem. The design of the reactors was such that, in one part of

Remember the basics: inherent safety in design

the performance envelope, insertion of the control rods, which would normally be done to slow down the nuclear reaction, caused the power to go up before dropping. This transient effect was what triggered the later meltdown at Chernobyl. No action was taken to change the design or operating procedures for other RBMK plants to take this into account because it was thought that no plant would ever operate with the combination of conditions that would lead to the effect being triggered. As IAEA investigators said following Chernobyl, 'It is reprehensible that such a deficiency had been known of for so long without its having been eliminated' (IAEA, 1992, pg 16).

These factors were to come together in April 1986 in Chernobyl. The immediate trigger for the accident was a test. Large volumes of cooling water needed to be continuously circulated for the reactors to remain safe. It was recognised that if power to the cooling water pumps failed, there was a time lag before the backup power generation system had sufficient energy available to power the pumps, leaving the reactors vulnerable to overheating. It was postulated that, in the event of a power failure, the rotating momentum of the turbines could power the cooling water pumps for the few seconds necessary prior to the plant emergency generators starting up and being able to take the load. A test was undertaken to confirm this theory, but at low power levels the reactor did not operate as expected and a meltdown occurred with a massive explosion that breached the reactor and sent highly radioactive material over a wide area.

Subsequent investigations into the accident criticised the safety culture at the plant (in fact this is the first use of that term) but also the inherently unsafe design and the weak system of regulation in place. On this last issue, the inquiry report states: 'The basic design of the RBMK reactors was approved [by the regulator] despite the lack of conformity to many of the USSR's design requirements for nuclear power plants' (IAEA, 1992, pg 21).

Lessons for the Energy Transition

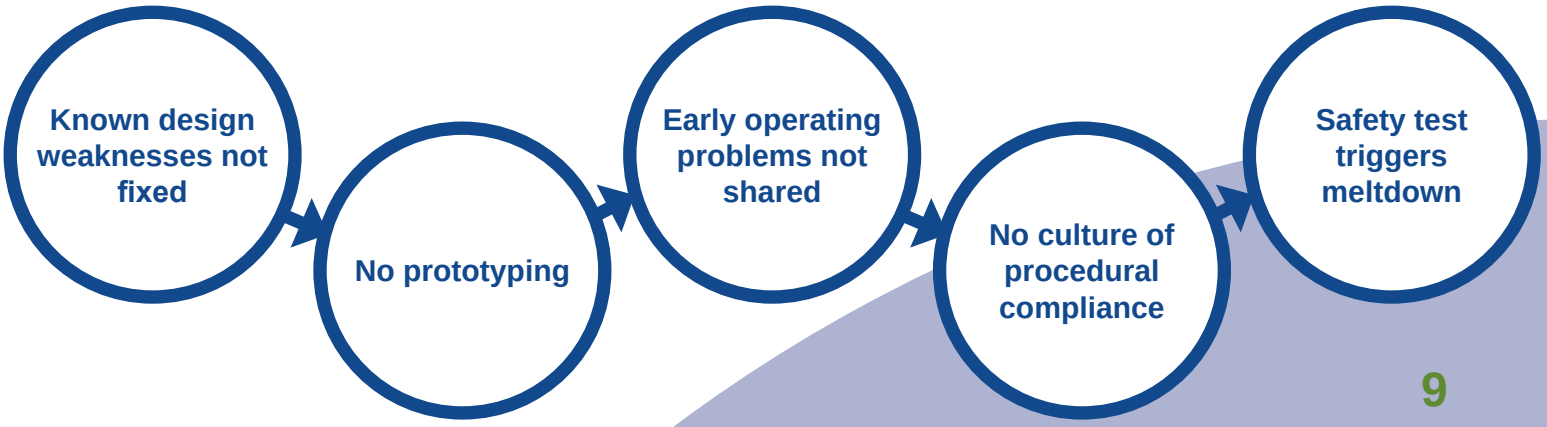
Sociotechnical risks that we see manifested in the Chernobyl accident case include:

- Inherent safety in design is critical – the industry has to live with safety problems that become embedded as a result of expedient but less safe choices made early on.
- In the enthusiasm for the new and exciting things, the basics can be forgotten, e.g., the need for testing of a new design before going into production.
- Political choices can have unexpected safety consequences, e.g., expedited construction led to parts being made in factories that normally make lower quality parts – with resultant quality problems.
- Early faults, failures and operating experiences should be seen as a gift for sharing and not something to be hidden. Lessons from early operating and design problems should be communicated to other similar facilities.
- Operating procedures must be accurate and workable so that compliance can be mandated and results in operations within a safe envelope.
- Political imperatives can drive weak regulation.

References

Higginbotham, A. (2019). *Midnight in Chernobyl: The Untold Story of the World's Greatest Nuclear Disaster.* Corgi Books.

