Proceedings World Geothermal Congress 2020+1
Reykjavik, Iceland, April - October 2021

Implementing a Safety Lifecycle and Functional Safety Approach on an Existing Organic Rankin Cycle Unit

Benjamin C. Baker, Mathew Staddon and Daniel Pearl

PO Box 2001, Taupo, Waikato, 3352, New Zealand

Ben.Baker@contactenergy.co.nz

Keywords: functional safety, safety lifecycle, IEC 61508, IEC 61511, Organic Rankine Cycle, safety case, Safety Integrity Level (SIL)

ABSTRACT

Changes to health and safety regulations in New Zealand now require that operators of many large industrial facilities prove to the health and safety regulator that their plant is safe to operate. To do this, operations, maintenance, engineering and health and safety personnel have to work together to identify and correct gaps in business processes, equipment and operations that could lead to large-scale industrial accidents. Contact Energy decided to implement a safety lifecycle approach as defined by International Electrotechnical Commission (IEC) standard 61508 (*Functional safety of electrical/electronic/programmable electronic safety-related systems*) and sub-standard IEC 61511 (*Functional safety – Safety instrumented systems for the process industry sector*) as a way of demonstrating adequate reduction of risks. To the owner's knowledge, this is the first time this standard has been fully applied to an existing Organic Rankine Cycle plant. This paper presents a case study of some of the challenges and solutions, both technical and managerial, encountered in this process. The paper also outlines the assessment methodology and some key aspects of the decision making process.

1. INTRODUCTION

Under new health and safety regulations recently introduced in New Zealand, the Wairakei Binary Plant has been classified as an upper tier major hazard facility (UTMHF) due to the quantity of iso-pentane (a specified hazardous substance) contained and used on-site.

The introduction of these regulations prompted the owner to undertake a thorough re-assessment of the risks of a major incident at this facility. As a result, the owner gained a much better understanding of these risks, identified some areas where further risk reduction measures are required, and has committed to a programme of safety enhancements that are currently being implemented.

The owner adopted an IEC 61508 and IEC 61511 based Safety Lifecycle approach for this assessment accordance with their existing policies and practices. This paper provides an overview of the process followed, selected outcomes, and some of key challenges and lessons learned along the way.

2. PLANT OVERVIEW

The Wairakei Binary Plant is a 14-MW Organic Rankine Cycle (ORC) geothermal power station located near Taupo, New Zealand. The power plant was originally commissioned in 2005.

The Wairakei Binary Plant is part of the owner's geothermal fleet in Taupo, which includes five geothermal power station sites and their associated steam production and reinjection facilities, with a current total capacity of over 400 MW. Two of these facilities utilise the ORC, and both are designated as UTMHFs.

The Wairakei Binary Plant consists of two identical ORC generation units. Each unit consists of two closed-loop ORC cycles driving two turbines connected to a single common generator. The Wairakei Binary Plant uses isopentane as the motive fluid (or working fluid) and geothermal brine as a heat source to superheat the motive fluid.

3. REGULATIONS OVERVIEW

The Health and Safety at Work Major Hazard Facilities Regulations 2016 (MHF regulations) came into effect in April 2018, requiring all operators of a designated MHF to prepare and submit a safety case for each UTMHF.

The purpose of a safety case is to provide a written demonstration to the regulator (WorkSafe New Zealand) that the facility is safe to operate. This is achieved by demonstrating that all major incident hazards have been identified and that adequate controls are in place to minimise the risks associated with these incidents so far as is reasonably practicable (SFAIRP).

A major incident hazard is defined as an uncontrolled event at an MHF that:

a) involves, or potentially involves, specified hazardous substances; and
b) exposes multiple persons to a serious risk to their health or safety (including a risk of death) arising from an immediate or imminent exposure to:
   i. 1 or more of those substances as a result of the event; or
   ii. the direct or indirect effects of the event. (New Zealand Government 2017).

The safety case is intended to ensure that special attention remains focused on understanding and controlling the types of high-consequence risks that can potentially occur at facilities that contain large quantities of hazardous substances. These risks, if they

cannot be eliminated, are managed in such a way as to ensure that the likelihood of occurrence is very low and remains so over the life of the facility. In the case of an ORC plant, the main consequences are fires and explosions involving the motive fluid.

Other risks associated with the facility that do not meet the definition of a major incident are managed in accordance with an overarching safety management system and are generally not the subject of the safety case. The safety case for each UTMHF can be considered to be a component of this larger safety management system.

Under the MHF regulations, a safety case should include a detailed summary of the following:

1. The safety assessment undertaken for the specific facility,
2. The safety management system under which the plant operates, and
3. The site-specific emergency plan in place for the facility.

This paper focuses on the safety assessment undertaken for the Wairakei Binary Plant and, in particular, the safety lifecycle approach adopted.

The MHF regulations place a strong emphasis on the need to engage widely with stakeholders in the process of identifying, evaluating and managing major incident risks. This includes direct involvement of a diverse range of employees, emergency services, local authorities, neighbouring facilities, and the surrounding community where applicable.

4. SAFETY LIFECYCLE APPROACH

IEC 61508 defines broad methodologies for the development, operation and maintenance of automated protection systems. This includes all phase of the systems lifecycle including risk assessment, design, commissioning, operation, maintenance, testing, plant modification and decommissioning. The standard sets out a staged approach in which the outcomes from each stage are used to inform subsequent stages, as outlined in Figure 1. IEC 61511 is a substandard of IEC 61508 and provides specific guidance for the process industry (which includes power generation).

