TCI RISK MANAGEMENT

LOPA Report
BLPH to Onshore
Crosswind

TCI Doc. nr: CW-25-001-R03

Issue: 1.0

Date: 17 September 2025

TCI Risk Management © 2025

This document has been prepared by TCI Risk Management BV. Subject to any contractual terms between TCI Risk Management BV and its client to the contrary, it is the property of TCI Risk Management BV. It shall not be reproduced in whole or part, nor disclosed to a third party without the express written permission of the owner. This document has been specifically prepared for the client of TCI Risk Management BV and no responsibility to third parties is accepted unless expressly agreed in writing.

ISSUE RECORD

Version	Date	Author	Reviewer	Approver	Revision History
1.0	17-09-2025	Farrah Adzhar	Jordi Alkemade	Stefan Otting	Issue to client

DISTRIBUTION

TCI Risk Management	Delft, The Netherlands
Crosswind	Den Haag, The Netherlands

HOLDS

1. Ballard linear heat detection SIL rating

EXECUTIVE SUMMARY

The Base Load Power Hub (BLPH) is an innovative project of Crosswind (CW), which is a joint venture between Shell and Eneco. The BLPH facility consists of a purified water electrolyser, hydrogen storage, fuel cell and a short duration lithium-ion Battery Energy Storage System (BESS). The BLPH platform has been initially developed for offshore to be connected as close as possible to the electrical network at the offshore wind turbine park Hollandse Kust Noord (HKN). However, the location of the BLPH facility has been altered to onshore in the Eemshaven, in the north of Dutch province Groningen. The change of location also involves a change in operation philosophy, meaning the Normally Unmanned Installation (NUI) classification no longer applies.

The scope of this workshop included the reassessment of LOPA scenarios based on the changed location. Hence, credit for control of personnel are not taken, as a conservative approach. In addition A SIL Verification/ Calculation report has been produced by Elogen, with the SIL of SIFs assessed in previous sessions of LOPA workshops have been verified. As a result, the actual PFD of verified SIFs were updated in the LOPA calculation, in order to obtain a more accurate LOPA assessment.

The scope of LOPA has been completed by defining and assessing a total of 19 scenarios for the Electrolyser and Fuel Cell packages. Of the 19 scenarios, 14 scenarios were put through the LOPA process to assess the tolerability of the LOPA scenario, and 5 scenarios which were previously put through LOPA have been taken off from LOPA. This is because they are no longer required to be put through LOPA as per LOPA DEP [1].

All but 4 LOPA scenarios were assessed to be tolerable (2 for the electrolyser package and 2 for the fuel cell package). The 2 intolerable scenarios of electrolyser package are related to the SIF of PDSHH-002 and PDSLL-002, with both scenarios having RRF of 4 respectively. Recommendation no 2 was raised to address this gap, and upon closeout of this recommendation, the PHA Team considers this scenario to be ALARP. The 2 intolerable scenarios of fuel cell package are related to the firewire linear heat detector around the Fuel Cell Modules shutdown via fire safety system. For closing this scenario, information regarding this trip is requested from Ballard (HOLD1)

The 5 scenarios which were taken off of LOPA are related to the design of the nitrogen utility lineup which is ALARP by HSSE Standards and Practices based on DEP 31.38.01.25 or internal explosion scenario which is no longer credible based on calculations from Elogen. One of the scenario is related to the failure of membrane in stack which is caused by degradation of membrane, where the initiating event frequency (IEF) data for this scenario is widely unavailable. Barriers in place to mitigate the effects of this scenario were identified, hence the PHA team considered this scenario to be tolerable if ALARP.

A total of three (3) recommendations were raised in this session of LOPA workshop. A complete list of LOPA recommendations raised are listed in Appendix C.

The LOPA worksheets produced as part of the workshop are attached in Appendix B, and the PHAPro files are attached in Appendix D.

TABLE OF CONTENTS

ISSUE RECORD 1
DISTRIBUTION 1
EXECUTIVE SUMMARY 2
TABLE OF CONTENTS 3
TABLE OF TABLES 4
TABLE OF FIGURES 4
ABBREVIATIONS 5
1 INTRODUCTION 6
1.1 Project Background 6
1.2 Scope 6
1.3 Objectives 6
2 WORKSHOP METHODOLOGY 7
2.1 LOPA Process 7
2.2 Ground Rules and Assumptions 7
2.2.1 Safeguards/barriers 7
2.2.2 SIFs 8
2.2.3 Relief valves 8
2.2.4 Overpressure consequences 8
2.2.5 Locked manual valves 10
2.2.6 Workshop Specific Rule 10
2.3 Tolerability Criteria 10
2.4 Recommendations 11
3 LOPA WORKSHOP 12
3.1 Time and Location 12
3.2 Team composition 12
3.3 Recording 12
3.4 Workshop References 12
4 LOPA RESULTS 14
4.1 Recommendations 14
4.2 Assessed SIFs 14
4.3 Recommendation Follow Up 16
REFERENCES 17
APPENDIX A ATTENDANCE LIST A.1
Appendix A.1 Workshop Attendance List A.1
Appendix A.2 Workshop Attendance Sheet A.2
APPENDIX B LOPA WORKSHEETS B.1
Appendix B.1 Electrolyser Package LOPA B.1
Appendix B.2 Fuel Cell LOPA B.13

