Brady Heywood.

Technical and Organisational Investigation of the Callide Unit C4 Incident

Month Year

DRAFT

This page is intentionally blank

Brady Heywood.

Executive Summary

EXECUTIVE SUMMARY

Introduction

Between 1:33 pm and 2:07 pm on 25 May 2021, an incident occurred at Unit C4 of the Callide C power station, culminating in its catastrophic failure. There were no fatalities, but the incident destroyed Unit C4's turbine generator and had a major impact on the Queensland electricity transmission grid.

The Brady Heywood investigation into the causes of the incident was undertaken in two parts: the technical investigation identified the engineering causes of the incident, and the organisational investigation identified the organisational factors that contributed to the catastrophic failure of Unit C4.

Technical Investigation

Unit C4 Overview

Unit C4 is a coal-fired turbine generator unit. Coal is burned in a boiler, which heats water and turns it into high pressure steam. This steam expands through a turbine and drives a rotor at 3,000 revolutions per minute (rpm). As the rotor spins inside the generator, it produces electricity that is exported to the Calvale substation, which forms part of the Queensland power grid.

The rotor shaft is held in position by bearings situated at eight locations along its length, see Figure 1.

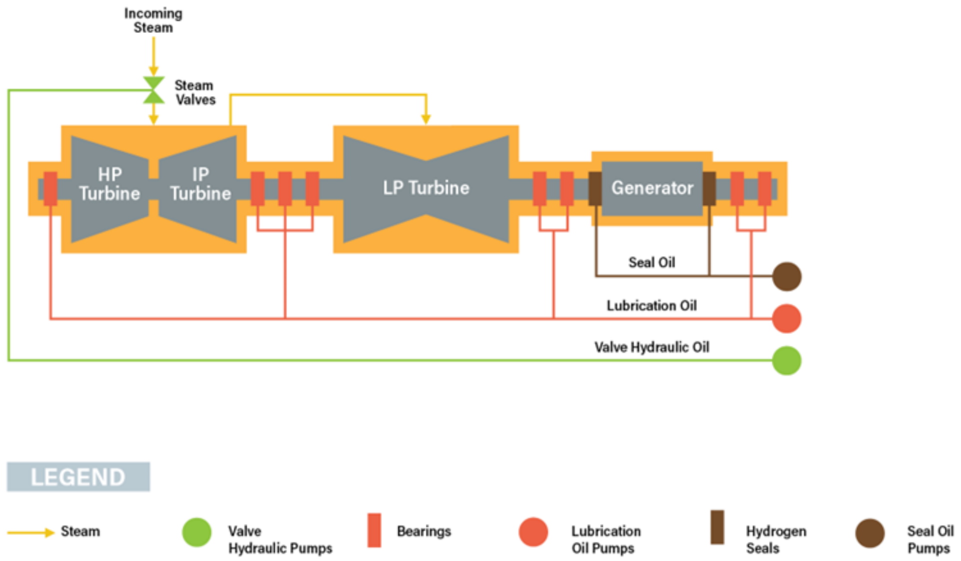

Figure 1 Illustration of the Unit C4 turbine generator

The bearings consist of cylindrical sleeves that are pumped with pressurised oil to provide a thin film of lubrication oil between the shaft and bearings. This allows the rotor shaft to spin freely without metal-on-metal contact.

Inside the generator, the rotor is cooled by pressurised hydrogen gas. To ensure hydrogen does not escape, a seal is created by pumping pressurised oil into the small gap between the shaft and generator casing at each end of the generator.

Unit C4 has two electrical systems, an AC system and a DC system. These systems provide electrical supply to the unit as follows:

- The AC system supplies most of the equipment required for the unit to operate, which includes equipment that provides lubrication oil to the bearings, provides cooling for the unit, and opens and closes valves.
- The DC system supplies the unit's protection, control, and monitoring systems. It also supplies backup equipment, such as the emergency lubrication oil pumps. The protection, control, and monitoring systems detect when the unit has issues and take appropriate action, for example they can disconnect the unit from the grid and shut it down safely.

The Unit C4 DC system is supplied by a battery charger and a battery. The battery charger is the primary source of supply to the DC system, with the battery providing redundancy should the battery charger fail. The battery charger receives its supply from the Unit C4 AC system.