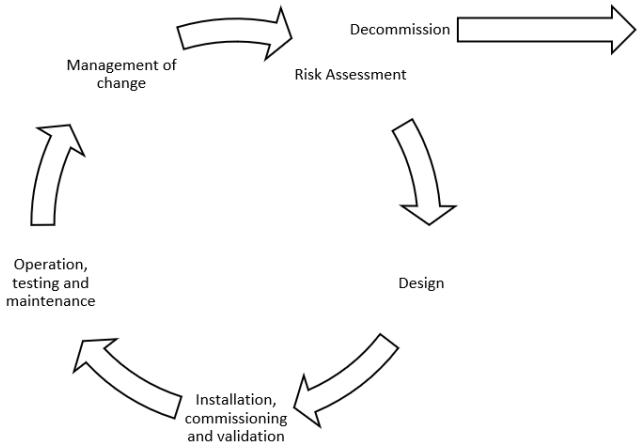

Figure 1: Simplified safety lifecycle.

The owner has previous experience with the implementation of an IEC 61508/61511-based safety lifecycle approach to risk reduction on power generation assets, and has a comprehensive suite of policies, guidelines and procedures to support this process. However, this is the first example of the process being applied to an ORC unit and to an UTMHF operating under a safety case.

This section summarises the assessment process and key findings and uses the specific example of the feed pump emergency isolation system – a new functional safety risk reduction measure identified during the assessment – to explore both the assessment process and the resulting implementation of additional controls in more detail. Similar processes were followed for other major plant components (turbines, vaporizers, motive fluid storage tanks, etc.).

The key steps in the safety lifecycle assessment are:

- Hazard Identification (HAZID)
- Hazard and Operability Study (HAZOP)
- Control Hazard and Operability Study (CHAZOP)
- Consequence modelling
- Layer of Protection Analysis (LOPA)
- Safety Requirement Specification (SRS)
- SFAIRP assessment and demonstration

This quorum of complementary assessment techniques was selected from a larger set of potential tools and techniques available for this type of assessment and was based on the requirements of the MHF regulations, the owner's preferred assessment approach as defined in their Asset Safety Lifecycle System, the configuration of the plant, and the expertise, information and systems available.

A different set of assessment tools and techniques may also be suitable, and the choice will depend on the specific application, available resources, and preferences of the assessor.

The use of a broad range of assessment techniques and participants (backgrounds and skill sets) helps to ensure a thorough and robust assessment. This diversity promotes overlap of differing perspectives, allowing issues to be identified that may otherwise be missed. The MHF regulations specifically require involvement of the wider workforce in the development and rollout of safety cases for this reason. The use of workshop-style techniques such as HAZID, HAZOP and CHAZOP are well suited to accommodating the input of a wide range of participants. For the Wairakei binary plant, representatives from engineering, operations, maintenance, health and safety, external contractors, and other parties were heavily involved in the assessments.

4.1 Risk identification

The first step in the safety assessment is the identification of hazards. Two primary techniques were employed for this process: HAZID and HAZOP.

The HAZID process is used to identify general hazards and perform a first-pass qualitative risk assessment. In this technique the plant is broken down into manageable sections, usually into major components such as vessels, turbines or pumps. A set of guide words is used as a prompt to help the assessment team identify similar hazards at the facility.

The HAZOP study is more focused and looks at individual components and failure modes (such as misoperation, or a transmitter failing high, low or in place) to identify those that could lead to a hazardous event. Understanding these pathways to failure is the main purpose of a HAZOP study.

Later in the design process, the owner conducted a CHAZOP study. This study is similar in form and content to a HAZOP but concentrates on the electrical, control and instrumentation design. A set of guide words specific to control systems is used.

The use of well-defined HAZID, HAZOP and CHAZOP processes helps to promote a robust and systematic approach to the identification of hazards. For these techniques to be used successfully, the owner should have well-defined procedures, methods and risk evaluation criteria for each assessment type.

However, it's important to note that these techniques typically do not address all risks. Some risks are better addressed in the general engineering design review process. Risk identification studies such as HAZID and HAZOP assume that the plant meets minimum code requirements for pressure equipment, electrical and environmental safety. The goal of these studies is to identify hazards which are not addressed directly in prescriptive codes and require special protections and design consideration.

For the Wairakei Binary Plant the qualitative outputs from the risk identification studies were then passed on to other assessment techniques (such as LOPA) to further refine and quantify these risks before and after the application of mitigation strategies.

For the Wairakei Binary Plant these risk assessments identified a number of areas in which further risk reduction measures needed to be considered. A specific example is the motive fluid feed pumps, where the risk of a fire or explosion caused by a failure of the feed pump mechanical seal (API Plan 54) was identified. Several such feed pump seal fires have occurred in New Zealand in the past. Given the proximity of the feed pump to the condenser, these fires have the potential to rupture condenser tubes and continue to escalate. It was determined that the existing manually operated valves could not be safely or effectively used to isolate the inventory in the event of a fire. Automated inlet and outlet shutoff valves, which would be triggered by flame and gas detectors or in the event of a seal oil system failure, were proposed as an additional control; see Figure 2 and Figure 3. Additional monitoring of pump vibration, motor bearings and cavitation was also incorporated. Similar features have been installed on newer ORC units.