APPENDIX C LOPA RECOMMENDATIONS C.1
APPENDIX D PHAPRO FILE D.1

TABLE OF TABLES

Table 2-1: Rupture probability 9
Table 2-2: Flange hole size 9
Table 2-3: Risk Tolerability Criteria 11
Table 3-1: LOPA Workshop Team Composition Overview 12
Table 4-1: SIFs Assessed 14
Table 4-2: Non-LOPA Scenario 15

TABLE OF FIGURES

Figure 1-1. Location for the BLPH facility in the Eemshaven [1]. Yellow dashed line indicates the BLPH facility location, red dashed line – location of the closest wind turbine. 6

ABBREVIATIONS

Acronym	Definition
ALARP	As Low as Reasonably Practicable
ASME	American Society of Mechanical Engineers
BESS	Battery Energy Storage System
BLPH	Base Load Power Hub
BPCS	Basic Process Control System
CM	Conditional Modifier
CW	CrossWind
DCS	Distributed Control System
DEP	Design and Engineering Practice
DSM	Downstream Manufacturing
EF	Enabling Factor
FC	Fail-close
FO	Fail-open
HAZOP	Hazard and Operability
HEP	Human Error Probability
HIOD	Hydrogen in Oxygen Detection
HKN	Hollandse Kust Noord
HPP	Hydrogen Purification Package
HSSE	Health, Safety, Security and Environment
IEC	International Electrotechnical Commission
IEF	Initiating Event Frequency
IPF	Instrumented Protective Function
IPL	Independent Protection Layer
LEL	Lower Explosive Limit
LFL	Lower Flammable Limit
LOPA	Layers Of Protection Analysis
LOPC	Loss of Primary Containment
MEF	Mitigated Event Frequency
NUI	Normally Unmanned Installation
PEM	Proton Exchange Membrane
PFD	Probability of Failure on Demand
PHA	Process Hazard Analysis
RAM	Risk Assessment Matrix
RRF	Risk Reduction Factor
SCE	Safety Critical Element
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TA	Technical Authority

1 INTRODUCTION

1.1 Project Background

The Base Load Power Hub (BLPH) is an innovative project of Crosswind (CW), which is a joint venture between Shell and Eneco. The BLPH facility consists of a purified water electrolyser, hydrogen storage, fuel cell and a short duration lithium-ion Battery Energy Storage System (BESS). The BLPH platform has been initially developed for offshore to be connected as close as possible to the electrical network at the offshore wind turbine park Hollandse Kust Noord (HKN). The platform provides the capacity to transform renewable electricity, intermittent in nature, into a constant power supply.

The location of the BLPH facility has been altered to onshore in the Eemshaven, in the north of Dutch province Groningen. The change of location also involves a change in operation philosophy, meaning the Normally Unmanned Installation (NUI) classification no longer applies. Operations may occur during business hours, and a control room will be installed nearby the BLPH facility for monitoring and control. It is the intention that the facility will still be operated with the same philosophy as offshore operations. However, a detailed manning, access and operating philosophy is yet to be developed for the new operating situation. Figure 1-1 shows the intended location and placement of the BLPH facility.