IAEA. (1992). *INSAG-7: The Chernobyl Accident: Updating of INSAG-1.*



Space Shuttle Challenger

In the late 1960s, when NASA's plan to put a man on the moon was essentially complete from a design perspective, NASA's attention turned significantly to development of orbital aircraft that were reusable so that space flight could become routine. This was a major departure from the Apollo program in which each spacecraft was effectively a disposable item - designed to last only long enough to safely bring crews and payloads back to Earth. The estimate to develop such an aircraft was $14 billion, but Congress approved only $5.5 billion. As a result, the project needed military support to be viable, necessitating major changes to some design parameters (increased range and payload weight). The original plan included a piloted and fully reuseable booster aircraft (to get the orbiter out of the Earth's atmosphere) and a piloted orbiter that could deliver payloads to space, conduct experiments and then return to Earth and land like a plane. Further budget constraints led to the final design of an unmanned solid rocket booster (SRB) leaving the shuttle with three main sections – an orbiter vehicle with liquid-fuelled engines, enormous external fuel tanks carrying hydrogen and oxygen, and two separate SRB engines to get the vehicle into orbit.

The SRBs were designed and manufactured by a contractor (Morton Thiokol) in Utah. Morton Thiokol had decades of experience in designing and manufacturing solid fuel rocket engines. The design philosophy they adopted for the shuttle boosters was to avoid inventing anything new, but the shuttle booster rockets were physically much larger than anything Thiokol had built before. Building a new manufacturing facility at Cape Canaveral (the launch site) was considered to be out of the question for financial reasons, so the SRBs were designed in sections to be transported and then assembled at site. The joints were understood from the start to be a potential weak point and it was also expected that joint failure would be catastrophic. The final design was for a system with primary and secondary O-ring seals packed with putty in between. The long-tested rocket design now included an experimental new component whose integrity was critical.

Early testing of the booster engines (1978/79) showed that, while the joints were holding, they were not functioning as the designers intended. Some NASA specialists pushed for a redesign noting the potential for catastrophic failure. They even spoke to the O-ring manufacturer, who expressed concerns about this use of their product, but these concerns were buried and never passed on to Thiokol. Thiokol and NASA considered conducting additional tests, but these were deemed to be unnecessary and in October 1980, the SRB seals were certified as flight-ready. As one senior NASA engineer observed 'you don't build in redundancy and then never expect to use the back-up. If you never use your back-up, you're wasting money'.

The space shuttle was first launched in 1981 and, while successful, there was an element of luck involved in this test flight. Some of the external insulating tiles were damaged on takeoff because the acoustic shock waves caused by the engines on launch had been underestimated by an order of magnitude. (The size of the shock wave was determined based on 1/15 model results scaled up to full size). Luckily, the damage occurred to parts of the shuttle skin that did not experience the most extreme temperatures on re-entry and the two test pilots returned safely. Inspection of the SRBs after the second test flight showed unexpected damage to seals but the sealing system overall functioned as required. Despite these serious engineering problems, after only four test flights the shuttle program was declared open for business to

Small failures are a gift: learn from them

begin transporting commercial payloads into space. A space shuttle crew for a normal mission now typically comprised seven astronauts – a combination of pilots, mission specialists and payload specialists.

By mid 1985, shuttles had made close to 20 flights but the concept of space flight becoming routine was far from the truth. The price charged for commercial payloads was still approximately 20 times the figures quoted by NASA when the program was first mooted because the effort required to keep the shuttles flying was much greater than expected - NASA calculated that three years of work on the ground was needed for every minute in space. Instead of simply conducting a few routine checks and refuelling, each shuttle had to be disassembled, examined carefully and reassembled before each flight. Despite this there was a large public appetite for members of the public to be allowed to fly to space and as a result the 'teacher in space' program was announced by Ronald Reagan in 1984.

The first teacher in space was aboard the Challenger when it took off in January 1986. The shuttle and its crew were lost on take-off when failure of an SRB seal allowed hot gases to escape which caused the adjacent liquid fuel tanks to explode. The cold weather on the day of the launch was another key factor in the failure. Repeated warnings about the dangers of the SRB joint design, particularly at low temperatures, were made by the contractor starting in 1981 and continuing until the night before the launch but their concerns were ignored by various parts of NASA management.

As described above, the technology behind this failure had a long history of discussion, analysis and (in)action over the life of the shuttle program making it typical of sociotechnical accidents and providing lessons for the energy transition.

Lessons for the Energy Transition

Sociotechnical risks that we see manifested in the Challenger case include:

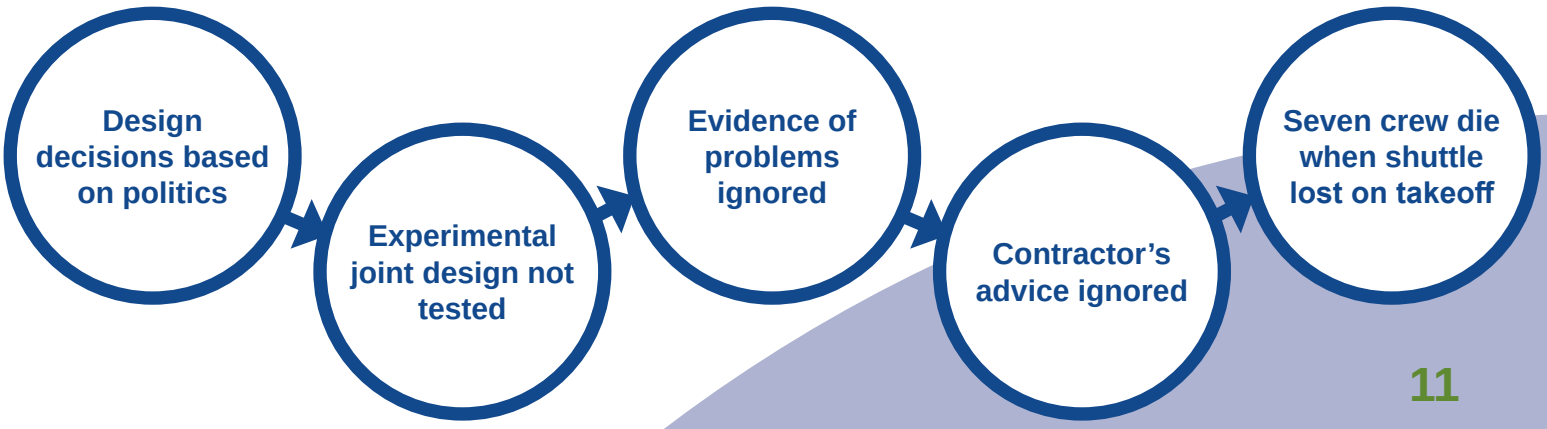
- Inherent safety in design is critical – Challenger's loss had its roots in early design decisions made to save money.
- In the enthusiasm for the new and exciting things, the basics can be forgotten, e.g., the need for adequate testing.
- Imagining worst case outcomes and linking this possibility to day-to-day actions can be difficult e.g., exposing a civilian teacher to the risk of a shuttle flight.
- Potential bad news must be taken seriously and not dismissed as inconvenient.
- Political choices can have unexpected safety consequences e.g., the segmentation of shuttle components.
- Four successful test launches did not demonstrate that the system was safe (as they were assumed to do).

Further Reading

Higginbotham, A. (2024). *Challenger: A True Story of Heroism and Disaster on the Edge of Space.* Penguin Viking

Rogers, W. (1986). *Report to the President by the Presidential Commission On the Space Shuttle Challenger Accident.* NASA.

Vaughan, D. (1996). *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA.* University of Chicago Press.



Titan Submersible

In June 2023, the OceanGate submersible vessel Titan imploded, killing its crew, during a deep ocean dive approximately 1 hour and 45 minutes into its planned dive to the wreck of the Titanic. The Titan previously initiated four dives at the Titanic location in 2021, four dives in 2022, and three dives in 2023. OceanGate was founded by Stockton Rush and Guillermo Sohnlein in 2009 with a vision to provide greater access for humanity to the deep ocean. The aim of OceanGate was to create a fleet of 4-5 submersible vehicles to facilitate an affordable (and thus accessible) experience where 5 people could dive to a maximum depth of 6,000m available for charter anywhere in the world, with no dedicated mothership.

The company had originally planned to purchase rather than design and build submersibles, but nobody was able to develop a submersible that met the OceanGate business criteria of a standalone submersible without a dedicated mothership. This approach would eliminate the costs associated with acquiring, operating, and maintaining a dedicated support vessel and the transit issues involved in that support vessel needing to travel to each dive destination globally. In designing a submersible, the CEO – Richard Stockton Rush – positioned himself and the company as 'disruptive innovators' which led them to pursue technological solutions that were beyond standard industry practice as a matter of principle, rather than for the purpose of achieving a particular organizational performance outcome.

Fundamentally, there are two "life-essential" systems on a submersible: (1) the pressure hull that protects the occupants from the crushing exterior pressure; and (2) the oxygen life support system. Pressure hulls are unique critical system elements in that they have no redundancy (unless double-hulled), meaning the entire safety of the crew and the integrity of the submersible depended on the hull's ability to withstand extreme underwater pressures. Unlike other systems in engineering that can have multiple layers of redundancy or backup systems, a pressure hull for a deep-sea submersible is a single point of failure—if the hull fails, there is no secondary line of defence to protect human life.

Modern commercial manned submersibles for deep-sea exploration are generally made from titanium, which is exceptionally strong and strengthens under repeated exposure to high stress. While the industry is in agreement about this, the company CEO believed that titanium was unnecessarily heavy, and so he directed the teams to manufacture the hull from carbon fibre instead, which can provide the necessary strength when first put into service but breaks down over time under pressure. Despite viewing carbon fibre as 'a great material', Rush also acknowledged the possibility for 'catastrophic failure where you have imperfections in the [carbon fibre] structure'. Given carbon fibre makes a 'crackling' noise under excessive stress, he proposed and installed an 'acoustic safety system' on Titan to detect such crackling. He referred to it as a safety system, but in reality, if it registers a problem, the failure is imminent.

The importance of non-destructive testing methods, such as ultrasonic scanning, is widely recognized for detecting flaws or weaknesses in pressure hulls before they lead to failure. OceanGate knew about these testing protocols but failed to apply them comprehensively. The industry also relies on third-party certification bodies, like DNV GL or the American Bureau of Shipping (ABS), to validate the design and safety of pressure hulls. OceanGate was fully aware of this practice but chose to bypass the certification process, citing innovation as their justification.