Unit C4 DC Supply Status Prior to Incident

Eighteen months prior to the incident, an upgrade program had been initiated to replace the battery charger in Unit C4. To facilitate this replacement, the Unit C4 battery charger and battery were both taken out of service. With these supplies unavailable, the unit received its DC supply from an alternative source, known as Station DC.

Loss of DC and AC Supply to Unit C4

On the afternoon of 25 May 2021, the replacement Unit C4 battery charger was being brought into service. It was being connected to Unit C4 using a preplanned, formal process for changing the power plant's electrical configuration, known as a switching sequence. During this process, with Unit C4 online and exporting electricity to the Queensland grid, the following took place:

- The replacement battery charger was first connected to the Unit C4 DC system.
- Then the alternative supply, the Station DC supply, was disconnected from Unit C4 in accordance with the switching sequence. At this step in the sequence, the Unit C4 battery had not yet been connected to the unit, which meant the Unit C4 battery charger was the sole source of supply to Unit C4.
- As the sole source of supply, the battery charger was required to instantly respond to the disconnection of the Station DC supply, and maintain the voltage in the Unit C4 DC system. The replacement battery charger, however, did not respond instantly, which caused the Unit C4 DC system voltage to collapse from ~243 V to ~120 V.
- The voltage collapse in the Unit C4 DC system caused one of the unit's protection systems, known as arc flap protection, to respond as if a fault had occurred on the unit's *AC system*. Despite no such fault occurring, the arc flap protection activated and disconnected the AC supply to Unit C4.
- Without AC supply, the replacement Unit C4 battery charger shut down, and with no battery to provide redundancy, this resulted in a complete loss of DC supply to Unit C4 (from ~120 V to ~0 V).

The loss of AC and DC supplies to Unit C4 occurred in less than two seconds, leaving the unit without the two electrical systems needed to operate normally, shut down safely, or disconnect from the grid.

A Failure to Restore DC and AC

There is a switch on the Unit C4 DC system, known as the automatic changeover switch, which can respond if the unit loses DC supply. This switch can automatically reroute DC supply to Unit C4 from another source, which can partially restore the DC system and bring back some of the unit protection systems. The Unit C4 automatic changeover switch had, however, been damaged in a previous incident, and it was not operable in automatic mode on 25 May 2021. DC supply to Unit C4 was not restored.

There is an emergency diesel generator on the Callide C power station which can restore AC supply to Unit C4 if lost. On the day of the incident, the emergency diesel generator operated, but it could not restore supply to the unit. This was because DC supply is required to reconfigure switches on the AC system, so it can receive this supply. With no DC supply, the AC system could not be reconfigured, and AC was not restored.

Motoring of Unit C4

Despite the loss of the AC and DC systems needed to operate the unit in a controlled manner, Unit C4's rotor continued to spin at approximately 3,000 rpm. This occurred because:

- With no AC supply, the turbine's steam valves closed, which resulted in no steam entering the turbine and driving the rotor.
- With no DC supply, the unit's protection systems could not operate, resulting in Unit C4 remaining connected to the Queensland grid.
- With no steam driving the unit, but it still connected to the grid, Unit C4 went from exporting, to importing power from the grid. This imported power resulted in the X tonne rotor continuing to spin by a process called 'motoring'.

In the Callide control room, the Unit C4 display screens went black because of the loss of AC and DC supplies. Without access to key data needed to assess the unit's status, the unit operators were unable to take informed action.

Loss of Key Systems

With the rotor still spinning, the loss of AC and DC supplies to Unit C4 led to the following:

- There was no power to Unit C4's cooling systems, which resulted in the unit overheating.
- No seal oil was being pumped to the generator hydrogen seals, which resulted in the hydrogen escaping, likely causing hydrogen fires as it combusted in the air. This loss of hydrogen, in combination with the loss of other cooling systems, caused the generator to overheat.
- No lubrication oil was being pumped to the bearings, which resulted in the thin film of oil between the rotor shaft and the bearings being lost. The rotor shaft and bearings began grinding metal-on-metal, which created friction and heat that led to the bearings melting and the shaft softening and deforming. The deformations caused the rotor shaft to wobble out of its finely tuned and balanced alignment.