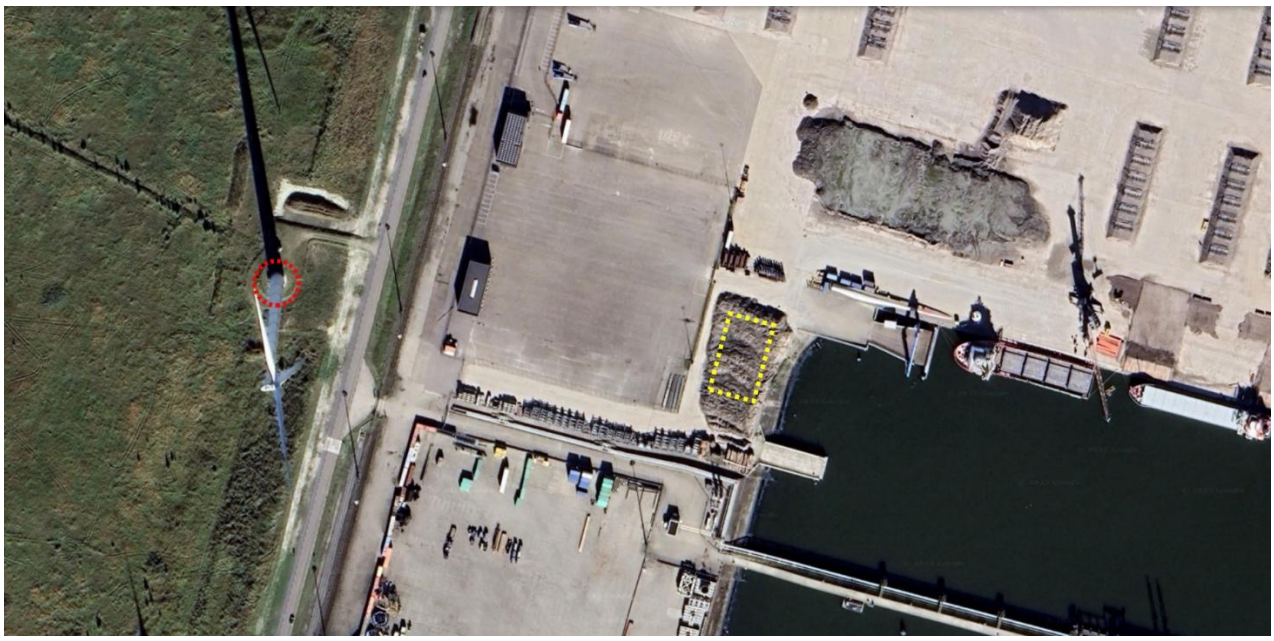


Figure 1-1. Location for the BLPH facility in the Eemshaven [2]. Yellow dashed line indicates the BLPH facility location.

1.2 Scope

During the design of the BLPH, a LOPA has been conducted for the different project parts:

1. Integration package system (H2 Storage) [3]
2. Electrolyser system [4]
3. Fuel cell system [5]

The scope of this workshop included the reassessment of LOPA scenarios based on the changed location.

1.3 Objectives

Objectives of the LOPA Workshop is to review LOPA scenarios previously assessed for the offshore location to ensure scenarios are managed to ALARP for the relocation to onshore.

2 WORKSHOP METHODOLOGY

2.1 LOPA Process

The LOPA was carried out in full accordance with the Shell LOPA DEP [1].

LOPA was applied to risk assessment scenarios for the following situations:

a) To establish the Probability of Failure on Demand (PFD) target for each SIF listed as a barrier, when it has not been specified elsewhere (e.g., a DSM model bowtie or specified in a DEP);

   Note that the SIF must have the design intent to protect against the consequence being considered to trigger a LOPA for this consequence.

   An example of a DEP specified PFD is the requirement for a SIL 2 rated backflow protection in case backflow can lead to overpressure.

b) When a HAZOP or other risk assessment team considers that there might not be sufficient barriers;

c) If required per local regulatory or by the business to support ALARP demonstration.

If the risks are well understood, if there is a standard and good practice (industry standards, DEPs) to follow, (e.g. simple relief valve without a SIF), and if the scenario is not covered by the situations mentioned above, then the following apply:

a) LOPA should not be done;

b) If LOPA is performed, then any additional SIF shall be subject to approval by the TA1 in Technical Safety of the Principal or the Business.

There is no requirement to do LOPA if there is no SIF as safeguard, risk is well understood and safeguarded as per DEP/ industrial standards/ good practices (e.g. what is indicated in the process guide, what is commonly applied in similar units). An example of this approach is an overpressure scenario safeguarded with a valid barrier and an adequately sized relief valve).

- All scenarios are to be safeguarded as per Shell /industry standards and good practices to demonstrate ALARP. Please note, DEP may cover part of the safeguarding, additional safeguards may be addressed in another DEP. A good example is double seals requirement for a pump in hazardous service. As double seals can fail, additional safeguards such as fire detection by polyflow activating the sprinkler may be needed, which is addressed in another DEP.
- ALARP demonstration text is always required in HAZOP/LOPA worksheets for yellow and red risks.
- When LOPA is done, perform ALARP assessment after achieving tolerable risk in LOPA worksheet and write down ALARP considerations (or alternatively specify actions for tolerable / ALARP).
- When LOPA is not done, write in ALARP column in HAZOP worksheet how ALARP was demonstrated (incl. reference to Shell/industry standard claimed) and (if applicable) which actions are required to meet ALARP.

2.2 Ground Rules and Assumptions

2.2.1 *Safeguards/barriers*

The following definitions was applied when identifying barriers in the HAZOP:

- Barriers are engineered systems or administrative controls designed to prevent the causes or mitigate the consequences of deviations (e.g., process alarms, process controls, interlocks, SIFs); and

- Barriers were only taken into account if they are part of the design (e.g., already part of the design hardware, documentation or operating procedures).

The barriers identified satisfied the following criteria to be considered valid:

- Effective;
- Independent;
- Auditable; and.
- Dependable (applicable for Safety Instrumented Functions (SIFs) only - being designed, implemented, maintained, inspected and tested in accordance with IEC 61511 .

In the HAZOP all safeguards (barriers) were listed, both valid and non-valid. Barrier validity was recorded in the HAZOP for yellow and red risks. Where a safeguard was identified as non-valid then the reason why was recorded. When the barrier was identified as valid, the checks made to ascertain validity were recorded, e.g., nature of operator response (e.g. tag of the valve that the operator will close), which operator (field or control room) will act (when the initiating event is a human error), sufficient time for operator response, direction of failure of the valve for a control loop barrier, sensors and final elements for SIFs, clean service, etc.