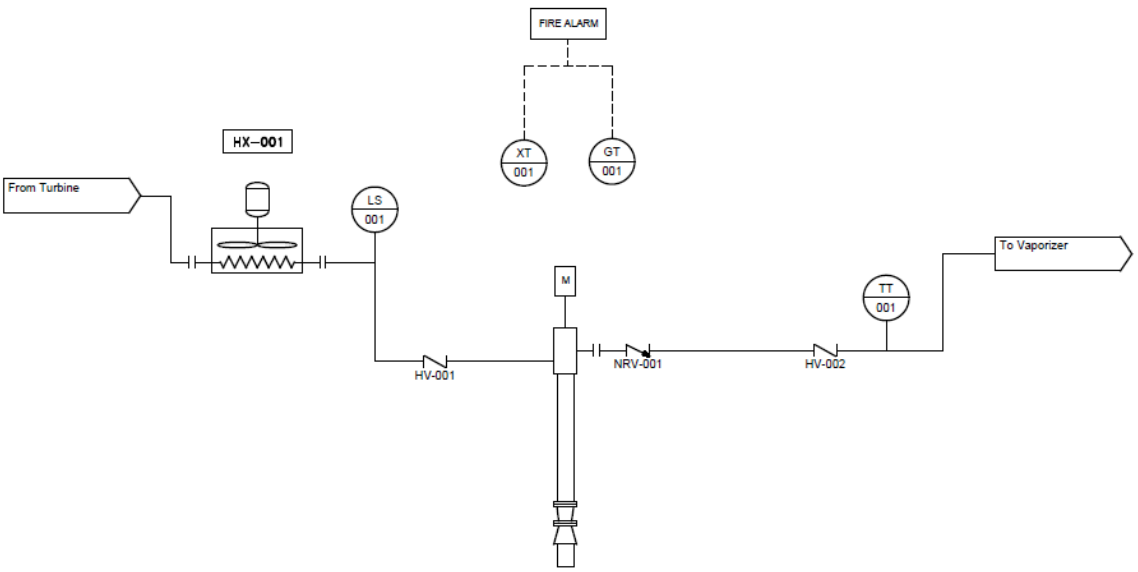

Figure 2: Initial feed pump configuration.

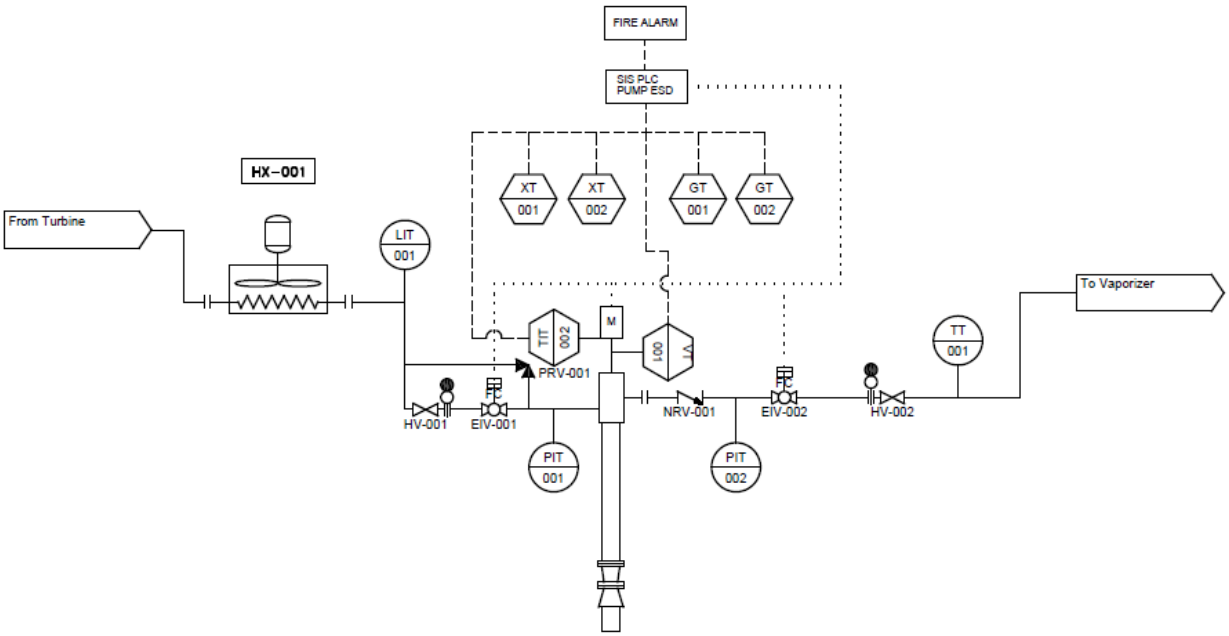

Figure 3: Final feed pump configuration.

4.2 Consequence analysis

Consequence analysis involves the detailed modelling of the major incident risks identified in the HAZID and HAZOP processes. For the Wairakei Binary Plant, the consequence analysis focused on the fire and explosion hazards resulting from accidental releases of iso-pentane. Consequence analysis employs detailed numerical modelling techniques and/or computer simulations to help establish both the plausibility and possible impact of these events. The specific release location, process and environmental conditions, site layout and other factors were modelled in order to accurately determine the likely maximum impacts of these events.

This analysis can be used to determine, for example, if the process conditions and failure mode can support the formation of a jet fire, and if so, how far this jet fire is likely to extend and how long it is likely to last. Other types of incidents modelled included flash fires, pool fires, vapour cloud explosions (VCEs), boiling liquid evaporation vapour explosions (BLEVE), and dispersion of non-ignited flammable or toxic vapours.

Consequence analysis is necessary because the safety assessment requires an accurate understanding of both the likelihood and the consequences of major incident scenarios in order to properly evaluate the overall risk. The analysis quantifies the potential for these events to cause harm to personnel and equipment, impact neighbouring facilities and cause escalation events.

In some cases, the consequence analysis may reveal further incidents or escalation scenarios that should be considered further, or it may disprove the credibility of a particular risk. For example, the toxic effects of pentane were determined to present no credible risk of serious harm to multiple persons. Risks from acute toxic exposure are present only at very high concentrations. Modelling revealed that these very high concentrations would occur only in very close proximity to the leak site (i.e., within a few meters), and it was determined that any risk of serious harm would be insignificant relative to the associated fire or explosion risks.

Relief valves capable of releasing iso-pentane to the atmosphere were also modelled to determine whether a flammable atmosphere could develop at ground level (and therefore result in a flash fire or VCE) during a release, and also to model the extent of thermal radiation that would be produced if a jet fire developed during release.

Figure 4 shows the maximum serious harm consequences from a pool or flash fire resulting from a mechanical seal failure on a feed pump.

4.3 Layers of Protection Analysis

Layer of Protection Analysis (LOPA) is a quantitative risk assessment technique that determines whether adequate independent protection barriers exist or if there is a need to either strengthen the existing barriers or recommend additional ones.

