EPRG-PRCI-APGA
23rd Joint Technical Meeting
Edinburgh, Scotland
6–10 June 2022

PAPER TITLE: LESSONS IN RISK GOVERNANCE FOR THE PIPELINE SECTOR FROM PAST PROCUREMENT FAILURES

PAPER NUMBER: 36

Jan Hayes*
RMIT University, Melbourne, Australia

Yen Pham
RMIT University, Melbourne, Australia

Rita Peihua Zhang
RMIT University, Melbourne, Australia

Nader Naderpajouh
University of Sydney, Sydney, Australia

* Presenting author

ABSTRACT

Public and private sector procurement failures are unfortunately common and also very costly. The cost of replacing off-specification cladding on buildings in Victoria is estimated to be up to $1.6 billion. In addition to financial impacts, procurement failures were a significant part of the Grenfell Tower disaster in the UK in 2017 which resulted in 72 deaths. Procurement failures have occurred in the pipeline sector, too, although details are not necessarily widely known.

In this paper, we focus on past procurement failures across a range of sectors (such as built environment, infrastructure, chemicals and aviation) to formulate lessons learned for better risk governance in procurement for the pipeline sector. The paper draws on public domain materials regarding 19 procurement failures in order to identify underlying causes in four major categories: supply chain coordination and management; supplier issues; external environmental factors and cooperation and trust issues.

The analysis shows that there are common factors across sectors. Key issues that emerge include the need for better project planning (e.g. clear scoping/specification before tendering begins), careful management of supply chain interfaces (e.g. a clear definition of responsibilities), the danger of counterfeit materials, and selection of technically competent contractors.

Effective strategies to reduce risk are grounded in developing common goals for all parties involved. This means providing contracting arrangements and incentives that align the interests of all parties by sharing risks and rewards.

Given supply chain disruption as a result of the COVID-19 pandemic and the rapid development of new major infrastructure projects in the wake of climate change action, learning lessons from past procurement failures becomes particularly pertinent.

1. INTRODUCTION

Failures of materials, equipment or services through ineffective supply chain risk management represent a threat to the successful development of the emerging hydrogen and biogas future fuels industry. In addition to the potential for major cost and schedule blowouts, failures on any early project in this new industry could cause significant reputation damage and so adversely impact the development of the entire sector. Public safety can also be impacted. Research into effective mitigation of such threats is warranted to ensure that societal expectations for public safety are met, company interests are protected and the reputation of both organizations and new technologies are enhanced.

Despite the criticality of procurement procedures and supply chain management in the successful execution of infrastructure projects, there have been many examples of procurement failure leading to unplanned adverse outcomes including:

- NSW trains too wide for tunnels (2018)
- Grenfell Tower fire (2017) and other building sector incidents
- South Korea nuclear reactor shutdowns (2013)
- HMAS Westralia (1998)
- Canberra Hospital Implosion (1997)

The gas industry has not been immune from similar incidents although specifics are often not readily available to share due to commercial/legal issues. Our research will make particular effort to better understand such incidents through confidential interviews with pipeline industry personnel.

Cost and schedule implications of late delivery of procured items, potential safety risks as a result of counterfeit items, and failure to meet expectations for levels of service provided are among the common issues. Widening of NSW railway tunnels to allow for incorrectly specified new trains cost the NSW government $75 million[1]. The cost of replacing off-specification flammable cladding in Victoria is estimated to be between $250 million and $1.6 billion[2].

The Future Fuels Cooperative Research Center (FFCRC) is undertaking research on risk governance in procurement (Project RP2.3-06) with a view to reducing the risk of unplanned outcomes caused by procurement failures and so supporting the emerging future fuels sector. The outcome of the project will be an understanding of critical gateway points in the procurement process and the practices that can be implemented to improve procurement risk governance in the gas pipeline sector. The primary output will be recommendations and guidance for member companies involved in the development of pipelines, hydrogen generation and storage, production of biogas and renewable power generation. In addition to providing the research data and results, the project will include as much practical guidance as possible making use of flow charts, checklists and similar. The project is targeted for completion in December 2022.

This paper reports on the first of four phases of this research project, the literature review aspect of the project, in particular a review of past procurement failures in order to determine lessons for the future fuels sector that can be learned.

[1] https://www.smh.com.au/national/nsw/blue-mountains-rail-line-gets-75-million-upgrade-20181218-p50mxn.html
[2] https://theconversation.com/flammable-cladding-costs-could-approach-billions-for-building-owners-if-authorities-dither-118121

2. BACKGROUND

2.1 Definitions

The project is grounded in the idea of how best to manage the risk associated with procurement failure, so it is important to define some key terms.

Procurement is a series of planning, organizing and coordinating processes to obtain goods and services from an external source by an organization [1].

In this project, we consider that ***procurement fails*** when failures in procurement planning (scoping or contracting), specification, purchasing, manufacturing, or delivery of goods or services result in a project failing to meet stakeholder objectives (both short and long term).

This implies that failures can occur at various stages along the supply chain. It should also be noted that stakeholders can have differing objectives so views on whether, and the extent to which, failure has occurred is at least partly a social construction.

The project draws on ISO 31000 for language related to risk. ***Risk*** is defined in the standard as the effect of uncertainty on objectives, noting that an effect is a deviation from the expected [2]. In ISO 31000, effects can be positive or negative but in this project, we focus on negative effects.