Control actions for BPCS loops (in or outside the unit being considered) that detect the deviation caused by the initiating event and react to it to restore normal conditions/resolve the upset were recorded as barriers in the HAZOP. Example: a level control loop in a vessel of which the inlet control valve fails open. Barrier validity must be assessed.

Control actions for those BPCS loops (in or outside the unit being considered) that do not detect the deviation caused by the initiating event and (therefore) do not react to it to restore normal conditions/resolve the upset are considered independent from the initiating event (of course only if they also have independent sensors and final elements). Example: a steam system pressure control loop is independent from the reflux control loop in the column the steam is used as reboiler medium.

The challenge of whether the BPCS can be claimed as an Independent Protection Layer (IPL), in accordance with the Shell LOPA DEP was carried out in the HAZOP.

The challenge of whether the alarm can be claimed as an IPL, in accordance with the Shell LOPA DEP, was carried out in the HAZOP.

2.2.2 *SIFs*

Only the final elements for each respective SIF which prevent the consequence were recorded, i.e. if the C&Es identifies several executive actions, only the primary actions which prevent the consequence were recorded against the SIF.

If a SIF is considered for a particular consequence (e.g. overpressure) but the SIF design intent does not include the consequence being discussed (e.g. prevent sending liquid to furnace), the SIF may be recorded in the HAZOP but the threat to consequence line will not take part in the LOPA to determine the SIL of the SIF. The SIF design intent should be recorded. If the final element that would be effective for the consequence being considered (e.g. valve in inlet) is not a primary final element (in SIFPro), the SIF was be considered valid for this particular consequence.

2.2.3 *Relief valves*

The following information were recorded for relief valves:

- Set points; and
- Correctly sized for the over-pressure event, with documentary evidence.

Passing relief valves were taken as a “cause” unless the relief valve discharges to atmosphere.

2.2.4 *Overpressure consequences*

In accordance with the Shell LOPA DEP, the LOPA Team records over-pressure consequences as follows:

1. Consequence of rupture – this will have the highest severity
2. Consequence of flange leak – possibly a lower severity

Recording the consequences this way will allow the probability of rupture to be identified in the LOPA in accordance with the data in Table 2-1 and the leak hole size in accordance with the data in Table 2-2. Only the determining case for the LOPA is required to be recorded in the worksheets.

The consequence were written to clearly indicate the design pressure and the maximum pressure generated from the upset case so that over-pressure ratio can be clearly seen.

A suitably sized relief valve is the default minimum safeguarding solution for overpressure cases. Only if implementing an adequate relief system is not practicable, an alternative design approach may have been adopted. See Shell Overpressure DEP Section 2.10.3 [6] for definition of what is not practicable and for an alternative safeguarding approach. It is not the purpose of a HAZOP or LOPA to design safeguarding systems. However, if the team identifies an overpressure case without suitable relief system and no documented justification of the non-practicability of the relief system, a recommendation to review the design and comply with DEP requirements were raised in the HAZOP.

Table 2-1: Rupture probability

Vessel Design Code	**Safety Factor**	**Probability of equipment rupture (Note 1)**		
		Prob = 0.01	**Prob = 0.1**	**Prob = 1.0**
ASME Section VIII Pre-2000	4:1	2.8≤PR<3.2	3.2≤PR<3.6	3.6≤PR
ASME Section VIII 2000 and newer	3.5:1	2.5≤PR<2.8	2.8≤PR<3.2	3.2≤PR
ASME Section VIII Div 2, Stoomwezen, or CODAP	3:1	2.2≤PR<2.4	2.4≤PR<2.7	2.7≤PR
EN-13445	2.4:1	1.8≤PR<2.0	2.0≤PR<2.2	2.2≤PR
AS-1210 or PD5500	2.35:1	1.8≤PR<2.0	2.0≤PR<2.2	2.2≤PR
NOTES: 1. PR = Pressure ratio, this being the ratio of [vessel over-pressure] to [MAWP or design pressure] 2. The probability of equipment rupture for PR below those given in this table are so small that the equipment rupture case can be omitted.				

Table 2-2: Flange hole size

Vessel Design Code	**Safety Factor**	**Pressure/MAWP ratio or design pressure (PR) that results in hole of given diameter (probability = 1)** (Note 1)		
		7 mm (0.28 in) (Note 2)	**25mm (1 in.)**	**100mm (4 in.)** (Note 3)
ASME Section VIII Pre-2000	4:1	cHTP≤PR<1.9	1.9≤PR<3	3≤PR<3.6
ASME Section VIII 2000 and newer	3.5:1	cHTP ≤PR<1.9	1.9≤PR<2.7	2.7≤PR<3.2
ASME Section VIII Div 2, Stoomwezen, or CODAP	3:1	cHTP ≤PR<1.9	1.9≤PR<2.5	2.5≤PR<2.7
EN-13445	2.4:1	cHTP ≤PR<1.9	1.9≤PR<2.1	2.1≤PR<2.2
AS-1210 or PD5500	2.35:1	cHTP ≤PR<1.9	1.9 ≤PR<2.1	2.1 ≤PR<2.2
NOTES: 1. PR = Pressure ratio, this being the ratio of [vessel over-pressure] to [MAWP or design pressure]. 2. cHTP = corrected Hydrotest Pressure= actual hydrotest pressure corrected for relief scenario or design temperature. 3. beyond the value of PR given in the 100mm (4 in) diameter hole size column, there is no need to assess a leak case as the probability for equipment rupture is considered to be 1 (i.e., leak case will not be determining).				