Focus on the right technical solution, not innovation for its own sake

OceanGate's attitude to design is further illustrated by the design of Titan's electronic systems. The submersible was piloted using a mass-produced Logitech video game controller rather than a controller custom-made for its design and operation. It was Bluetooth rather than hardwired. Titan also had only 'one button' (for power) within its main chamber. All other controls and gauges were touchscreen meaning that none of the controller, controls or gauges would work without a constant source of power and a wireless signal.

These and other concerns about the design were raised within the organization but were dismissed to the degree that those actors were fired and legal action was threatened. During the US Coast Guard Marine Board hearing in September 2024, testimony revealed that the resignation of several seasoned and highly experienced personnel at OceanGate was a critical warning sign that went unrecognized or was dismissed by company leadership. These individuals, many of whom had deep expertise in submersible technology and maritime safety, left the company after expressing concerns about the Titan submersible's design and testing protocols.

David Lochridge, OceanGate's former Director of Marine Operations, testified that after he voiced serious concerns about the structural integrity of the Titan's carbon fibre hull and the lack of proper testing, he was not only dismissed but also faced legal threats from the company. OceanGate filed against Lochridge a lawsuit accusing him of breaching a non-disclosure agreement (NDA) and making unfounded claims, which effectively silenced him and prevented further public discussion of his safety warnings. Similarly, Rob McCallum, a deep-sea exploration consultant, testified that he too was met with legal threats when he urged OceanGate to adhere to established certification processes and standards. McCallum stated that he was warned to cease public criticism or face legal action. These testimonies illustrate a troubling pattern where OceanGate leadership used legal intimidation to stifle critical safety feedback, creating an environment where valid concerns were dismissed rather than addressed, ultimately contributing to the disaster. The OceanGate CEO, who was central to the company's strategy of threatening those who raised problems, apparently really believed that these concerns were unfounded. He was on the Titan at the time of the implosion and was killed with the rest of the crew.

Lessons for the Energy Transition

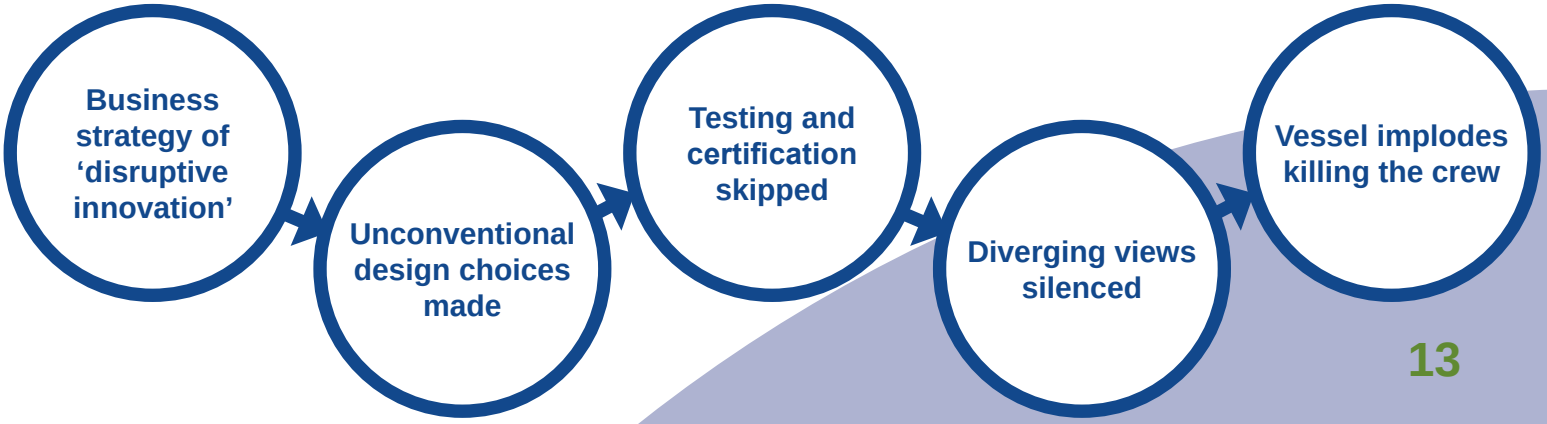
Sociotechnical risks that we see manifested in the Titan case include:

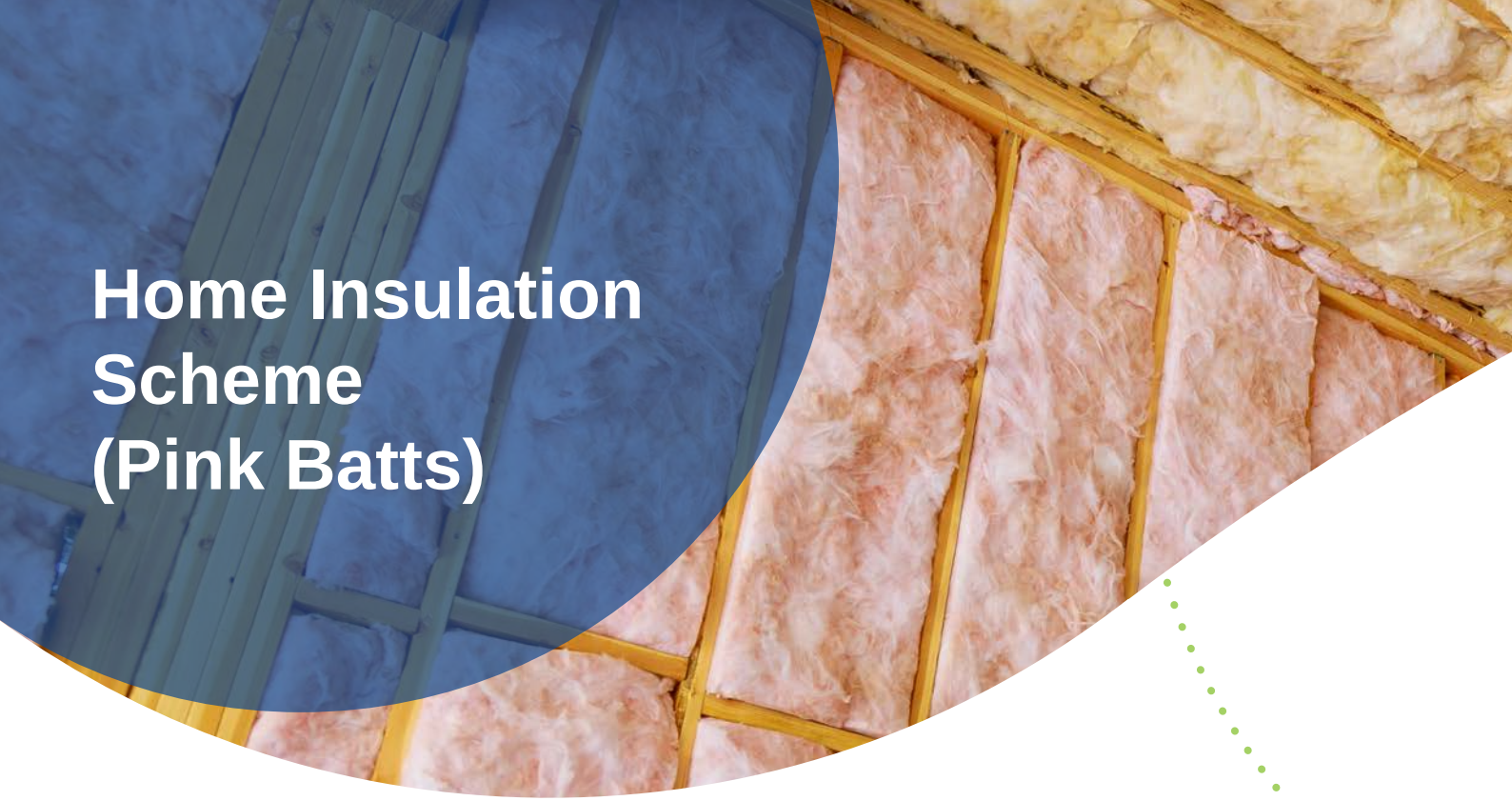
- Inherent safety in design is critical
- The possibility for people to be overly confident about hazard management with untested technologies
- Losing sight of the consequences in the face of a desire to be at the forefront of a field
- Skipping testing phases in a rush to getting product into operation
- Not listening to technical experts within the company and the sector more generally

Further Reading

Schecter Shaffer & Harris LLP. (2024). *Wrongful Death Complaint: Richard Ortoli vs OceanGate inc et al.*

Additional information can be found on the US Coast Guard Titan Submersible Marine Board of Investigation website: https://www.news.uscg.mil/News-by-Region/Headquarters/Titan-Submersible/





Home Insulation Scheme (Pink Batts)

The Home Insulation Program (HIP) emerged in response to a search for policies that were a good political candidate as part of an economic stimulus package from the Australian Government during the Global Financial Crisis. This scheme was part of the $42 billion Nation Building and Jobs Plan. The hunt for the policy idea started in late 2008. Prime Minister Kevin Rudd announced the scheme on 3 February 2009 with a 1 July 2009 roll out date. The HIP originally had $2.7 billion allocated to it. HIP aimed for a fifteen-fold increase in the number of installations per year in a tight timeframe, which also demanded a major increase in the workforce. Until very late in the HIP, the Australian Government failed to identify and manage the risk to installers of injury and death. Four people died whilst working under the HIP and a Royal Commission was established to examine the development and implementation of the HIP (Hanger, 2014).

The decision to proceed with HIP was made at a political level. The public servants involved in scoping this possible stimulus intervention identified that the industry, in its current state, did not have the capacity to deliver the program. There were several departments and agencies involved in the program, including the Department of the Environment, Water, Heritage and the Arts (DEWHA) who were operating under the oversight of the Office of the Coordinator-General (OCG) and the Department of the Prime Minister and Cabinet (PM&C). They knew a rapid upscale would be required. Indeed, in the risk assessment meetings about the program, one of the identified risks related to the lack of a current workforce to deliver the program. No safety concerns were raised in the risk assessment, which was undertaken in a meeting of public servants without industry input.