LOPA provides a robust and systematic approach for calculating the effectiveness of aggregate risk reduction measures including the impact of safety instrumented systems, passive protections, procedures and other mitigations. Because LOPA is a quantitative technique, it is possible to estimate the likelihood of the event occurring and compare this to established levels of risk tolerance (Target Mitigated Event Likelihood, or TMEL). If the risk remains above tolerable levels, LOPA can be used to accurately determine what level of additional mitigation is required, and the specific performance requirements these barriers must achieve. Generally, risks with higher consequences have lower tolerable exposure limits as shown in Table 1

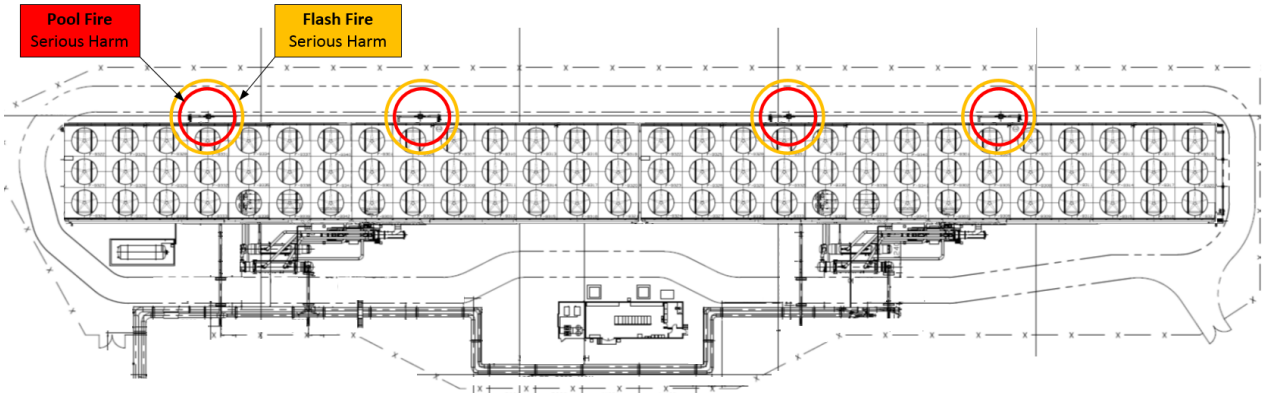

Figure 4: Example: Pool and flash fire serious harm consequences resulting from feed pump mechanical seal failure

Table 1 TMEL for various consequences severities

Consequence Rating	TMEL (Tolerable Likelihood per Year)	Tolerable Occurrences per Years
6 (catastrophic)	10^{-6}	1 in 1,000,000
5 (critical)	10^{-5}	1 in 100,000
4 (major)	10^{-4}	1 in 10,000
3 (serious)	10^{-3}	1 in 1,000
2 (moderate)	10^{-2}	1 in 100
1 (minor)	10^{-1}	1 in 10

A LOPA calculation is made up of the following components:

- initiating events likelihood,
- prevention barriers,
- hazard scenario and consequence, and
- mitigation factors.

4.3.1 Initiating events

Each of the major incident hazards is assessed in a separate LOPA. A major incident may have multiple initiating events. The initiating event frequencies are given (in occurrences per year) based on the owner's experience and/or available industry data. The initiating event likelihoods are then added together to calculate the overall likelihood of the event occurring (in occurrences per year).

4.3.2 Prevention barriers

Barriers capable of preventing the major incident from occurring are then identified, and the likelihood of each barrier not successfully operating when it is called on to do so is calculated (this is referred to as the Probability of Failure on Demand, or PFD).

PFD values are calculated using either the information provided by the equipment manufacturers or on the basis of historic or industry-accepted values. IEC 61508 contains a rating system for classifying the PFD of electronic actuated safety systems called the Safety Integrity Level (SIL). During the initial LOPA, target SILs are set for each independent barrier; the actual PFD is then calculated when a final design and component-specific information are available (see section 4.4). The SIL level is defined as a range of PFD values, as shown in Table 2.

Table 2: Safety Integrity Level vs Reliability

Safety Integrity Level	PFD Range	Failure Rate in Years
SIL 1	1×10^{-1} to 1×10^{-2}	10 to 100 years
SIL 2	1×10^{-2} to 1×10^{-3}	100 to 1,000 years
SIL 3	1×10^{-3} to 1×10^{-4}	1,000 to 10,000 years
SIL 4	1×10^{-4} to 1×10^{-5}	10,000 to 100,000 years

Confirming the independence of barriers is of critical importance. If multiple barriers can be affected by a common cause fault, for example, a faulty input card on a PLC (programmable logic controller), PLC coding errors, or the failure of a common final element (such as a turbine stop valve), the barriers are not truly independent of each other and only one layer of protection can be counted (for risk reduction) in the LOPA.

4.3.3 Hazard scenario and consequence

The major incident hazard scenario and its consequence are derived from the HAZID, HAZOP and consequence analysis.

4.3.4 Mitigation factors

Mitigations or modifiers that have an influence on either the likelihood of the event occurring or the severity of the consequence are then identified and evaluated. These mitigations or modifiers can include the likelihood of an ignition source being present in the event of a pentane leak or the likelihood of a person being in the area when the fire or explosion occurs.

4.3.5 Calculation of risk and other considerations

The likelihood of initiating events occurring is then combined with the likelihood of all prevention barriers failing to act as required, the maximum consequence being realised, and the influence of mitigating factors taken into account in order to calculate the overall level of risk; see Figure 5. This is then compared to a predefined acceptable risk target (or TMEL), shown in Table 1.

If the predicted frequency of the event occurring does not meet the TMEL, additional barriers or mitigations need to be added or the reliability of existing layers needs to be increased until it does. The preference should be to add or strengthen prevention barriers rather than add or strengthen mitigation measures (such as fire systems) where possible, as it is generally easier to keep an accident from occurring than to prevent it from escalating.