In the language of ISO 31000, objects, events or circumstances that have the potential to give rise to risk are called ***risk sources***. An outcome impacting objectives is a ***consequence***, noting that consequences can escalate due to cascading and cumulative effects.

2.2 Organizational failures

Many of the risk sources in procurement are organizational so it is important to set out the way in which the work conceptualizes organizational failure.

In recent years, an extensive research literature has examined both the prevalence and causality of major failures within complex socio-technical systems (for example, see [3]). These studies demonstrate that disasters are as much an outcome of social relations as they are a result of technical failings and so these types of disasters can most usefully be thought of as organizational accidents. Organizational accidents are events that occur within complex modern technologies, such as nuclear power stations, commercial aviation, and oil and gas facilities and have multiple causes involving many people working in different areas and at different levels. Analyzing an incident in this framework involves a search for not only technical causes but also causes related to systems of work and the actions of people throughout the organization.

One of the most well-known models of organizational accidents is James Reason's Swiss Cheese Model of Accident Causation shown in Figure 1 [4]. In this way of thinking about accidents, there is a range of defenses in place that are functionally designed to prevent any given hazard from leading to a loss of some kind (such as an accident). In practice, these defenses are imperfect (like holes in Swiss cheese). The various hardware and procedural measures in place ensure that failure of any individual measure is not catastrophic. An accident occurs when the holes in the cheese line up and provide an accident trajectory through the defenses.

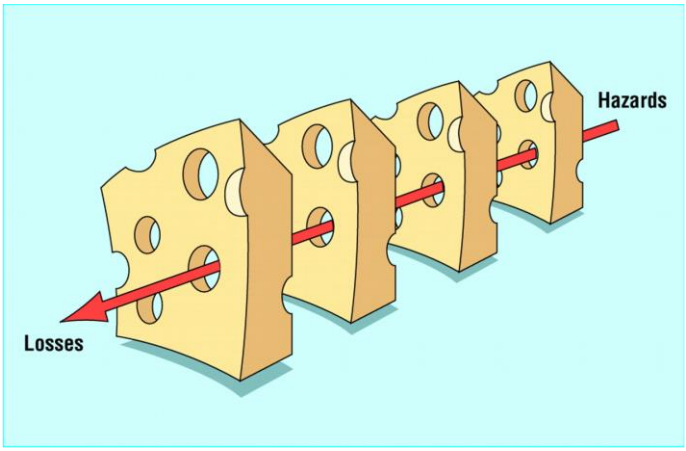

Figure 1. Swiss cheese model

In this model, the "holes" in the cheese have two interesting features. First, they may be due to active failures, such as the mistakes or non-compliant behavior of frontline operators, or they may be due to latent failures. Latent failures are weaknesses in the system that do not, of themselves, initiate an accident, but they fail to prevent an accident when an active failure calls them into play on a given day. Problems arise when latent failures in the system accumulate – maintenance is not done, records are not kept, audits are not done. The consequence of a small active failure can then be catastrophic as the protective systems fail to function as expected.

The second feature of the holes in the Swiss cheese is that they are a function of the organization itself. In this model of accident causation, operator actions in the field are linked to workplace factors, such as competency, rostering, control room design, task design, etc., and these issues are linked to organizational factors such as budgets, safety priorities, management styles, etc. In this way of thinking about safety defenses, the performance of all components in the system is interlinked.

While Reason's model was developed with physical disasters in mind, this type of thinking about failure applies equally to other types of objectives such as meeting schedule and cost in a project environment. The aspect of Reason's model that is of relevance is the 'holes' in the Swiss cheese that represent vulnerabilities of the system.

Organizational failures are significantly linked to the way work is organized and so are common across complex socio-technical systems. This means that risks linked to organizational factors are likely to appear across sectors and so lessons can be learned by the pipeline sector from procurement failures in other complex industries such as the high-rise built environment sector, major infrastructure, and the process industries. This is reinforced by the study done on behalf of the UK Institution of Civil Engineers following the Grenfell Tower disaster [5]. The In Plain Sight report showed that civil engineering infrastructure generally is potentially vulnerable to the same system failures as were experienced in the Grenfell Tower case. Those failures were significantly related to procurement. The relevance of the procurement lessons learned from these cases is further emphasized by the fact that many of the same or similar issues are arising in the fieldwork interviews with energy sector personnel being undertaken for the next phase of the research.

3. METHOD

The FFCRC research project RP2.3-06 Risk Governance in Procurement for Future Fuels entails four primary stages:

- Literature review
- Study current procurement practices
- Develop risk governance framework
- Develop risk mitigation recommendations

This paper reports on some of the results of the literature review stage which has included the following steps:

1. Construct risk taxonomy
   Firstly, academic and grey literature (i.e., public domain material from non-traditional publishing sources including reports and guidance material) on risks in procurement was sourced and summarised to develop a risk taxonomy. The final taxonomy identified multiple sources of risk falling into four key categories which are:

   a. supply chain management and coordination,

   b. suppliers,

   c. external environment, and

   d. trust and cooperation.

   The full taxonomy can be found in the FFCRC report RP2.3-06 Risk Governance in Procurement for Future Fuels Interim Report #1 dated March 2022.

2. Identify procurement failures
   The next stage was to create a list of procurement failures that are potentially useful for the future fuels sector to learn from. The criteria used were that the failure must be a procurement failure, not just a project failure, it must be from a complex industry and there must be sufficient secondary data available to analyze it drawing on both the organizational view of accidents and the risk taxonomy described above. Cases were drawn from both major projects and procurement in the operation of complex facilities. Nineteen cases were identified in the public domain. Most of these are either cases where the consequences of the failure were safety-related and so a major public investigation was triggered, or public sector project failures where cost and/or schedule overruns triggered an investigation of some kind with public findings.