2.2.5 *Locked manual valves*

If inadvertent closure of a Locked Open (LO) valve causes "immediate" overpressure, compliance with ASME VIII Appendix M (North America) or corresponding (outside North America) Shell interpretation was verified (single valve with or without lock is normally not accepted as an open system if closure of that valve can create an immediate overpressure case greater than 110% of the design pressure) [6].

For locked valves, 2 human errors could occur:

1. The operator has intentionally operated the locked valve (e.g. for shutdown/start-up) and forgot to re-instate it in its normal, locked position. In this case, the lock is not a barrier since the valve was intentionally operated. Operating a locked valve should follow a procedure and therefore initiating event frequencies can be calculated based on LOPA DEP Table 5 and the expected frequency of operation of the locked valve. For this, it is important to understand why the valve was implemented and why it needs to be operated. It is quite different to have a valve that was put for construction purposes only and will never be operated versus a valve that will be used for some special modes of operation.
2. Inadvertent operation of the wrong valve. Operator should close valve B but closes valve A instead. In this case, the lock is a barrier with PFD=0.1 as per LOPA DEP Table 2 Row 25 (Keyed Bypass /Interlock). In this case, the frequency of operation of the "other/right" valve (in this example valve B) should be considered. This could be a valve physically nearby or a valve on a parallel string/train.

In cases where the human error related to the locked valve is another reason for e.g. a path to be closed, it may not be significant mathematically (in a LOPA/SIF classification). However, it may be quite important to look at if the locked valve is not the only cause for the scenario to develop.

2.2.6 *Workshop Specific Rules*

Credit for Control of Personnel (CoP)

Since the scope of the LOPA assessment conducted was specifically to review the existing LOPA with the relocation of the facility to onshore, credit for Control of Personnel across various LOPA scenarios is no longer valid. The philosophy for onshore operations is still anticipated to be similar to that offshore. However, due to the onshore location, it is anticipated for there to be personnel visits. For the purpose of conservatism, credit for control of personnel is hence not taken.

Actual PFD for Valid SIFs

A SIL Verification/ Calculation report has been produced by Elogen, with the SIL of SIFs assessed in previous sessions of LOPA workshops having been verified. As a result, the actual PFD of verified SIFs were updated in the LOPA calculation.

2.3 Tolerability Criteria

The tolerability criteria for residual risk, are as stated below:

- The tolerability criteria (i.e., occurrences per year) shall be equal to the values shown in Table 2-3 below.
- For events with a People consequence severity 3, the tolerability criteria shall be 1E-3 per year.
- For events with "asset" consequence severity RAM 4 or RAM 5, a tolerability criteria of 1E-3 per year may be applied.
- "Asset" consequence includes only direct damage to assets, and does not include consequential business loss (e.g., lost production, quality costs, clean-up costs).
- For events with "community" or "environment" consequence severity RAM 3, a tolerability criteria of 1E-2 per year may be applied.

Table 2-3: Risk Tolerability Criteria

Consequence Severity	People	Community	Environment	Tolerability Criteria (Occurrences per year)
RAM 5	**10 or more fatalities.**[2]			1E-05
	>Than 3 fatalities <10 Fatalities Multiple illnesses with irreversible health effects.	**Massive Effect:** • Persistent, severe impact on livelihood, social and cultural assets, community security, health, vulnerable or Indigenous Peoples and/or human rights infringements. • International public concern.	**Massive Effect** Persistent severe environmental damage that will lead to loss of natural resources over a wide area.	1E-04
RAM 4	**Permanent total disability or up to 3 Fatalities.** Illnesses with irreversible health			1E-04
		Major Effect: • Persistent effects on livelihood and/or social and cultural assets, community health. • National public concern. • National government and/or NGO involvement	**Major Effect** Severe environmental damage that will require extensive measures to restore beneficial uses of the environment.	1E-03

2.4 Recommendations

Recommendations raised will be collected with the close-out and tracked into a HSSE Action Tracking Register by DOT. Each action-sheet will indicate the recommendation, with the responsible of closing the action, the answer showing how the recommendation is properly closed.

3 LOPA WORKSHOP

3.1 Time and Location

The LOPA workshop was conducted for 1 day, on the 13th August 2025, in person at the TCI Office in Delft.

3.2 Team composition

The LOPA team composition is presented in Table 3-1, and a detailed attendance list is presented in **Error! Reference source not found.**.