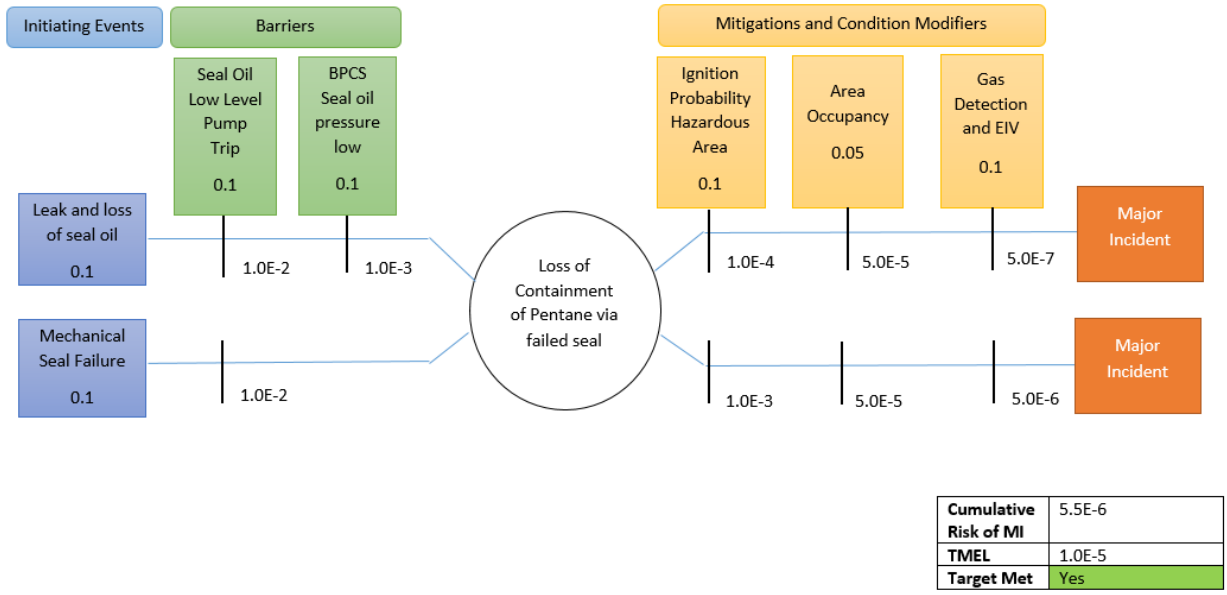

Figure 5: Example LOPA diagram and calculation. Note this is a simplified diagram, not all actual initiating events shown.

In its existing state, the following independent barriers were in place that were capable of detecting/preventing a pentane leak at the feed pumps:

1 Seal oil low pressure switch,
2 Operator rounds and routine monitoring,
3 Flame and gas alarm.

To meet the TMEL (Table 1**Error! Reference source not found.**) the following independent layers were added:

1 SIL 1 flame and gas detection triggering feed pump stop and isolation,
2 SIL 1 high and low seal oil level triggering feed pump stop and isolation,
3 SIL 1 pump shaft run-out triggering feed pump stop,
4 PLC pump motor thrust bearing temperature monitoring triggering feed pump stop,
5 PLC seal oil pressure monitoring triggering feed pump stop,
6 PLC seal oil return temperature monitoring and alarm,
7 PLC pump cavitation monitoring and alarm,
8 PLC condenser level transmitter and pump interlock.

Table 3 shows the change in overall risk exposure before and after these additional controls were added. See section 5.1 for further information.

Table 3: Risk Reduction Factors

	Target Frequency	Calculated Frequency	Required Risk Reduction Factor
On-Site Serious Injury Before	1×10^{-5}	1.5×10^{-3}	1.5×10^{2}
On-Site Serious Injury After	1×10^{-5}	1.3×10^{-6}	N/A

4.4 SRS (& PFD)

If it has been determined that an additional layer of protection in the form of a Safety Instrumented System (SIF) is required, it is necessary to carefully define the functional and integrity requirements for the SIF. This is referred to as the Safety Requirement Specification (SRS). The SRS is the key document that defines how the system is to be designed, validated, tested, maintained and operated. The SRS should describe the following:

1. design and architecture;
2. reliability (nuisance trip rate);
3. availability (SIL);
4. support systems;
5. installation, testing and maintenance;
6. hardware specification; and
7. software development and security.

The SRS is developed in an iterative process that is initiated in conjunction with the initial PFD calculations. It is necessary to do this early in the development process to ensure that the design is at least capable of meeting the performance requirements identified in the LOPA before proceeding to detailed design. Further development of the SRS continues into the detailed design phase as the specific components are selected and the testing and maintenance requirements are further understood.

Two areas of the SRS in which issues commonly arise and which therefore require special attention are (1) design and architecture and (2) installation, testing and maintenance.

4.4.1 Design and architecture

Key design and architecture considerations can have a significant impact on the cost and effectiveness of a SIF. Understanding and managing these impacts at an early stage in the development process (when the concept SRS is developed) and considering these decisions from a safety lifecycle perspective are very important if a good balance of overall cost, benefit and risk is to be achieved.

For example, when a designer is considering turbine configuration and over-speed protection, they may consider the option of having a single or double turbine inlet. The double inlet configuration may have some benefits (smaller and cheaper valves, pipework flexibility, etc.). However, the implications for the operation of the SIF can be significant. It is more difficult to achieve SIL 2 performance across the entire SIF for the double inlet configuration because two valves are required and both must close successfully to protect the turbine. This means that higher-integrity components will be required to achieve an equivalent PFD relative to the single inlet configuration, including higher-integrity turbine stop valves and actuators (final elements).

Not all components of the SIF contribute equally to the overall PFD of the SIF. Final elements have the most significant impact on the average PFD rating of the SIF, and therefore more expensive valves and actuators are likely to be required; see Figure 6. In many cases, the additional costs associated with the SIF may outweigh the benefits realised in other areas of the design.