That the industry was ‘largely unregulated’ was one of the reasons it was selected for the stimulus. South Australia was the only state or territory with insulation-industry specific regulation beyond general occupational health and safety regulations. There was a view among the public servants involved that the barrier to entry was therefore low and this was a good thing. This decision reflected a focus on economic stimulus over worker and public safety.

The need for an instant workforce resulted in the decision on the part of the Project Control Group (PCG) to relax training and competency requirements. The PCG was comprised of representatives from DEWHA, PM&C/OCG, Medicare, the Department of Education, Employment and Workplace Relations, and the Australian Taxation Office, in addition to consultants and auditors who participated as observers. Centrelink and the Department of Human Services attended some early meetings. The PCG “agreed to a set of installer minimum competencies, which specified that installers need not receive training in insulation installation, or hold a specified competency, if they were supervised by a person who had been so trained, or held that competency” (Hanger, 2014, pg 159). While they substituted ‘supervision’ for insulation specific training, they were not specific about what constituted supervision. Consultation with industry experts identified the need for training of installers. The industry and DEWHA were all unanimously of the view that this was vital. The decision to proceed without this requirement was pushed by PM&C and OCG in the interests of keeping barriers low and was justified on the basis that, with the exception of South Australia, at the time the States had no requisite training or registration for installers. Indeed, it was not until the first death under the HIP that it was specified that supervision required the presence of an on-site supervisor.

Political pressures can make for bad safety choices. What is driving major design decisions?

Everyone involved was under the impression that the commencement date was immovable. The perceived need to rush the design and implementation of the HIP brought about a failure to properly consult with industry about the risks and a failure to heed more than one warning about the risks of installing insulation, especially Reflective Foil Laminate (RFL) sheeting. Indeed, there had been a death in New Zealand the year before related to RFL. This was a matter of public record, and yet the case was not considered by decision makers prior to the announcement of the scheme. The public servants involved also did not consult with the NZ counterparts who were rolling out a similar scheme at the time, excluding RFL sheeting for reasons of safety.

There is evidence that by early April, people were aware of the NZ case, and the expert hired as a technical advisor -- Dr Tony Delbridge -- was particularly vocal. His insistence on raising safety concerns led to the cessation of his contract with DEWHA. Following the announcement of the scheme, the Prime Minister's office also received 33 emails from constituents imploring caution, including 7 letters specifically on OH&S matters. Multiple parties also raised concerns about worker safety, including electrical risks that could cause death or serious injury. These risks were raised again in mid July 2009 when the draft resources for installers were released for consultation. Those resources note in particular the risk of electrocution associated with using staples when installing RFL sheeting. The Royal Commission concluded that RFL sheeting should never have been included in the scheme and directly contributed to two of the four deaths by electrocution when installing the RFL. Another worker was electrocuted when installing fibreglass insulation. The fourth worker died from hyperthermia when installing fibreglass insulation.

The Royal Commission concluded that given the lack of regulation, the cash injection carried the predictable risk of rorting and other unscrupulous behaviour. The decision to effectively terminate the HIP had a profound effect on businesses which manufactured insulation and which were engaged in the installation of it.

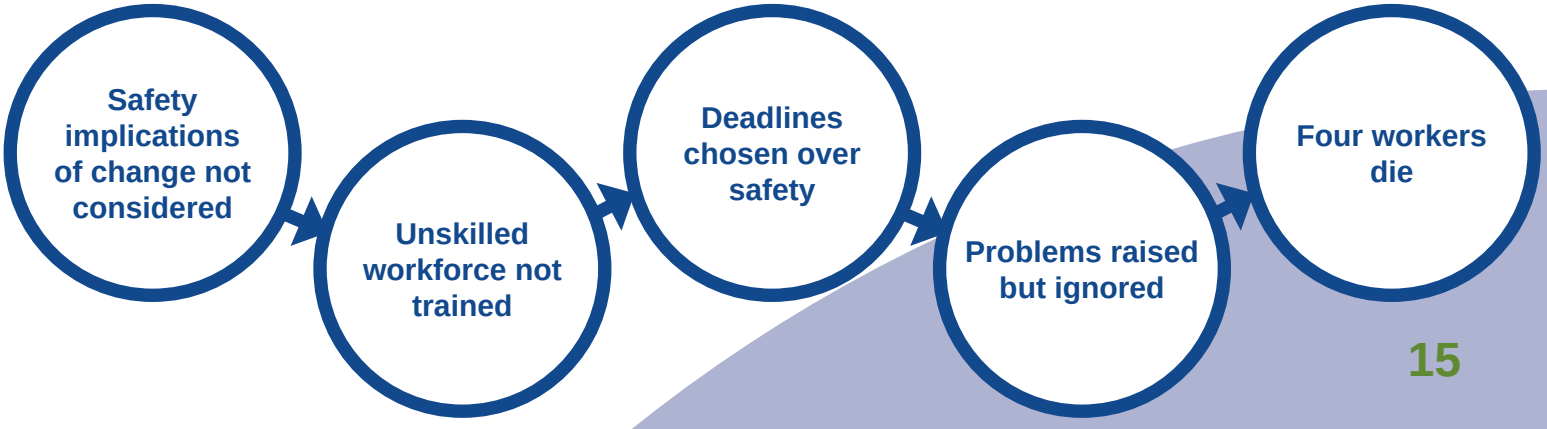
Lessons for the Energy Transition

Sociotechnical risks that we see manifested in the HIP case include:

- The potential for political as opposed to technical failure, where decision makers focus on policy factors over considerations of the implications for the technology and show little interest in the technology itself
- Relaxing training because of production pressure
- Inadequate regulation of an area of practice

Further Reading

Hanger, I. (2014). *Report of the Royal Commission into the Home Insulation Program.*



California Energy Policy

> ***Beware of undesired business outcomes if regulatory requirements conflict***

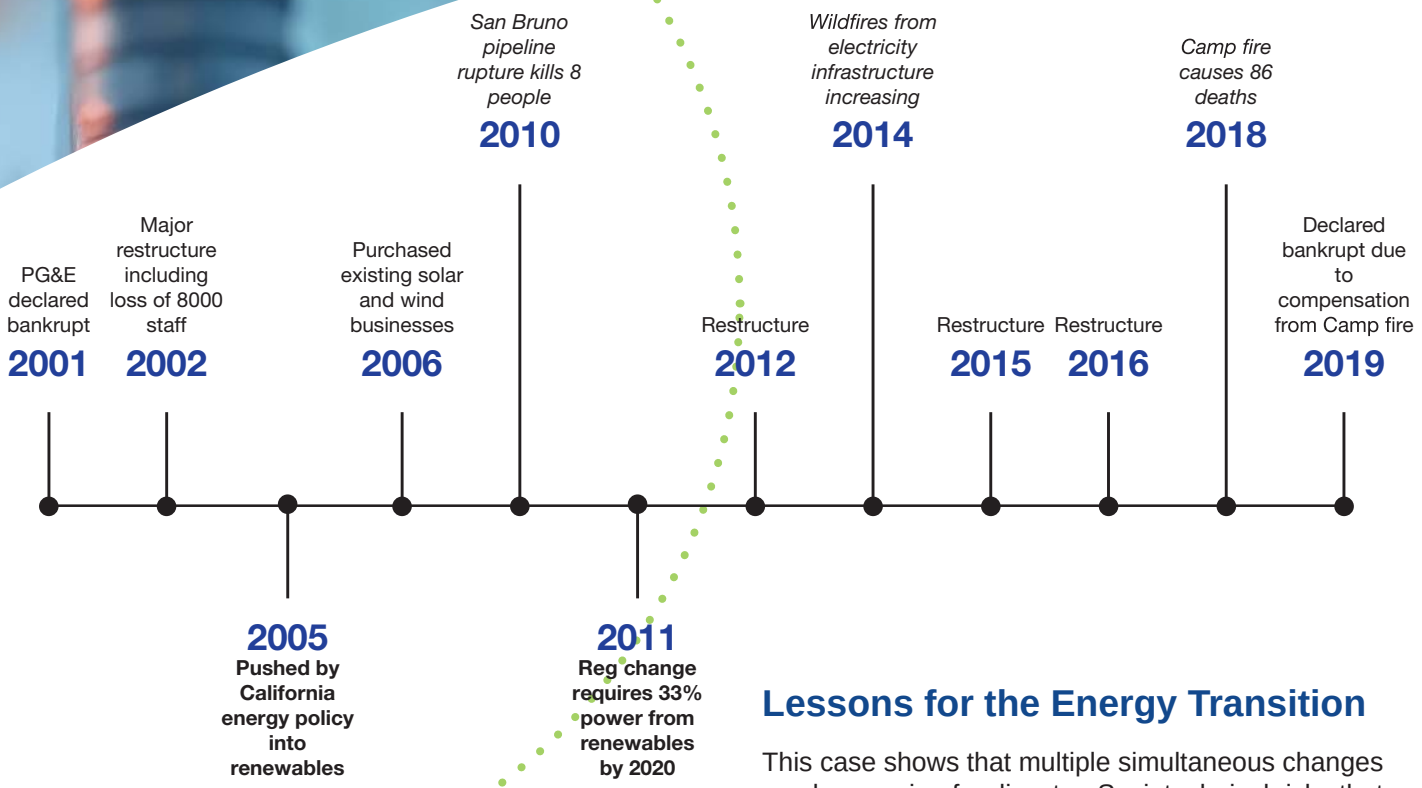
Pacific Gas & Electric (PG&E) operate gas infrastructure in California, and their activities are regulated by the Pipelines and Hazardous Materials Safety Administration (PHMSA), which is part of the US Department of Transportation. Enforcement is contracted to the California Public Utility Commission (CPUC). PG&E has had a turbulent corporate history since the turn of the century; it has twice declared bankruptcy and been held responsible for several major disasters. While there are no doubt ways in which the corporation could have behaved better, California energy policy over this period was a major source of problems for the company.

PG&E was declared bankrupt in 2001 as a result of deregulation of the California electricity market and the resultant huge increase in power procurement costs. PG&E's plans to restructure the company were contested by CPUC and the bankruptcy settlement took several years to negotiate. PG&E exited bankruptcy in April 2004. Following this, under a new CEO, the top organizational priority was 'transforming our business with a focus on trying to serve our customers faster, better and more cost-effectively'. From mid 2005, Accenture advised on Business Transformation to modernize PG&E's work processes. After studying company operations, Accenture recommended reducing staffing by 8000 people. At the same time, supported by Californian government policy regarding low carbon emissions, PG&E were expanding rapidly into renewable energy and buying existing solar and wind power businesses. Electricity was always the major focus of the organization internally to the extent that workers joked PG&E had a big E and a little g.