Table 3-1: LOPA Workshop Team Composition Overview

Name	Company	Function
Jordi Alkemade	TCI	Facilitator
Farrah Adzhar	TCI	Scribe
Jonquelle Low	DOT	Project Manager
Frans Quispel	DOT	Engineer
Casper Aarnts	DOT	Engineer
Paul van Rossum	Crosswind	Technical Safety Engineer
Omkar Sane	Crosswind	Electrical and Integration Lead
Thijs Philippo	Crosswind	Process/Project Engineer
Stephen Bremner	Crosswind	Package Lead
Leila Shamekhi	Fores/ Crosswind	Project Manager Coordinator

3.3 Recording

The discussion and actions raised during the workshop were recorded by the scribe on worksheets using PHApro Software (Version 8).

The findings of the LOPA session were recorded into the original PHApro files (see Appendix D). The Facilitator was responsible for leading and directing discussions to ensure that all aspects of LOPA for each section were adequately considered.

3.4 Workshop References

For the documents used for the LOPA workshop, refer to the previous HAZOP-LOPA reports:

1. Integration package system (H2 Storage) [3]
2. Electrolyser system [4]
3. Fuel cell system [5]

Table 3-2 shows the additional documentation used during the workshop.

Table 3-2: Additional documentation

Doc nr	Description	Revision
C63-PWI-002	Electrolyzer Cause and Effect Matrix	06
C63-PWI-001	Electrolyzer P&IDs	10
C63-PUY-002	Electrolyzer Safety Loop Calculations	05

Doc nr	Description	Revision
K559-2254-CWIWP4202202-C03-001	Fuel Cell P&IDs	06
123A90-DDL-PR-PID-80011	ELECTROLYSER PACKAGE	05
123A90-DDL-PR-PID-80012	FUEL CELL PACKAGE	04
123A90-DDL-PR-PID-80013	HYDROGEN STORAGE VESSELS HEADER (INLET)	02
123A90-DDL-PR-PID-80014	HYDROGEN STORAGE VESSELS HEADER (OUTLET)	03
123A90-DDL-PR-PID-80015	HYDROGEN STORAGE VESSEL A	03
123A90-DDL-PR-PID-80016	HYDROGEN STORAGE VESSEL B	03
123A90-DDL-PR-PID-80017	HYDROGEN STORAGE VESSEL C	03
123A90-DDL-PR-PID-80018	HYDROGEN STORAGE VESSEL D	03
123A90-DDL-PR-PID-80019	HYDROGEN STORAGE VESSEL E	03
123A90-DDL-PR-PID-80020	HYDROGEN STORAGE VESSEL F	03
123A90-DDL-PR-PID-80027	INSTRUMENT AIR PACKAGE	03
123A90-DDL-PR-PID-80028	HYDROGEN VENT HEADER	03
123A90-DDL-PR-PID-80029	HYDROGEN VENT DRUM	04

4 LOPA RESULTS

The scope of LOPA has been completed by defining and assessing a total of 19 scenarios for the Electrolyser and Fuel Cell packages. Of the 19 scenarios, 14 scenarios were put through the LOPA process to assess the tolerability of the LOPA scenario, and 5 scenarios which were previously put through LOPA have been taken out of LOPA. This is because they are no longer required to be put through LOPA as per LOPA DEP [1].

All but 4 (2 for the electrolyser package and 2 for the fuel cell package) LOPA scenarios were assessed to be tolerable. The 2 intolerable scenarios of the electrolyser package are related to the SIF of PDSHH-002 and PDSLL-002, with both scenarios having RRF of 4 respectively. Recommendation no 2 was raised to address this gap, and upon closeout of this recommendation, the PHA Team considers this scenario to be ALARP. The 2 intolerable scenarios of the fuel cell package are related to the firewire linear heat detector around the Fuel Cell Modules shutdown via fire safety system. For closing this scenario, information regarding this trip is requested from Ballard (HOLD1).

The 5 scenarios which were taken off of LOPA are related to the design of the nitrogen utility lineup which is ALARP by HSSE Standards and Practices based on DEP 31.38.01.25, or internal explosion scenario which is no longer credible based on calculations from Elogen. One of the scenario is related to the failure of the membrane in stack which is caused by degradation of the membrane, where the initiating event frequency (IEF) data for this scenario is widely unavailable. Barriers in place to mitigate the effects of this scenario were identified, hence the PHA team considered this scenario to be tolerable if ALARP.

4.1 Recommendations

A total of three (3) recommendations were raised in this session of LOPA workshop. A complete list of LOPA recommendations raised are listed in Appendix C.

4.2 Assessed SIFs

The following SIFs assessed and the associated recommendations and/or ALARP statements are specified in Table 4-1. For SIFs which are part of a SIF Summation, all associated scenarios to the SIF summation are identified in the table.

Table 4-2 lists the scenarios which were taken off from LOPA, and the associated justification or ALARP statements.