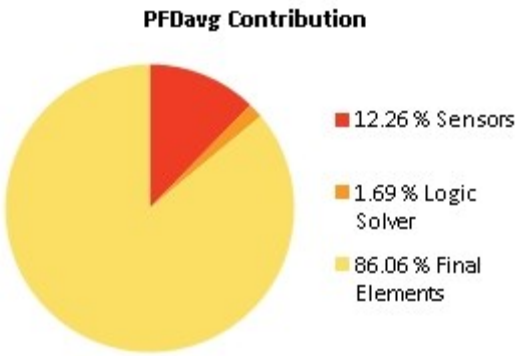

Figure 6: Typical result of average PFD contributions. The reliability of the final elements (valves, breakers, etc.) dominates.

4.4.2 Installation, testing and maintenance

Installation, testing and maintenance requirements can have a significant impact on the lifecycle costs and benefits of a SIF and should be considered carefully at an early stage in the development process. The SRS should clearly identify these requirements so that the implications can be carefully considered before a final design is established.

For example, the required PFD may be achieved by using lower-integrity components and increasing the testing frequency. However, increasing the test frequency may have a detrimental impact on plant output, or require increased maintenance effort, that far outweighs the SIF component cost savings. This may be avoided by adopting a design that allows online testing of a final element (like partial stroke testing of a turbine stop valve). However, this design may necessitate other design changes, such as the implementation of overrides or pressure relief functions, which may again outweigh the SIF component cost savings.

The frequency of inspection and testing can have a significant impact on the average PFD of a SIF, and this should be understood and taken into consideration when a system is designed. Figure 7 illustrates the impact of different inspection and testing regimes on the feed pump emergency isolation system developed for the Wairakei Binary Plant. Increasing the testing frequency lowers the average PFD.

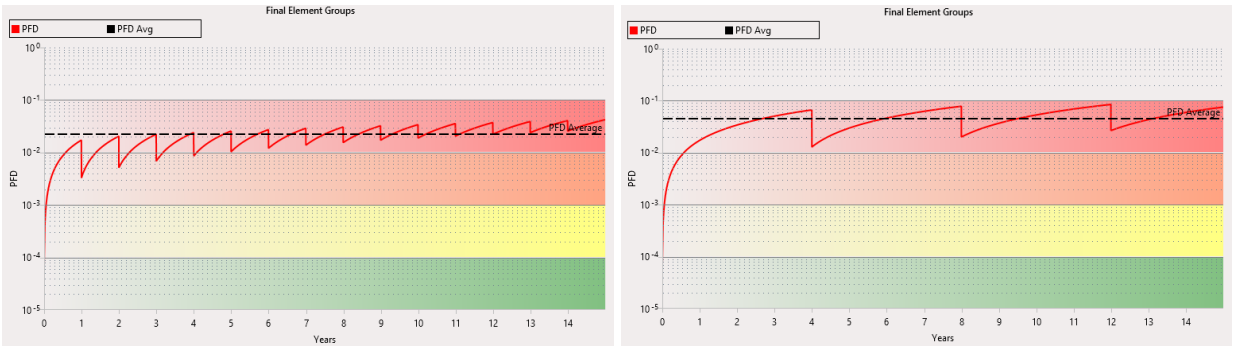

Figure 7: Average PFD plots for feed pump seal oil level trips. Left: Annual testing with a PFD Average of 2.23×10^{-2}. Right: Testing every 4 years with a PFD Average of 5.33×10^{-2}.

4.5 SFAIRP

The MHF regulations require risks associated with major incidents to be reduced SFAIRP. For major incident risks, it is necessary to first identify risk reduction measures that are capable of reducing these risks to tolerable levels (using techniques such as LOPA) and then continue to identify and implement further risk reduction measures if it is reasonably practicable to do so.

The process generally involves the following key steps:

1. Identification of further risk reduction measures
2. Determination of technical feasibility of the proposed risk reduction measures, and
3. Determination of whether it is reasonable to implement these further risk reduction measures.

The identification of further risk reduction measures was conducted in a multi-disciplinary workshop environment similar to that employed for other risk studies. Once a control measure has been selected for consideration, it is then necessary to determine if it is technically feasible. Technical feasibility is typically an evaluation made by appropriately experienced and competent personnel, using good engineering practice. Control measures that are not technically feasible are not required to be considered further. If the control measure is technically feasible, it is necessary to test whether the control measure is reasonable to implement. This is typically a trade-off between the risk benefit of the control measure and the cost (time, resources and monetary cost), with the following parameters tested:

- Level of risk reduction offered by the control measure;
- Incident severity that the control measure protects or mitigates against;
- Reduction in incident likelihood that the control measure offers;
- Control measure effectiveness and the ability of it to perform its function when required;
- Whether other control measures that can eliminate or better mitigate the risk are available; and
- The cost of the control measure, which should take precedence over safety only when it is grossly disproportionate to the risk.

Where a control measure is considered to be technically feasible, it should be implemented, or justification should be provided for why it should not. Cost is considered last, in which case the test of gross disproportion is applied, with a control measure being rejected only when the cost is considered grossly disproportionate to the risk benefit gained.

The extent to which the cost outweighs the benefit can be described as a Disproportion Factor (DF). When that factor exceeds a certain threshold, it demonstrates that the additional measure is not reasonably practicable to implement. For this approach to be implemented, the owner is required to establish a justifiable DF (a typical value is 5).

$$Disproportion\ Factor, DF = \frac{Cost\ of\ Additional\ Control}{Value\ of\ Risk\ Reduction\ achieved\ by\ the\ control}$$

where:

$$Cost\ of\ Additional\ Control = Initial\ capital\ cost + [(annual\ operation\ and\ maintenance\ cost) * (life\ of\ the\ facility)]$$

$$Value\ of\ Risk\ Reduction = [(Current\ annual\ risk - residual\ annual\ risk\ with\ the\ additional\ control\ in\ place) * (life\ of\ the\ facility) * (financial\ value\ of\ risk)]$$

All proposed risk reductions were evaluated in a SFAIRP workshop attended by a cross section of the workforce. The participants were asked to identify other potential risk reduction measures that could be considered in addition to the risk reduction measures already identified in the risk assessments,. In some cases, this involved risk reduction measures known to have been implemented at other similar facilities but not specifically identified as necessary at the Wairakei Binary Plant.