3. Analyze / describe risks that came to fruition and so lessons to be learned from each failure case
   Note that this analysis has been drawn from secondary sources. Given the time available to conduct the work, primary sources have not been consulted but rather the analysis draws on multiple investigation reports and other published analyses of the given cases. Links have been drawn to the four categories of risk described at point 1 and the list of specific risk sources developed from the literature for each category.

4. Summarize sources of risk based on individual failures and taxonomy
   The lessons from the entire group of 19 failures cases have been reviewed collectively to determine key themes.

4 FINDINGS

The final list of procurement failures is shown in Table 1.

	Incident	Sector
A	Lacrosse apartment fire (2014)	Building
B	Grenfell Tower fire (2017)	Building
C	Hyatt Regency walkway collapse (1981)	Building
D	Opal Tower cracking (2018)	Building
E	Channel Tunnel (1985-1994)	Infrastructure
F	Demolition of the Royal Canberra Hospital (1997)	Infrastructure
G	I-90 Tunnel ceiling collapse (2007)	Infrastructure
H	Berlin-Brandenburg Airport project delay (2011-2020)	Infrastructure
I	NSW public transport failures	Infrastructure
J	The CBD and South East Light Rail project (2011-2020)	Infrastructure
K	Loss of Space Shuttle Challenger (1986)	Aerospace
L	Boeing 737 MAX failure (2018)	Aviation
M	The Myki ticketing system failure (2005-2014)	ICT-based transport
N	HMAS Westralia ship fire (1998)	Maritime
O	South Korean nuclear reactor shutdown (2013)	Energy generation
P	Cabin Creek Hydroelectric Tunnel Fire (2007)	Energy generation
Q	Explosion at Shell in Moerdijk (2014)	Chemicals
R	Fireworks Disassembly Explosion and Fire (2011)	Chemicals
S	Buncefield explosion and fire (2005)	Oil & gas

Table 1. List of procurement-related incidents

To give an indication of the level of analysis and the procurement lessons learned from these cases, details of three failure cases are included. These are the Grenfell Tower fire, the Boeing 737 MAX failure and the Buncefield explosion and fire.

4.1 Grenfell tower fire (2017)

The 24-storey Grenfell Tower was part of the Lancaster West Estate, which is a council housing complex in North Kensington, West London. Grenfell Tower together with other council housing were originally managed directly by the Royal Borough of Kensington and Chelsea Council (RBKC) until 1996 when the council established the Kensington and Chelsea tenant management organization (KCTMO) under the UK Government's Housing (Right to Manage) Regulations 1994 to manage the council housing stock [6].

A major refurbishment was conducted on the Grenfell Tower during 2014-2016. The refurbishment involved installing an insulated rainscreen cladding system covering the exterior of the building. The cladding system consists of combustible polyisocyanurate (PIR) foam insulation and aluminum-polyethylene composite material, separated by a ventilated cavity [7].

Early on the morning of 14 June 2017, a fire broke out in a fourth-floor flat in the Grenfell Tower. The fire, caused by a malfunctioning refrigerator, spread rapidly to the building's external cladding. Crews from the London Fire Brigade arrived within six minutes and later were joined by firefighters and fire engineers from stations across London as well as the London Metropolitan Police Service [6]. By the time the blaze was extinguished, 72 residents had lost their lives and an additional 71 had been injured. It was the deadliest structural fire in the UK since the 1988 Piper Alpha disaster and the worst UK residential fire since the Second World War. Investigations into the Grenfell Tower fire revealed that the combustible material used in the building cladding was the cause for the rapid spread of fire [7]. The cavity between the cladding and the insulation acted like a chimney to spread the fire. This incident clearly indicates a failure in procuring safe and compliant building materials.

4.1.1 Replace the cladding with a cheaper version

The Inquiry into the Grenfell Tower fire identified cost-driven behaviors of the client organization, suggesting a poor organizational culture. Documents released by the RBKC Housing and Property Scrutiny Committee from 2013 revealed that the company Leadbitter, who was the original contractor scheduled to carry out the Grenfell refurbishment work, was dropped by KCTMO-RBKC because its quotation of £11.278 million was £1.6 million above the budget proposed by KCTMO-RBKC [6]. The contract was put back out to competitive tender, and the other company Rydon was then appointed as the contractor to carry out the work with a quotation of £8.7 million [8]. The scopes of work set out for both companies were similar, with the latter company agreeing to carry out the work for £2.5 million less. This suggests contractor evaluation and selection were inadequate. It appeared that KCTMO-RBKC selected the contractor primarily based on the criterion of cost, overlooking the factors of quality, the standard of work and competency.

A project execution strategy of Design and Build (D&B) was used in the Grenfell Tower refurbishment project. Under the D&B strategy, consultants (e.g., architects and engineers) undertake the concept design stage of a project, which will then be passed on to the D&B contractor (in this case Rydon) to complete the detailed design and construction stages. Leadbitter's original plans included recommendations from architects and engineers, who undertook the concept design, to adopt a zinc composite external cladding with a fire-retardant core. The fire-resistant zinc cladding was also approved by residents of Grenfell Tower. However, RBKC implemented a value engineering initiative with the aim of saving costs. Evidence showed that amendments were made to the contract between KCTMO and Rydon after tender to save £293,369 by replacing the cladding with cheaper aluminum panels, which contain a polyethylene core that was proven to be more combustible in tests and banned on building higher than 12 meters in Germany and the US at that time [6]. Meeting minutes, price outlines and other project correspondence suggested a strong focus on cost-cutting from RBKC with little concern for safety [9].