In 2010, an operational upset caused by maintenance work at a terminal resulted in a gas pipeline rupture at San Bruno which killed eight members of the public (Hayes & Hopkins, 2014; NTSB, 2011). One investigation noted that in the period leading up to the accident, PG&E had been in a state of perpetual reorganization for more than a decade. This incident brought regulatory attention to, amongst other things, poor record-keeping and out-of-date systems within the gas division of PG&E. The major effort to fix this is illustrated by reports of hundreds of pallets of records stacked with tens of thousands of boxes delivered to a local arena for sorting. As part of the modernization effort following San Bruno, PG&E built a new digital control center at San Ramon and hired more than 2000 extra workers in the gas division. By 2014, PG&E had improved sufficiently to be recertified as a best-in-class operator. Investigations into legalities linked to the San Bruno pipeline rupture were continuing and in April 2014 PG&E was charged with twelve counts of violating federal pipeline safety laws.

In parallel with these major issues in the gas division, PG&E senior management was also preoccupied by issues linked to climate change. Regulatory changes were introduced in 2011 requiring 33% of PG&E's power to be sourced from renewables by 2020 in an environment where renewable power was more expensive than other forms of generation, putting a major financial burden on PG&E. Further regulatory changes to push more strongly towards renewables were being contemplated. The pace of reorganization also continued with another review of PG&E's operations noting divisional restructures in 2011, 2015, and 2016 (NorthStar, 2017).

During this same period, CPUC was increasing their focus on wildfire risk. While the initial focus was on other Californian utility companies, PG&E undertook a study to assess wildfire risk linked to their activities and concluded that the risk was low. In fact, driven by



deregulation, bankruptcy and the transformation project, the company had cut back on power line maintenance and inspection, and the electricity division suffered from the same record-keeping problems that San Bruno had revealed in the gas division. Assessing the true level of risk was difficult due to the lack of records about the electricity infrastructure and the remote areas through which some utilities were running, although in the period 2014 to 2019, PG&E reported more than 1500 fires started by their equipment. Most of these were minor but, combined with the drought conditions, the potential for a major fire seemed significant and resulted in a major program of tree cutting and plans being developed for shutting off power during the worst of adverse weather conditions. The situation came to a head with the Camp fire which started on November 8, 2018 and resulted in 86 deaths. Possible claims from this and other fires resulted in PG&E declaring bankruptcy for a second time in early 2019.

The adversarial regulatory relationship between the CPUC and its regulated utilities also provides important context. As an example, most of the regulatory decision making at the CPUC is conducted within a public legal proceeding, that is an adversarial process with formal testimony from competing advocates. Also, the CPUC has adopted a prescriptive, compliance-based and punishment-centered approach to regulation. PG&E, for example, has been recently fined over $2 billion for various violations: $1.6 billion for record-keeping failures and other negligence in the San Bruno gas explosion case in 2015; an additional $97.5 million by the CPUC for illegal back-channel communications with Commission officials about that case; and most recently, $110 million for falsification of Locate and Mark records.

Lessons for the Energy Transition

This case shows that multiple simultaneous changes can be a recipe for disaster. Sociotechnical risks that we see manifested in the PG&E case include:

- Deregulation introduced business pressure that resulted in cost cutting on safety.
- A regulated push to renewables and increased wildfire risk as a result of drought interacted to lead to several major accidents.
- Major fines and pressure from the regulators did not lead to improvements but rather drove problems underground.

Further Reading

Blunt, K. (2022). *California Burning: The fall of Pacific Gas and Electric and what it means for America's power grid.* Portfolio/Penguin.

Hayes, J., & Hopkins, A. (2014). *Nightmare pipeline failures: Fantasy planning, black swans and integrity management.* CCH.

Hayes, J., Maslen, S., & Schulman, P. (2024). A case of collective lying: How deceit becomes entrenched in organizational safety behavior. *Safety Science*, 176(106554). https://doi.org/https://doi.org/10.1016/j.ssci.2024.106554

NorthStar. (2017). *Assessment of Pacific Gas and Electric Corporation and Pacific Gas and Electric Company's Safety Culture, Final Report, Prepared for CPUC May 8, 2017.*

NTSB. (2011). *Pipeline Accident Report: Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire, San Bruno, CA, September 9, 2010.*

Research team

Prof Jan Hayes

Prof Sarah Maslen

RMIT University
School of Property, Construction and Project Management
www.rmit.edu.au

Future Fuels CRC
www.futurefuelscrc.com

For more information contact:
jan.hayes2@rmit.edu.au

Australian Government
Department of Industry, Science and Resources

AusIndustry
Cooperative Research Centres Program

This work is funded by Future Fuels CRC, supported through the Australian Government's Cooperative Research Centres Program. We gratefully acknowledge the cash and in-kind support from all our research, government and industry participants.