A total of 50 risk reduction measures were accepted for implementation for the entire facility, with another 7 pending further investigation and review. Twelve risk reduction measures required no action to be taken, because the measure was not applicable to the plant, alternative control measures were implemented, or existing control measures were already in place. Eight risk reduction measures were rejected.

4.6 Stakeholder engagement and emergency response planning

The MHF regulations set out specific requirements for stakeholder engagement and the development of a UTMHF-specific emergency response plan appropriate for managing the major incident hazards identified in the safety assessment.

The broad goal of the stakeholder engagement requirements set out in the MHF regulations is not only to make impacted parties aware of the potential consequences of major incidents at the facilities but also to encourage their participation in the risk identification and reduction process.

The development of the safety assessments and emergency response plans required extensive engagement with a broad range of stakeholders, including:

- The workforce (including selected contractors as appropriate),
- Other UTMHF operators,
- Impacted neighbours,
- Emergency services, and
- Local authorities (local and regional government).

The owner worked extensively with another ORC operator in the development of the safety assessment and emergency response plans. This approach was beneficial for both parties, providing a larger pool of resources, more diverse viewpoints and the opportunity to challenge some entrenched organisational norms. The parties also worked in close cooperation to develop commonly structured emergency response plans, and to conduct joint emergency response exercises in an effort to reduce the burden on emergency services and ensure a clear and consistent response to major incidents at similar facilities.

Some neighbouring businesses were identified as being at risk from the direct consequences of a major incident. Representatives from these businesses were invited to be involved in the development of emergency response plans and, in some cases, in the safety assessment workshops and development and implementation of risk reduction measures at their facilities.

Local authorities were informed of the major incident risks associated with the facility, the current level of risk exposure, plans for further risk reduction, and the emergency management plans in place.

5. IMPLEMENTATION OF FUNCTIONAL SAFETY UPGRADES

5.1 Overview of feed pump upgrades

One of the key outcomes of the safety assessment was that further risk reduction measures were warranted in some areas. These were presented in the safety case in a Committed Further Actions Plan, which included implementation timeframes. The additional risk reduction measures included additional functional safety enhancements, further investigation, changes to processes and procedures, changes to emergency response facilities and procedures, and other enhancements. A total of 56 committed further actions were included in the safety case for the Wairakei Binary Plant. A list of the actions and upgrades related to the feed pump emergency isolation system is provided in Table 4.

Table 4: Feed Pump Upgrades

Action	Reason for Risk Reduction Measure
Installation of new SIS PLC to replace existing hard-wired shutdown systems and modifications to final elements to meet Safety Integrity Level (SIL) requirements	A truly independent (from the basic plant control system) high-integrity safety PLC was necessary to support the implementation of numerous safety instrumented functions, including the feed pump emergency isolation system. This included the stand-alone safety system infrastructure and significant modifications to final elements such as feed pump emergency isolation valves, etc. These modifications were necessary to achieve the low PFD values necessary to achieve the risk reduction benefits being sought.
Installation of slam-shut valves on either side of the pentane feed pumps that can be automatically and manually closed if a fire or gas leak is detected	New SIL-rated full bore ball valves fitted with spring return actuators were installed on the inlet and outlet of the feed pumps. Full bore valves were selected to avoid exacerbating dynamic head losses in the existing pipework. Spring return actuators were selected to ensure the valves would close in the event of control air system failure. Metal seated ball valves were selected because they are inherently fire safe and do not require the spring return actuator to hold the valve closed in the event of a fire or extended duration event.
Feed pump vibration monitoring and trip	SIL-rated shaft run out transmitters were selected. These transmitters initiate a pump shutdown when pump run out approaches maximum acceptable levels for the seal.
Enhancement of gas and flame detectors	Additional SIL-rated flame and gas detectors were installed near the feed pumps to enhance coverage and redundancy. The fire and gas detectors were migrated from the existing fire system to the independent safety system in order to increase system integrity (decrease PFD) and support the level of risk reduction required. Activation of any one flame or gas detector will initiate an emergency shutdown of the plant and closure of the emergency isolation valves (EIV).
Addition of feed pump seal oil tank level trip (high and low)	New SIL-rated guided wave radar level transmitters were installed in the feed pump seal oil tanks to detect failure of the seal system including loss of oil and leakage of pentane into the seal oil system. Potentially dangerous oil levels initiate a plant shutdown and closure of the EIVs.
Installation of new feed pump bearing temperature monitoring with high temperature alarm and trip	New bearing temperature transmitters were installed near the pump motor drive end bearings. These transmitters support long-term monitoring of bearing temperatures and can initiate a plant shutdown via the basic plant control system.
Installation of feed pump seal oil low pressure trip	New feed pump seal oil pressure transmitters that are capable of initiating a plant shutdown via the basic plant control system were installed.
Replacement of feed pump seal temperature gauge with a transmitter	The existing seal oil temperature gauge was replaced with a transmitter. A high seal oil temperature will initiate a normal plant shutdown via the basic plant control system.
Upgrade of condenser pentane level switch to a transmitter	This permits better monitoring of condenser level. A low level causes pump cavitation due to lack of head. On low low level, the pump will turn off until condenser level recovers.
Replacement of manual butterfly valves with gate valves and addition of spectacle blinds	To allow for better isolation during maintenance, the existing butterfly valves were replaced with gate valves and a spectacle blind was added inboard. This allows for better isolation of the pump and reduced leakage across the valves during purging. Replacement of the butterflies with full bore gate valves also had the added benefit of reducing pressure drops in the system.
Installation of feed pump inlet relief valve	An additional pressure relief valve was required to protect the new isolatable volume of pipework created by the fed pump emergency isolation valves. This relief valve discharges to the condenser.