4.1.2 Testing, certification and inspection of the cladding

The Inquiry into the Grenfell Tower fire revealed compelling evidence that the cladding system failed to comply with the Building Regulations in that it failed to adequately resist the spread of fire with regard to the height, use and position of the building [10]. Cladding using a composite aluminum panel with a polyethylene core should not be used on buildings over 18m in height according to the Building Regulations. This has led to the question of how the non-compliant cladding was approved to be used on the Grenfell Tower by relevant inspection and regulatory bodies. Investigation into the incident of the Grenfell Tower fire indicates severe procurement non-compliance issues in terms of supplier behavior and quality assurance and control.

The Grenfell Tower Inquiry shows that the suppliers that manufactured Grenfell Tower's cladding "abused" the testing system, deliberately provided misleading information about the performance of their products and circumvented regulations with marketing strategies [11]. Specifically, the company which manufactured the cladding sheets, Arconic, obtained a certificate for its polyethylene-filled panels on "a false premise" by providing test reports for a more fire-retardant version of the product.

The company Celotex, which manufactured the combustible PIR insulation foam, demonstrated a "widespread culture … of ignoring compliance", including distorting a full-scale fire test of its products. In addition, the company Kingspan, which produced the rest of the insulation, carried out tests that involved "concealing components in a manner designed to facilitate a pass and/or using materials that were not as described in the test reports", including adding fire retardants to materials in order to slow down ignition [11]. The unethical supplier behavior was enabled by the deregulation and privatization of testing and certification bodies [12]. The testing and certification are often commissioned by the manufacturers of the products (i.e., self-certified), which is highly problematic because of conflict of interest and lack of independence.

The inability to identify the problematic cladding also suggests the issues of experience and expertise of building surveyors and inspectors and the ineffective enforcement of laws and regulations. Before construction work can commence, full plans or detailed design drawings need to be reviewed and approved by building surveyors to ensure that the plans fully comply with the requirements of Building Regulations. In the Grenfell Tower case, despite the fact that the composite aluminum panels did not comply with the Building Regulations in terms of fire resistance and were not allowed to be used on tall buildings, they were still approved by building surveyors from the local council. This clearly demonstrates surveyors' negligence and ineffective enforcement of regulations. Further, during 2014-2016, sixteen inspections were undertaken by building inspectors on the Grenfell Tower refurbishment project, but all these inspections failed to identify that the building was being clad with material effectively banned on tall buildings by the Building Regulations [13]. This raises the concern as to whether the building regulation officers were sufficiently competent, as one investigation noted [14], there are "no legislative requirements that set standards of competence or training for building control inspectors".

4.1.3 Procurement lessons to be learned

1. The contractor Rydon was selected by the client organization purely based on the criterion of price. There is a need to change the cost-driven culture. The consideration of cost should be balanced with quality and safety requirements and a contractor's technical competency when evaluating tenders.
2. The supplier demonstrated unethical behaviors by manipulating tests and providing misleading information about the performance of building products. It is important that the purchaser has internal testing and auditing mechanisms in place to verify the information provided by the supplier. In addition, the industry and regulatory bodies should set and apply a clear code of conduct for suppliers, who are held to account for breaching the code of conduct.
3. The privatized material/product testing and certification lack independence and transparency. The privatization of testing and certification can be conductive to the unethical behaviors of suppliers. It is important to have the testing and certifying process undertaken by an independent third-party to avoid conflict of interest and provide reliable product or material information.
4. The surveyor in the Grenfell Tower case approved the use of cladding panels that are clearly not compliant with building regulations, suggesting the enforcement is inadequate and ineffective. Auditing mechanisms should be in place to review and monitor the performance of regulation officers and enhance their professional accountability.
5. The ineffective enforcement was partially attributed to the building surveyor's lack of competency. It is important that regulation officers are equipped with adequate skills and clear about their roles and responsibilities, for example through professional development and assessment.

4.2 Boeing 737 Max failure (2018)

On 29 October 2018, an Indonesian domestic flight operated by Lion Air crashed after pilots advised air traffic control that the aircraft was experiencing flight control, altitude and air speed issues. 189 people

were killed. 157 people died on 10 March 2019 when another aircraft crashed in Ethiopia after experiencing similar control problems [15]. After the second accident, the problems were traced to Boeing's new aircraft - the 737 MAX.

4.2.1 Overview

Boeing 737 aircraft have a long flying history being first certified for commercial aviation use by the US Federal Aviation Administration (FAA) in 1967. The design of Boeing's 737 MAX aircraft was the 4th generation of 737 aircraft and was based on the previous model (737 Next Generation). On 8 March 2017, the FAA granted an amended type certificate to Boeing for the new design and the first aircraft went into service two months later. Seventeen months after that, the first of two catastrophic crashes occurred.