Table 4-1: SIFs Assessed

SIF	SIF Description	Places Used	Status	ALARP Statement	LOPA Rec No.
Electrolyser Package					
FAHH-640	FAHH-640 High Flow Trip will trigger IS-3 will close PV-641 and Safety Stop	4.2.5.1	Tolerable	PHA Team considers this scenario, after implementation of recommendations, to be ALARP and that adding additional barriers would be grossly disproportionate to the risk reduction achieved. Adding a lock on the valve, in addition to the trip is considered ALARP.	1
FALL-600	FT-600 Low Low Flow Trip will trigger IS 1. IS 1 will de-energise the stacks(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	1.1.9.4. 2.1.2.1. 2.1.7.2. 4.1.8.3. 4.1.10.2.	Tolerable	PHA Team considers this scenario to be ALARP and that adding additional barriers would be grossly disproportionate to the risk reduction achieved. There are additional non valid barriers e.g. alarm, BPCS switches and a non-rated SIL which have not been claimed in the LOPA.	-

SIF	SIF Description	Places Used	Status	ALARP Statement	LOPA Rec No.
				Considering these additional barriers, the scenario is considered ALARP.	
LASLL-641	LSL-641 Low Low Level trip will trigger IS 3. IS 3 will close PV-641 (Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	4.2.2.1. 4.2.7.1.	Tolerable	PHA Team considers this scenario, after implementation of recommendations, to be ALARP and that adding additional barriers would be grossly disproportionate to the risk reduction achieved.	3 -
PAHH-631	PT-631 High High Pressure will trigger IS 1. IS 1 will de-energise the stacks(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	5.1.11.1. 5.1.13.2.	Tolerable	ALARP by HSSE Standards and Practices. Assessment based on: Overpressure DEP 80.45.10.11 (2021)	-
PDAHH-002	PT-611 and PT-631 High Differential Pressure trips of IS 1 (Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	3.2.5.1.	RRF = 4	PHA Team considers this scenario, after implementation of recommendations, to be ALARP and that adding additional barriers would be grossly disproportionate to the risk reduction achieved. Additional barriers considered: Installing additional trips.	2
PDSLL-002	PT-631 and PT-611 Low Low Pressure Differential between 02 and H2 loop with a set point of -0.5 bar. It will trigger IS 1, IS 1 is a safety fault leading to a hard shutdown, depressurization of unit.	6.2.2.1.	RRF = 4	PHA Team considers this scenario, after implementation of recommendations, to be ALARP and that adding additional barriers would be grossly disproportionate to the risk reduction achieved. Additional barriers considered: Installing additional trips.	2
Fuel Cell Package					
N/A	Firewire Linear Heat Detector shutting down Fuel Cell Module	4.9.1.1 4.9.2.1	RRF=3		HOLD1 HOLD1

Table 4-2: Non-LOPA Scenario

Scenario No.	Scenario Description	Justification / ALARP Statement	LOPA Rec No.
2.3.2.1.	Failure of membrane in Stack gradual degradation. Potential to create flammable atmosphere within ST-600, fire and explosion within ST-600.	The design life of the stacks is 10 years assuming continuous stable load, and degradation of the stacks overtime is anticipated. As current safeguard, there is H2 in 02 detection (HIOD) with an alarm (Valid), which will give sufficient time for operations to shut down the system. In addition, there is 2oo3 SIL2 SIF which shutsdown the electrolyser at 50%LEL. There is also continuous monitoring of stack voltage which might indicate degradation, however it is not considered valid. With all of the barriers considered, therefore this scenario is considered tolerable if ALARP.	-
2.2.4.2.	LIC640/FX-642/FIC642 control loop failure closing PV642. Gradual build up of H2 gas in DG-640 resulting in release of gas contents of DG-	Based on calculations from Elogen, the amount of H2 that is flashed in DG-640 is insufficient to result in a flammable mixture in	-

Scenario No.	Scenario Description	Justification / ALARP Statement	LOPA Rec No.
	640 into ST-600, explosive mixture with potential for ignition and explosion.	ST-600. H2 in O2 content will not exceed 50%LFL. Internal explosion is no longer considered credible.	
3.2.1.1.	PV-900 Driven open by PI-610. Operating pressure of ST-600 is greater than N2 supply pressure potential back flow of O2 into N2 system. Potential for flammable atmosphere to be formed within ST-620 or DG-640 or H2 panel. Potential for explosion within unit when purging.	ALARP by HSSE Standards and Practices. Assessment based on DEP 31.38.01.25 for the N2 utility lineup	-
5.1.9.1.	MV-642 set incorrectly at commissioning. Shorter residence time of Hydrogenated water in DG-640 leading to higher H2 concentration in ST-600 resulting in a flammable atmosphere of H2 and O2 in ST-600 potential for ignition and an explosion.	Based on calculations from Elogen, the amount of H2 that is flashed in DG-640 is insufficient to result in a flammable mixture in ST-600. H2 in O2 content will not exceed 50%LFL. Internal explosion is no longer considered credible.	1
5.2.1.1.	PV-920 Driven open. Operating pressure of ST-620 is greater than N2 supply pressure potential back flow of H2 into N2 system. Potential for flammable atmosphere to be formed within ST-600. Potential for explosion within unit when purging.	ALARP by HSSE Standards and Practices. Assessment based on DEP 31.38.01.25 for the N2 utility lineup	-

4.3 Recommendation Follow Up

Each recommendation shall have a unique number and be closed-out in an auditable manner. The person/department/company identified in the “Responsibility” column of the worksheet is responsible for timely resolution of the recommendation .