Sustained motoring over a period of 34 minutes, without these systems, led to the catastrophic failure of the unit.

Catastrophic Failure

At 2:06 pm, the wobbling of the rotor shaft likely caused the turbine blades to snag on the metal turbine casing. With the X tonne rotor still spinning at approximately 3,000 rpm, this sudden impact transferred tremendous force to the rotor shaft, which caused the shaft to tear apart at nine locations.

A piece of shaft weighing more than two tonnes was thrown five metres across the floor. A piece of equipment weighing 300 kg, known as the 'barring gear', was ejected 20 metres into the air, punching through the turbine hall roof. The force from the impact also ejected remnants of coupling covers, bearings, and shaft sections from the turbine generator, resulting in widespread damage to the surrounding environment, including the turbine hall's wall and roof. The catastrophic failure of the turbine generator is referred to as the 'turbine missile event'.

After the turbine missile event, the generator remained connected to the grid for approximately 40 seconds. During this time, an electrical fault developed in the generator, causing it to arc and draw high current from the grid – nearly three times the unit's rated export power. The protection systems at Calvale substation responded by detecting the fault and disconnecting the substation from the grid.

The disconnection of the substation at 2:07 pm also disconnected Unit C4 from the grid, concluding the incident. By this time, the turbine generator, along with other equipment, had been destroyed, and Calvale substation's sudden disconnection had initiated the destabilisation of the Queensland grid.

Technical Causes of the Incident

The technical causes of the incident are summarised as follows:

(a) **Switching with Unit C4 online without DC redundancy** – The switching sequence to bring the replacement battery charger into service was carried out with the unit online and no redundancy to the Unit C4 DC system (namely the battery or automatic changeover switch).

This switching sequence, therefore, created a situation that when the Station DC supply was disconnected, the battery charger became the sole source of DC supply to Unit C4. The switching sequence, therefore, required that when Station DC was disconnected, the Unit C4 battery charger would respond instantly and maintain the DC voltage in Unit C4.

(b) **The Unit C4 battery charger** – The replacement Unit C4 battery charger did not respond instantly and did not maintain the DC voltage, which caused the voltage in the Unit C4 DC system to collapse from ~240 V to ~120 V.

(c) **The Unit C4 automatic changeover switch** – The Unit C4 automatic changeover switch, which should operate and partially restore DC supply to the unit in the event of a loss of DC, was damaged and inoperable in automatic mode on the day of the incident. As a consequence, DC supply was not restored to the unit. If the Unit C4 automatic changeover switch had been operable, and had partially restored DC supply to the unit, then the turbine missile event would likely have been avoided, but the unit would still have suffered significant damage.

(d) **Loss of AC** – The DC voltage collapse in Unit C4 directly led to the loss of AC supply to the unit. This occurred because the unit's arc flap protection responded to the DC voltage collapse as if a fault had occurred in the AC system. The arc flap protection then disconnected Unit C4's AC supply.

The loss of AC supply then caused the battery charger to shut down, leading to the complete loss of DC supply to Unit C4.

These factors combined to result in catastrophic failure. The switching sequence was carried out with Unit C4 online, with the only source of supply to the unit's DC system being the replacement battery charger. There was no redundancy to the DC system in the form of a battery or the automatic changeover switch. When the battery charger did not respond as required by the switching sequence, both DC and AC supply to Unit C4 were lost. The loss of these supplies, combined with the unit being online and generating electricity, led to its catastrophic failure.

The catastrophic failure of Unit C4 would have been unlikely or mitigated if any one of these causes had been absent:

(a) **Switching with Unit C4 online without DC redundancy** – The incident could have been avoided if the Unit C4 automatic changeover switch had been operable or the switching sequence had permitted redundancy to the DC system, which would not have required the battery charger to be the sole source of supply. The incident would have also been avoided if the unit had been offline, i.e., with the rotor stationary, the damage to the turbine generator would have been avoided.

(b) **The Unit C4 battery charger** – The incident would have been avoided if the battery charger had maintained the voltage in the DC system and prevented its collapse.