The 737 MAX aircraft contained a new feature compared to previous models. The Manoeuvring Characteristics Augmentation System (MCAS) had the ability to trigger flight control movements independently of pilot action and could place the aircraft into a dangerous nose-down position. Inputs to the MCAS system came from the angle of attack (AOA) sensors externally mounted on either side of the aircraft fuselage. In both accident cases, faulty data from an AOA sensor triggered the MCAS system to incorrectly force the nose of the aircraft down. Pilots repeatedly struggled to regain control of the aircraft but were unsuccessful. In the Lion Air case, a similar incident had occurred with the same aircraft on the previous day, but the flight crew came up with an innovative method to control the aircraft (removing electrical power from the flight control that was incorrectly activated by MCAS) and the flight landed safely. The sensor problem was noted in the aircraft log, but the aircraft response and the innovative way around the problem were not recorded.

The US investigation into the accidents identified contributing causes as flawed technical design criteria, faulty assumptions about pilot response times and production pressures [16]. In the context of this project, it is useful to consider Boeing as a supplier of complex, high-tech equipment to airlines with third-party certification of the design of the equipment carried out by the US FAA on behalf of the airlines. In that framing of events, the accidents can be seen as procurement failure where a key supplier failed to deliver a fit-for-purpose product to the airlines.

Boeing and the US Department of Justice came to an agreement whereby prosecution has been deferred. Boeing agreed to pay over US$2.5 billion composed of a criminal penalty (i.e., fine), compensation to Boeing's airline customers and the cost of establishing a victims beneficiaries fund linked to the two crashes mentioned above [17]. In addition, Boeing's chief test pilot at the time of the aircraft development and certification has recently (October 2021) been indicted for fraud, effectively for lying to the FAA [18].

4.2.2 Airline requirements

Applying a procurement lens to the disaster, the first key issue is that Boeing failed to supply the airlines with a fit-for-purpose product. Airlines had a choice of aircraft to purchase at that time. The 737 MAX was in direct competition with Airbus's A320neo aircraft. As a result, the contract arrangements pushed all schedule and cost risks of developing the new aircraft onto Boeing. The project team developing the aircraft was under enormous pressure to cut costs and maintain the project schedule for production of the new aircraft in order to meet airline requirements.

As part of the design of the new model, Boeing developed MCAS in response to identified stability issues in certain flight conditions induced by the plane's new, larger engines, and their relative placement on the 737 MAX aircraft compared to earlier models. Despite the system's critical role in assurance of in-flight stability, it was not declared a safety-critical system. The system also operated on a single input (an AOA sensor) which contravened Boeing's safety philosophy. Despite pilots not being told that the system operated in this way, Boeing assumed that pilots could quickly compensate for any potential malfunction.

More than that, AOA sensors are not new and previous 737 models had an alarm to indicate if AOA sensor readings disagree (i.e., if one sensor is faulty). This alarm was also part of the certified 737 MAX design but in fact it was not functional in the 737 MAX aircraft delivered to airlines, making it even more difficult for pilots to determine the nature of the problem if the MCAS activated incorrectly [16].

In summary, the malfunction of one of two AOA sensors had moved from something that would trigger an alert to something that would not trigger an alert but would threaten flight stability in completely unexpected ways. Risk management processes failed to ensure any of these issues were addressed.

4.2.3 FAA Certification

Boeing is a U.S.-based multinational corporation that designs, manufactures, and sells commercial airplanes to airlines worldwide. When an airline buys new aircraft, they are custom manufactured but the basic airworthiness of the design of the aircraft is not checked by each purchasing airline. Aircraft designs and operational requirements are certified. The US Federal Aviation Administration (FAA) prescribes minimum standards for the design and operation of aircraft and is responsible for ensuring compliance.

Much of the detailed work linked to certification is undertaken by Boeing Authorized Representatives (ARs), Boeing employees who represent the interests of the FAA and act on the FAA's behalf in validating aircraft systems and checking design compliance with FAA requirements. Such a system presents ARs with an inherent conflict of interest. The investigation found that ARs were aware of some of the design problems that contributed to the accidents and raised these with Boeing but the issues were not addressed and also not reported back to the FAA [16]. In this way, quality assurance and quality control (QA/QC) requirements for the new aircraft were fatally flawed.

Linked to certification is the level of pilot training required for the new aircraft. This is critical to schedule as Boeing's airline customers were permitted to fly the 737 MAX only after training requirements are approved by the FAA. Boeing technical pilots were responsible for providing the relevant information to the FAA. The investigation found that these individuals knew of the issues with the MCAS design and yet they deliberately hid this information from the FAA. As a result, the FAA deleted all information about MCAS from the final version of FAA documentation regarding operating the 737 MAX. In turn, aircraft manuals and pilot training materials lacked information about MCAS, and pilots flying the 737 MAX for Boeing's airline customers were not provided any information about MCAS in their manuals and training materials [17]. As the US Department of Justice has said, 'Boeing chose profit over candor by concealing material information from the FAA concerning the operation of its 737 MAX airplane and engaging in an effort to cover up their deception.' [17] All this indicates a major cultural issue at Boeing and a failure to link the work to flight operations in the airlines.

The investigation also found many cases where FAA management had overruled a determination of their own technical experts when requested to do so by Boeing management. The FAA was completely 'captured' by Boeing and was not providing any degree of independent oversight. Consistent with this finding, the US Senate investigated aviation safety oversight following these accidents and received input from 57 whistle-blowers regarding failings at the FAA [19].

4.2.4 Procurement lessons to be learned

1. Contractual terms and conditions: Boeing were cutting corners in complying with their own safety systems due to schedule and cost pressures as a result of commercial competition between otherwise similar suppliers. In cases such as this, the potential for cutting corners to recoup costs by the successful supplier should be identified, assessed, and mitigated where possible, likely by additional inspection/audit activities.
2. The supply chain configuration separated Boeing's activities from the actual airline operating pilots and their needs. Pilot training provided by Boeing failed to address key safety issues.