5.2 Key challenges

5.2.2 Removal of pentane for upgrades and maintenance

To install new emergency isolation valves around the feed pumps, the owner had to perform hot work including welding and grinding. To safely perform hot works it was necessary to reduce the pentane vapour concentration in the circuit to significantly below the lower explosive limit (LEL) of pentane (American Gas Association 2001). Hot tapping, stopples and other in-process installation methods were considered but dismissed because of cost, availability or dimensional constraints.

No purging procedure was available and the pentane storage tank capacity was too small to hold the full pentane inventory. However, some similar ORC facilities were known to undertake this process on a routine basis. The owner was invited by the OEM to observe this procedure being performed at one of these facilities A Wairakei Binary Plant specific procedure was then developed and reviewed using a procedural HAZOP (similar to the HAZOP described above but with procedure-specific guide words).

Nitrogen gas was used to pressurise the pentane circuit, allowing liquid pentane to be safely transferred to mobile tankers and then transported to a registered hazardous area storage facility for the duration of the works. With the majority of the liquid pentane removed, a large vacuum pump was used to vapourise the remaining liquid in the circuit. Nitrogen gas was then introduced into the circuit, and this process of drawing vacuum and breaking with nitrogen was repeated until the necessary concentration was achieved.

This operation takes approximate 3-4 days per unit to complete. This process requires specialist equipment such as a hazardous-area-rated vacuum pump and a high volume nitrogen supply, as well as specialist contractors to operate the equipment.

Nitrogen and vacuum purging has now become standard practice at the owner's facility for all work on motive fluid systems.

5.2.3 Communicating the need for change

When reassessing fundamental risks and safety systems on an aging facility through the lens of new regulations and assessment techniques, it is quite likely that previously unidentified issues will be revealed. This may lead to a recommendation for expensive upgrades, changes to operational and maintenance behaviours, or other challenges to organisational norms.

Effectively communicating the need for these changes can be challenging, particularly for an existing facility that was otherwise understood to have operated safely in the past. The application of established assessments methodologies such as the safety lifecycle approached defined in IEC61508/61511 can be used to support and justify these arguments.

5.2.3 Experience and capability in the industry

The owner's experience was that the expertise required to complete an assessment of this type was not readily available in the New Zealand market, and ideally some core expertise should be developed and retained in-house. This in-house competency should include an understanding of IEC 61508/61511, functional safety and other aspects of asset safety lifecycle management in order to ensure that safety systems and procedures are appropriately designed, monitored and maintained so that they continue to provide the level of risk reduction required over the lifetime of the facility.

IEC 61511/61508 has not historically been prescribed as a requirement by asset owners in the New Zealand power industry. On occasion, these standards have made it into the asset owner's technical requirements, but neither the supplier nor the asset owner fully understood what was required. As corporate knowledge and understanding of risk improves, so does the understanding that ownership of risks and responsibilities cannot be transferred to a third party.

To achieve compliance with IEC 61511/61508, every decision that affects functional safety throughout the lifecycle of the plant has to be well managed. This includes concept design, detailed design, commissioning, maintenance, operation and decommissioning phases. To achieve this, appropriately trained people must be involved in all aspects of the project lifecycle. This will require functional safety awareness training for engineers, operators, as well as maintenance and managerial staff.

In the past, process and functional safety may have been seen as the responsibility of the designer. However, it is important to consider that the operation phase of the functional safety lifecycle is usually the longest.

5.2.4 Maintenance and performance monitoring

The focus of the operational phase of the safety lifecycle is to ensure that all safety functions operate as designed (as defined in the SRS) over the operational life of the plant. For the Wairakei Binary Plant this resulted in the need for increased monitoring, maintenance, and testing effort including the development and implementation of:

- Detailed performance standards defining minimum performance, monitoring, testing, verification, maintenance and audit criteria for all safety critical equipment
- New maintenance, inspection, and testing routines to support these performance standards
- New procedures, check sheets and other resources required to support these routines
- A digital dashboard for tracking both leading and lagging indicators of system performance, such as preventative maintenance scheduling (leading) or failures of key systems (lagging)

6. CONCLUSION

A safety lifecycle approach based on IEC 61508/61511 was used as the basis for the development of a safety case for the Wairakei Binary Plant. This method was used to identify and evaluate plant risks, determine where additional risk reduction measures were

required, configure and specify the most appropriate risk reduction measures, and ultimately demonstrate that risks of major incidents at the facility were, or would be, reduced SFAIRP.

A safety lifecycle assessment of an existing facility may reveal significant risk reduction shortcomings. In the case of the Wairakei Binary Plant, the need for an extensive programme of safety upgrades and other operational and organisational changes was identified. This situation can present organisational challenges in terms of justifying significant additional costs and changes to current practices for an existing plant that may have previously been understood to be safe. However, a safety lifecycle approach based on IEC 61508/61511 can be used to develop a robust and compelling justification.

References

American Gas Association. *Purging Principles and Practice.* Washington DC: American Gas Association, 2001.

Center for Chemical Process Safety. *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis.* New York: Wiley, 2015.

Center for Chemical Process Safety. *Layers of Protection Analysis Simplified Process Risk Assessment.* New York: American Institute of Chemical Engineers, 2001.

International Electrotechnical Commission. *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.* Geneva: IEC, 2010.

International Electrotechnical Commission. *IEC 61511: Functional safety - Safety instrumented systems for the process industry sector.* Geneva: IEC, 2016.

New Zealand Government. "Health and Safety at Work (Major Hazard Facilities) Regulations 2016." Wellington: Parlimentary Counsel Office, 1 December 2017.