(c) **The Unit C4 automatic changeover switch** – The incident would likely have been mitigated if the Unit C4 automatic changeover switch was operable and had successfully restored DC supply. Upon restoration of DC supply, the unit's protections would have likely responded to the collapse of DC voltage and disconnected the unit from the grid. While there still would have been significant damage to the unit, the turbine missile event would likely have been avoided.

(d) **Loss of AC** – if the DC voltage collapse had not led to the loss of AC supply, then the Unit C4 battery charger would have likely responded to the collapse in DC voltage and restored DC supply to the unit. This would have restored protection systems and likely tripped the unit.

There is no evidence that mechanical or metallurgical factors contributed to the incident, nor is there evidence of a cyber contribution.

Organisational Investigation

The organisational investigation identified the organisational factors that contributed to the catastrophic failure of Unit C4. Organisational factors that directly affected the four technical causes will be discussed first, followed by a discussion of the wider organisational causes that contributed to the incident.

Direct Organisational Factors

Switching with Unit C4 Online without DC Redundancy

On the day of the incident, there was no redundancy to the Unit C4 DC supply. The Unit C4 DC system is typically supplied by a battery charger and a battery. The battery primarily provides redundancy should the battery charger cease operation. The Unit C4 automatic changeover switch also provides redundancy to the DC system because, if lost, it can partially restore DC supply. These two redundancies were unavailable when the switching sequence was being carried out. This created the situation that if the battery charger did not operate as required, DC supply to Unit C4 would likely be lost.

No evidence has been sighted that CS Energy understood or formally considered the risks posed by this lack of redundancy, particularly combined with carrying out the switching with the unit online and exporting power. There was an absence of any formal consideration of these risks, and CS Energy's processes do not require any form of formal risk assessment when planning or executing switching sequences. CS Energy's processes only require consideration of the personal safety risk posed to those undertaking the work, not any risks posed to the wider plant by the switching.

While formal risk assessments would not necessarily have led to avoidance of the incident, they could have increased the likelihood of identifying the risks associated with proceeding with the switching sequence, with the unit online and without a redundant DC supply.

The two redundancies were unavailable for the following reasons:

(a) The switching sequence's steps removed the redundancy provided by the battery. The design of the Callide C power plant dictated that two batteries could not be connected to the same DC system at the same time. As discussed above, when the planned switching sequence commenced, the Station DC system was providing DC supply to Unit C4. But because the Station DC system was supplied by its own battery charger and battery, the Station DC supply (and its battery), had to be disconnected from the Unit C4 DC system before the Unit C4 battery could be connected. Further, the DC system was designed with a physical mechanism in place to ensure the switching sequence proceeded without connecting two batteries to the same DC system.

The physical mechanism and switching sequence, therefore, actively removed redundancy from the Unit C4 DC system. They enforced a step in the switching sequence that left the Unit C4 DC system with no battery connected. While the system's limitation regarding the inability to connect two batteries had been identified following an event in 2010, the proposed actions to understand this limitation were not explored further or implemented.

(b) The Unit C4 automatic changeover switch was inoperable at the time of the incident, as it had been damaged in a previous incident. This inoperability further removed redundancy from the Unit C4 DC system.

No evidence has been sighted that the inoperable status of the Unit C4 automatic changeover switch was considered in preparing or executing the switching sequence, despite its inoperability removing redundancy from the DC system.

This lack of redundancy placed an implicit requirement on the Unit C4 battery charger to instantly respond to the removal of the Station DC supply and maintain the Unit C4 DC system voltage. No evidence has been sighted that CS Energy understood this implicit requirement, considered the risk of the battery charger not performing as required, nor considered the consequences that could result from a lack of performance with the unit online. If the incident had occurred with the unit offline, i.e., with the unit shut down and rotor not spinning, the damage to the turbine generator would have been avoided.

While the design, execution, and decision-making regarding the switching sequence were all in accordance with CS Energy's processes, these processes were deficient because they did not require the consideration of the risks posed by the switching sequence to the wider plant.