Having operational personnel embedded in the design office would likely uncover this type of issue.

3. Given the structure and culture of the sector, operational input to the aircraft design was provided by Boeing technical pilots whose loyalty was to Boeing, rather than the airlines. They were actively involved in hiding design problems from the FAA. This emphasizes the importance of having operational input from those who will actually be operating new facilities.
4. QA/QC were not effectively provided through the regulatory system. FAA certification activities were significantly undertaken by individuals working in-house at Boeing, so they lacked any independence or power when problems arose. Arrangements with third-party certifiers must be structured to ensure no conflict of interest either individually or organizationally. Further, Boeing lied to the FAA. Not everyone in business always behaves ethically. It is important to consider how important information can be independently verified.

4.3 Buncefield Tank Farm fire (2005)

The immediate trigger for the December 2005 catastrophe at the Buncefield oil storage depot in the UK was a large petrol storage tank that overflowed whilst it was being filled from a pipeline. The magnitude of the resultant vapor explosion was much greater than anyone knew was possible. Houses close to the terminal were destroyed and buildings as far as 8km away had windows broken. Forty-three people received minor injuries (but there were no fatalities). Over 20 large storage tanks on the site were destroyed in the subsequent fire which burned for five days. There was also significant damage to the adjacent industrial estate and interruption to aviation fuel supplies in the UK. The response involved over 1000 emergency services personnel [20].

4.3.1 The failure

Hertfordshire Oil Storage Ltd (HOSL) operated part of the Buncefield site. Tank 912 was being filled with unleaded petrol from a pipeline. The tank was overfilled because the tank gauging system was not working and the independent high-level system in place failed to shut off the supply to the tank. Petrol continued to flow from the top of the tank into the surrounding bund and a large vapor cloud formed. At 6am on Sunday 11 December 2005 the first explosion occurred likely ignited by traffic in a nearby carpark.

The Buncefield fire highlights procurement issues with the tank level instrumentation where the operation of a key safety device was compromised by a poor design and lack of communication along the supply chain.

4.3.2 The independent high-level switch

The high-level switch that failed to protect the tank had been supplied by a company called TAV Engineering in July 2004, replacing an original switch of different design. The replacement switch design allowed for some functionality to be routinely tested but the design also meant that it was easy for the switch to be left in a non-functioning state after such tests had been performed. A padlock was used to lock a lever into the 'operational' position. The padlock was to be removed for testing to allow the test lever to be moved and then reinstated to ensure that the test lever did not interfere with the operation of the switch. Without the padlock in place there was no guarantee that the switch was functional. This is not a good design for a safety-critical instrument. TAV were aware that the switch was to be used in a safety-critical application but they chose not to modify the design [21]. The switch was replacing a model that did not include this padlock design.

The replacement switch was part of an overall tank instrumentation package designed by Motherwell Control Systems. Motherwell engineers did not understand the criticality of the lever position or the padlock, seeing it only as an anti-tampering device. TAV did not tell them and they did not ask, despite the safety-critical nature of the switch. The subsequent investigation criticized Motherwell's actions as follows:

- *'The process for ascertaining and then specifying the requirements of switches they supplied and/or installed was not adequate.*
- *They did not obtain the necessary data from the manufacturer and it follows that they did not provide such data to their customers.*
- *They did not understand the vulnerabilities of the switch or the function of the padlock.*
- *There was a reliance on TAV, which was not justified given the lack of information provided and the critical role that Motherwell had in installing safety-critical equipment.'* [21, pg 14]

HOSL was also criticized for failing to provide sufficient oversight of the ordering, installation and testing procedures [21]. The switch was tested periodically but operational personnel were not aware that the padlock needed to be preplaced in order to hold the test lever in the correct position for the device to perform its safety-critical function. COMAH also criticized aspects of the contractual relationship between HOSL and Motherwell, saying 'Where contractors are engaged to carry out work upon which the safety of many and much depends, something more rigorous than the evident causal relationship with Motherwell was called for:

- *There should have been a formal contract in place clarifying the expectations inherent in safety-critical work.*
- *There should have been an effective system of reporting and recording all significant faults and their resolution. This system should have been understood and implemented by both contractual partners.*
- *Reliable and up-to-date specifications of what was in place and what was required should have been provided.*
- *Critically, in respect of the replacement of the IHLS switches in 2004, there should have been a formal 'management of change' process. This typically would have included an engineering assessment of the benefits and disadvantages of any such change, and a consideration of what changes in procedures (e.g., in testing) would be necessary as a result.'* [21, pg 20]

4.3.3 Procurement lessons to be learned

6. Contractual terms and conditions: HOSL, Motherwell and TAV had informal arrangements in place for providing safety-critical equipment and as a result, things were missed. No clear vendor data was supplied for the safety-critical items. Formal arrangements must be in place where safety-critical equipment is to be provided to ensure that requirements and responsibilities are clear. Vendor data on key items is critical.
7. The replacement high-level switch was designed differently to the one it was replacing and yet the safety impact of the differences was not assessed. Effective 'management of change' is important when procuring replacement items.
8. No explicit specification was provided regarding the new high-level system. Clear specifications for safety-critical equipment must be mandatory.

5. DISCUSSION

The lessons taken from each failure case can be summarized using the risk source taxonomy. Table 2 shows the occurrence of the four categories of risk across the nineteen incidents reviewed. It also shows the proportion of lessons to be learned divided across the same four categories. It is clear that supply chain coordination and management issues occur most frequently.

Category	Occurrence in cases		Proportion of risk sources	
Supply chain coordination and management	11/19	58%	54/73	74%
Suppliers	5/19	26%	5/73	7%
External environment	5/19	26%	5/73	7%
Trust and cooperation	9/19	47%	9/73	12%

Table 2. Lessons from failure cases by risk category

As shown in Table 2, we have identified 73 sources of risk and associated practice lessons to be learned from the nineteen procurement failures described above. Of those, 54 relate to the first risk category, supply chain coordination and management. The most common risk sources within that category are described below. Project identifying letters refer to Table 1.

Eleven of the nineteen incidents were partly caused by issues with supply chain configuration i.e., the organizations included in the supply chain and the formal structures that link them. In most cases, this relates to the selection of a supplier that was not suited to provide the goods/services required. In some cases, it was because there was no effective prequalification system in place (B, F, M, O). In other cases, it was because a supplier with marginal capability in relevant areas was chosen on the basis of low cost, but no additional measures were put in place to ensure that a suitable quality was maintained (K, P, R). Another supply chain configuration issue common to several failure cases is a poor link from procurement activities into ongoing operations so failures occurred at the end of the project when this gap was uncovered (L, E). Other interface coordination issues arose in four cases – in one case the supply chain was configured so that oversight functions reported to those that their activities were meant to check, meaning that no action was taken when problems arose (K). One project suffered as responsibilities were not clearly defined between different work groups (C), and in the other two cases there was no effective construction management contractor, so no one was responsible for managing the interfaces between multiple smaller pieces of work (E, H).

QA/QC issues also contributed to ten of the nineteen incidents. Poor testing (usually testing conditions not matching service conditions) (K, N), lack of independent inspection (L), fraudulent test certificates (O), product substitution (A, B), gaps in QA scopes (C, D, F, R) and poor links from adverse QA results back into project decision making (K) are the key themes.

For seven of the failure cases, lack of experience and/or expertise within the project team was a significant causal factor. For several projects, this was an issue at several levels, meaning that the supply chain was poorly managed and there was no effective governance/supervision to detect and correct the problem (A, B, F, H, M, N).

Six of the causes linked to supply chain coordination and management are about scope and baseline specifications. In most cases, key information was missing from scope and specification documentation (A, G, M, S), particularly critical contexts such as interfaces with existing systems (E, I).

Moving on to the other three categories in the risk taxonomy, the analysis of failure cases revealed five cases where causal factors were directly linked to suppliers. This might seem surprisingly low, but as noted above selecting the wrong supplier or not supervising suppliers appropriately are classified as supply chain coordination and management issues, rather than a supplier problem per se. Three supplier behavior issues were noted, all related to providing false or misleading information (test certificates, product data) (B, G, O). Two performance issues were noted – both related to constructed facilities that did not meet the required specification (C, D).

Five of the nineteen cases also demonstrated a connection to external risk factors that became contributing causes. Four of these relate to legislation. In some sectors, legislated inspections form part of the risk governance process and in three failure cases, these systems failed with statutory inspections failing to reveal significant problems (A, B, D). In the fourth case, the project experienced delays because of a lack of appropriate engagement with the relevant regulator (E).

Trust and cooperation issues between organizations along the supply chain were flagged as contributing causes in nine of the nineteen failure cases. Common factors include lack of common goals (C) brought about by adversarial contracting arrangements (E) or inappropriate organizational structures/reporting lines (L). In some cases, this leaves known risks unaddressed as people are afraid to speak up (G, K). A low standard of professional ethics was an issue in two cases (A, O).

There are a small number of causal factors identified that do not fit into the risk taxonomy drawn from the literature. They fall into two areas. Firstly, for three of the case studies of procurement failure in an operational environment (Q, R, S), management of change systems failed, effectively meaning that the wrong item was purchased. In three other cases (H, J, M), failures in overall project governance, particularly in the planning stage, meant that procurement problems arose and went unaddressed.

6. CONCLUSION

These failure cases provide input into later stages of the project, but they may be directly useful to the industry in their current form. Experienced professionals learn best by considering cases and the project interim report (FFCRC report RP2.3-06 Risk Governance in Procurement for Future Fuels Interim Report #1 dated March 2022) examines nineteen examples of procurement failures that provide the basis for discussion to reflect on current procurement practices and the potential for the same weaknesses to be present in any specific set of company procurement procedures, policies and practices.

It is apparent that behaviors which are driven by commercial pressures, combined with inadequate attention to assessment of risks and assurance of quality, are significant threats to the procurement process. Based on this review the top five lessons for risk governance from past procurement failures for the pipeline industry to consider are:

- Ensure that a selected contractor or supplier has the technical capability to do the work

  There are many cases in the literature where projects failed due to errors by a supplier or contractor who never should have been selected to perform work in the first place because they did not have the necessary skills and experience to complete their work successfully. In some cases, owner/operators deliberately chose a marginal supplier, noting that extra inspection would be required to ensure a good outcome and then such inspection/supervision was never put in place. Falling into this trap can be avoided by pre-qualifying suppliers and contractors and only inviting bids from groups who are competent to do the work.