In summary, the planning, execution, and decision-making around the switching sequence did not consider the risks associated with bringing the battery charger into service, without DC system redundancy and with the unit online. Nor was there any requirement in CS Energy's processes to do so. This created a situation where if the replacement Unit C4 battery charger did not perform as implicitly required by the switching sequence, DC supply could be lost to the unit.

The Unit C4 Battery Charger

With no redundancy in the Unit C4 DC system, the switching sequence implicitly required the Unit C4 battery charger to maintain the DC system voltage. This did not occur and the DC voltage collapsed, which led to the loss of the Unit C4 DC and AC supplies.

Before being put into service, the replacement Unit C4 battery charger was specified as part of CS Energy's procurement process and was subject to various tests to confirm its compliance with the specification. However, it was neither specified nor tested for the implicit requirements of the switching sequence, and it did not meet them. The replacement battery charger's technical specification appears to have only considered its performance in typical operation, i.e., supplying Unit C4 DC in combination with a battery. It did not specify its performance when operating without a battery.

The differences between these operational requirements are significant. In typical operation, when the battery charger operates in combination with a battery, it is the battery that caters for any sudden changes in demand on the DC system. For example, if there is a sudden increase in demand, the battery will supply this demand instantly, which provides time for the battery charger to respond. In this situation, with a battery connected, the response time for the battery charger is not critical. By contrast, if a battery charger operates without a battery, then its ability to respond to changes in demand must be carefully considered and specified to ensure the battery charger can maintain supply.

The specification for the replacement Unit C4 battery charger contained no such requirements. This contributed to a battery charger that could not meet the implicit requirements of the switching sequence.

In addition to the Unit C4 battery charger not being specified for the requirements of the switching sequence, the battery charger replacement project did not follow an effective management of change process. A failure to effectively manage change is a common causal factor in many major industrial accidents, and effective management of change provides opportunities to understand, evaluate, and mitigate the risks associated with any changes to plant. The project to replace the battery charger should have been subject to CS Energy's management of change process. However, while there is some evidence that this process was followed in the very early stages of the project, no evidence has been sighted that it was followed in later stages. Further, when these processes were followed, they were ineffective in both identifying and understanding the risks associated with the project, and in producing an adequate specification for the battery charger. The Unit C4 battery charger was, therefore, specified, installed, tested and brought into service without effective management of change.

In summary, the battery charger was neither specified nor tested for the switching sequence being carried out at the time of the incident, and CS Energy's management of change process was neither effective nor effectively applied. While an effective management of change process would not have necessarily led to the avoidance of the incident, it could have increased the likelihood of identifying the performance requirements for the replacement battery charger and the risks posed to the wider plant when bringing it into service.

The Unit C4 Automatic Changeover Switch

When the DC voltage to Unit C4 was lost, the Unit C4 automatic changeover switch should have operated and partially restored supply. But the Unit C4 automatic changeover switch was damaged and inoperable on the day of the incident. If it had been operable, and it had partially restored DC to the unit, the turbine missile event would likely have been avoided, but the unit would still have sustained significant damage.

Understanding why the Unit C4 automatic changeover switch was inoperable requires an examination of CS Energy's response to an event that occurred four months prior to the 25 May 2021 incident.

On 13 January 2021, both Unit C3 and C4 tripped simultaneously in what is referred to as a dual trip event. Following the event, the Australian Energy Market Operator (AEMO) placed restrictions on Callide C's power generation. In order to have these restrictions lifted, CS Energy implemented changes to the Callide C power station to prevent another dual trip event occurring. These changes included in the automatic changeover switches for Unit C3 and Station being deliberately rendered inoperable. As a result, if a loss of DC supply occurred in either Unit C3 or Station, the automatic changeover switches would be unavailable to restore supply.

By contrast, CS Energy does not appear to have deliberately rendered the Unit C4 automatic changeover switch inoperable in the same way as in Unit C3 and Station. Following the January event, however, CS Energy identified that the Unit C4 automatic changeover switch was damaged and inoperable in automatic mode (it had blown fuses). While a notification was raised to repair it, no evidence has been found of a work order to complete the repair. On the day of the incident, the Unit C4 automatic changeover switch was still unrepaired and inoperable.