- Clearly define responsibilities and supervision

  There are several high-profile procurement failures that have ill-defined responsibilities and lack of effective supervision as a significant causal factor. Interfaces are a known location for errors to arise in organizations so clear responsibilities for all parties and effective supervision

up and down the supply chain is important to ensure any problems are identified early and addressed. This also reduces conflict and misunderstandings. Linked to this is the need for a high level of project team experience and effective project oversight.

- Value QA/QC and make it independent

  Procurement goes wrong when the work of suppliers and contractors is not independently checked or inspected. Problems can arise due to fraudulent test certificates, etc. but not all testing issues are the result of mal-intentions on the part of suppliers. Genuine misunderstandings regarding requirements and/or technical errors occur and are most likely to be identified by a competent, independent inspection focusing on key risk activities. Problems identified must also be taken seriously in the short term because making changes is usually more difficult as time goes on.

- Embed operational requirements into procurement decision-making

  Procurement failures occur when operational requirements are not adequately considered in procurement decisions. This can be avoided by the preparation of specifications to ensure the right operational inputs and outputs are included.

- Establish common organizational goals

  The failure record shows that problems arise when a power balance between client and suppliers/contractors is not achieved and one side becomes highly dominating. An extremely dominating client does not necessarily get the best outcome. For complex projects, 'partnering' style contracts are preferred to align goals and share risk and reward.

7. ACKNOWLEDGEMENT

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

8. REFERENCES

1. Turban, E., et al., *Electronic Commerce 2018: A Managerial and Social Networks Perspective*. Springer Texts in Business and Economics. 2017, Cham: Springer International Publishing AG.
2. ISO, *ISO 31000:2018. Risk Management – Guidelines*. 2018, International Organization for Standardization: Geneva.
3. Vaughan, D., *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA*. 1996, Chicago: University of Chicago Press.
4. Reason, J., *Managing the Risks of Organizational Accidents*. 1997, Aldershot: Ashgate.
5. ICE, *In plain sight: assuring the whole-life safety of infrastructure*. 2018, Institution of Civil Engineers: London.
6. MacLeod, G., *The Grenfell Tower atrocity.* City, 2018. **22**(4): p. 460-489.
7. McKenna, S.T., et al., *Fire behaviour of modern facade materials - Understanding the Grenfell Tower fire.* J Hazard Mater, 2019. **368**: p. 115-123.
8. Hills, J. *Grenfell Tower: Original proposed contractor was dropped to reduce cost of refurbishment project*. 2007 [cited 2021; Available from: https://www.itv.com/news/2017-06-15/grenfell-tower-original-proposed-contractor-was-dropped-to-reduce-cost-of-refurbishment-project.
9. Construction Manager, *Grenfell cladding was replaced with cheaper version*, in *Construction Magazine*. 2017, Construction Magazine. p. 7.
10. Moore-Bick, M., *Grenfell Tower Inquiry: Phase 1 Report Overview. Grenfell Tower Inquiry.* 2019, APS Group: UK. p. 32.

11. Booth, R. *Makers of Grenfell cladding abused testing regimes, inquiry told*. 2020 [cited 2021; Available from: https://www.theguardian.com/uk-news/2020/nov/05/makers-of-grenfell-cladding-abused-testing-regimes-inquiry-told.
12. Voutsadakis, E. and C. Gonzalez, *Grenfell tower fire: the importance of ethics and professionalism for the procurement of safe buildings and infrastructure in the construction industry*, in *International conference on Professionalism and Ethics in Construction*. 2018: London, UK.
13. Booth, R. *Grenfell Tower: 16 council inspections failed to stop use of flammable cladding*. 2017 [cited 2021; Available from: https://www.theguardian.com/uk-news/2017/jun/21/grenfell-tower-16-council-inspections-failed-to-stop-use-of-flammable-cladding.
14. Hackitt, J., *Building a Safer Future Independent Review of Building Regulations and Fire Safety: Interim Report*. 2017, Presented to Parliament by the Secretary of State for Communities and Local Government by Command of Her Majesty: London.
15. KNKT, *Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP Tanjung Karawang, West Java Republic of Indonesia 29 October 2018*. 2019, KOMITE NASIONAL KESELAMATAN TRANSPORTASI: Republic of Indonesia.
16. Majority Staff of the Committee on Transportation and Infrastructure, *Final Committee Report: The Design, Development and Certification of the Boeing 737 Max*. 2020, The House Committee on Transportation and Infrastructure.
17. DoJ, *Boeing Charged with 737 Max Fraud Conspiracy and Agrees to Pay over $2.5 Billion*. 2021, The United States Department of Justice.
18. DoJ, *Former Boeing 737 MAX Chief Technical Pilot Indicted for Fraud*. 2021, The United States Department of Justice.
19. Commerce Committee Majority Staff, *Committee Investigation Report Aviation Safety Oversight December 2020*. 2020, US Senate Committee on Commerce, Science and Transportation.
20. Hayes, J. and S. Maslen, *Buncefield stories: organizational learning and remembering for disaster prevention*, in *The Routledge Companion to Risk, Crisis and Emergency Management* R. Gephart, C. Chet Miller, and K.S. Helgesson, Editors. 2018, Routledge.
21. COMAH, *Buncefield: Why did it happen? The underlying causes of the explosion and fire at the Buncefield oil storage depot, Hemel Hempstead, Hertfordshire on 11 December 2005*. 2011, The Competent Authority for Control of Major Accident Hazards: http://www.hse.gov.uk/comah/buncefield/buncefield-report.pdf.

DISCLAIMER