Therefore, by the time of the incident, the Unit C3 and Station automatic changeover switches had been deliberately rendered inoperable, and the Unit C4 automatic changeover switch, with its blown fuses, was also inoperable. CS Energy's investigation report into the January incident shows they were aware of the risks posed by an inoperable automatic changeover switch: they acknowledged that an inoperable automatic changeover switch was removing '*designed redundancy*' from the DC systems.

To restore this redundancy in the long term, CS Energy planned to redesign the Unit C3, Station, and Unit C4 automatic changeover switches. This redesign was planned to occur by the end of November 2021, ten months after the January 2021 event. CS Energy, therefore, planned to leave the Unit C3 and Station automatic changeover switches inoperable for this ten-month period. It is also considered likely that the Unit C4 automatic changeover switch was intentionally left inoperable (and unrepaired) for this time, i.e., it is unlikely that the failure to repair the Unit C4 automatic changeover switch was an oversight.

While CS Energy was aware that inoperable automatic changeover switches were a removal of '*designed redundancy*', no evidence has been sighted to show any management of change or formal risk assessments were undertaken that considered the risks associated with leaving them in this state. The decision to deliberately render the Unit C3 and Station automatic changeover switches inoperable, and leave the Unit C4 automatic changeover switch inoperable, should have been subject to CS Energy's management of change process because this directly affected the reliability of the Callide C power station.

There is also little evidence of a wider discussion within CS Energy regarding the decision to leave them inoperable, nor evidence of a discussion on the risk this posed to the wider plant. For example, those undertaking the switching sequence were unaware the Unit C4 automatic changeover switch was inoperable. No evidence has been sighted to ascertain whether or not the status of the Unit C4 automatic changeover switch was considered in the preparation or decision to proceed with the switching sequence with the unit online.

The Collapse of DC Leading to the Loss of AC

It is considered highly unlikely that CS Energy could have anticipated that the DC system voltage collapse could have led to the loss of Unit C4 AC. There is also little evidence that there was any understanding within CS Energy that if the DC and AC systems were lost, the AC system could not be restored without the DC system reconfiguring the switches.

Summary

The direct organisational factors that contributed to the incident were a failure to understand and address the risks associated with bringing the replacement Unit C4 battery charger into service, and a failure to provide effective management of change with respect to the battery charger and the likely decision to leave the Unit C4 automatic changeover switch inoperable.

While the effective application of risk assessment and management of change processes would not necessarily have prevented the incident, they would have provided an opportunity to identify and manage the risks involved.

Organisational Investigation – Wider Factors

Process Safety

Within high hazard industries, there is a widely accepted and well-established approach to manage the risk of catastrophic failure known as 'process safety'. Before examining the wider organisational factors that contributed to the incident, there are a number of process safety concepts that are useful to understand.

Process safety consists of practices that companies adopt in order to understand and control the catastrophic risks associated with their operations. From an organisational perspective, the catastrophic failure of Unit C4 should be examined through the lens of process safety.

The investigation examined the following process safety aspects at CS Energy:

- CS Energy's organisational context, environment and culture.
- CS Energy's critical risk program.
- The effectiveness of CS Energy's systems, such as management of change.

The sections that follow examine each of these aspects.

Organisational Context

CS Energy has two significant structural influences. As a government-owned corporation it is obliged to meet shareholder mandates, as well as meet the annual performance indicators contained in the Statement of Corporate Intent. In the years leading up to the incident, these mandates focused on cost savings, and performance indicators were dominated by financial and production metrics, as well as personal safety-related metrics. Callide C power station is a 50/50 unincorporated joint venture between Callide Energy Pty Ltd and an international power generation company called Genuity Group (formerly known as Intergen Australia). Shared ownership of the Callide C power station led to increased complexity in its management, including competing asset investment priorities.

More broadly, CS Energy had been through an extended loss-making period between 2008 and 2015. This period overlapped a period of political debate around the privatisation of the State's energy assets, and overlapped with a prolonged dispute with Anglo American regarding the supply of coal to the Callide power stations.

CS Energy also had to respond to the challenge posed by climate change and the energy transition, which has included investment in renewable energy technologies and commencing transforming the power stations from fixed to flexible generators to reduce the cost of production.

After CS Energy returned to profitability in 2015, there was a period of significant organisational reform. Multiple initiatives to improve performance were delivered across the organisation, six of which had direct impact on operations at the Callide site. One of those reforms, discussed in more detail below, was the launch of the Critical Risk Program, which focused on managing the risk of major incidents. Another was the separation of the asset management and operational functions. This reform overlapped with a period of high turnover of Callide site management – between 2017 and the time of the incident, the Callide power station had had four different general managers, three different maintenance managers and five different production managers.

In this context of a focus on financial and production considerations, with the organisation responding to external pressures, such as climate change, special effort was required to foster and maintain a focus on process safety. The Critical Risk Program was intended to provide this focus.

The Critical Risk Program

In response to emerging process safety risks, CS Energy piloted in 2017, and then launched in 2018 , its Critical Risk Program. This program aimed to develop a better understanding of CS Energy's risks across all its sites, and would include both a personal and process safety perspective.

The program started well, and it was consistent with emerging best practice regarding process safety in the power industry. It utilised a site-specific bowtie analysis approach to map out the casual pathways for major risks, and to identify controls to prevent or mitigate the consequences of these risks. The process of developing bowties plays a critical foundational role in the development of an organisation's understanding of its risks, and the controls in place to manage them. It becomes the bedrock for risk competency in an organisation and feeds into critical processes, such as risk assessment and management of change.

But in the two years that followed, the program lost key resources and funding, and changed organisational owners. The planned bowtie analysis for the Callide site, necessary to build process safety competence, was never completed.

A new process safety strategy was then developed in mid-2020, which reduced the critical risk program down to two key components: the development of six organisation-wide and high-level bowties, and the adoption of a single lag process safety metric. These two changes fundamentally and negatively impacted the effectiveness of CS Energy's approach to process safety. These new bowties would not provide CS Energy with detailed insights into its specific risks or of the effectiveness of its controls. The lag metric also had the tendency to support a confident, but unfounded, view of the health of CS Energy's process safety systems – it measured the absence of events, rather than the presence of effective process safety systems. No evidence was sighted that CS Energy at the time analysed or understood the implications of this new approach to process safety.

By the time of the incident, the critical risk program had not materially impacted the understanding or management of process safety risk on the Callide site. Despite this, internal and external messaging presented a confident view that an effective process safety program had been established within CS Energy.

Effectiveness of CS Energy Systems

The independent assurance program, which is delivered by an independent assurance team within CS Energy, reviews parts of the organisation to provide assurance that the internal processes are operating in an efficient, effective and ethical manner.

In the years leading up to the incident, there had been reviews of how CS Energy managed change, how it conducted maintenance work, how it responded and learned from incidents, and the effectiveness of its Permit to Work systems. These are all key systems for the effective management of process safety.

Substantive issues were identified with each of these systems. CS Energy's agreed actions in response to these issues tended to be cosmetic, and rarely addressed underlying causes. The assurance system only monitored completion of those agreed actions, and did not consider whether those actions had improved the effectiveness of the systems.

In particular, the reviews into how CS Energy conducted management of change (plant modification procedure) identified substantive and long-term issues with the effectiveness of this system, which are consistent with those identified in both the procurement of the battery charger and the decision-making surrounding rendering or leaving the automatic changeover switches inoperable.

In relation to how CS Energy learned from incidents, in the two-and-a-half-year period leading up to the incident, the majority of investigations focused on personal safety, with only four incident investigations providing organisational learnings for the organisation with respect to process safety. This left CS Energy with a learning from incident system that provided limited insight into the effectiveness of its systems.

Summary

The failure to effectively implement CS Energy's critical risk program, with respect to process safety, resulted in the organisation not having a comprehensive view of the risks it faced on the Callide site. This vulnerability combined with known issues relating to key systems, such as management of change, resulted in an organisation with a reduced likelihood of being able to anticipate and prevent a process safety incident.

In this context, the failure to understand and assess risk, and to not effectively apply sound management of change processes in relation to the engineering factors that led to the catastrophic failure, suggests these were not isolated incidents, but rather a symptom of an organisation's failure to value and implement effective process safety practices.

This page is intentionally blank

CONTENTS

This page is intentionally blank