All response documentation shall have a full auditable trail on how each LOPA recommendation has been addressed.

All process documents shall be updated to reflect the resolution of the LOPA recommendations. Recommendations closeout is managed by DOT.

REFERENCES

[1] Shell, “LAYERS OF PROTECTION ANALYSIS (LOPA), DEP 01.00.02.13-Gen.,” 2021.

[2] *Platform Orientation Preference,* 2025.

[3] Rosetti Marino, “LOPA Allocation Report rev01,” 2024.

[4] Risktec Solutions, “Elogen Electrolyser Package HAZOP/LOPA rev 2.0,” 2023.

[5] Risktec Solutions, “BLPH Project Fuel Cell HAZOP/LOPA rev 4.0,” 2023.

[6] Shell, “OVERPRESSURE AND UNDERPRESSURE – PREVENTION, DEP 80.45.10.11-Gen.,” 2021.

APPENDIX A ATTENDANCE LIST

Appendix A.1 Workshop Attendance List

Name	Company	Position	Presence (13th August 2-25)
Jordi Alkemade	TCI	Facilitator	✓
Farrah Adzhar	TCI	Scribe	✓
Jonquelle Low	DOT	Project Manager	✓
Frans Quispel	DOT	Engineer	✓
Casper Aarnts	DOT	Engineer	✓
Paul van Rossum	Crosswind	Technical Safety Engineer	✓
Omkar Sane	Crosswind	Electrical and Integration Lead	✓ (Online)
Thijs Philippo	Crosswind	Process/Project Engineer	✓
Stephen Bremmer	Crosswind	Package Lead	✓ (Online)
Leila Shamekhi	Fores/ Crosswind	Project Manager Coordinator	✓ (Online)

Appendix A.2 Workshop Attendance Sheet

Attendance Sheet:
Project: BLPH
Date: 13/08/2025
Location: TCI Office, Delft

TCI RISK MANAGEMENT

Name	Position	Company	Attendance morning	Attendance afternoon	Signature	E-mail (optional)
FARRAH AZHAR	SCRIBE	TCI	✓	✓		
JORDI ALKEMADE	FACILITATOR	TCI	✓	✓		
Casper Aarnts	Engineer	DOT	✓	✓		
Thijs Philippo	Consult	CW/Shell	x	x		
Jonquelle Law	PM	DOT	x	x		
Pau[illegible]	TSE	CW	✓	✓		
Frans [illegible]	Engineer	DOT	✓	✓		

APPENDIX B LOPA WORKSHEETS

Appendix B.1 Electrolyser Package LOPA

Node: 1. Purified Water - 300

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers							SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations							Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y/N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
1.1. Flow No/Less	1.1.9. PV-300 closed by signal failure or driven closed by LI-600 Consequence: 1.18.1.1	1.1.9.4. Downstream: No make-up water to the O2 Loop leading to low level in ST-600 resulting in CP-600A/B running dry causing pump damage. Results in no flow of make-up water to Electrolyser leading to stacks overheating, ultimately resulting in LOPC of stacks creating an explosive mixture with potential for ignition and explosion.	Hydrogen	P	5	A	5A	Y	PAH-300		PAH-300 High pressure alarm. Not valid as 3rd BPCS and no operator action.	NV				FALL-600	Control Loop (Electronic): Fails to danger	1.0E-01	N/A	1.0E+00	1.0E-01	4.0E-04	4.0E-05	Control of Ignition not claimed	1.E+00	1.0E+00	4.0E-05	9.8E-05	1.0E-04	Y									9.8E-05	PHA Team considers this scenario to be ALARP and that adding additional barriers would be grossly disproportionate to the risk reduction achieved. There are additional non valid barriers e.g. alarm, BPCS switches and a non-rated SIL which have not been claimed in the LOPA. Considering these additional barriers, the scenario is considered ALARP.
				A	4	B	4B		FSL-300A/B		FSL-300A/B Low Flow Switch will trip LP-300A/B.	NV																	1.0E-03	Y											
				C	4	B	4B		LAL-600		LT-600 Low Level Alarm with operator action to perform a soft shutdown. Not valid as same sensor as IE.	NV																	1.0E-03	Y											
				E	3	B	3B		LALL-600		LT-600 Low Low Level Controlled Shutdown will trigger a major fault leading to a soft shutdown, depressurization of unit. Not valid as same sensor as IE.	NV																	1.0E-02	Y											
									LASLL-600		LSL-600 Low Low Level Switch will trigger a safety fault leading to a hard shutdown, depressurization of unit. IS 6	V		SIL0 - Non SIL rated IPF	1.0E+00																										
									FALL-600		FT-600 Low Low Flow Trip will trigger IS 1. IS 1 will de-energise the stacks(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	4.0E-03																									
									TAH-601/2/3/4/5/6/7/8		TT-601/2/3/4/5/6/7/8 High Temperature Alarm with insufficient time for operator action. Temperature rises rapidly.	NV																												
									TAHH-601/2/3/4/5/6/7/8		TT-601/2/3/4/5/6/7/8 High High Temperature Trip will trigger a major fault leading to a soft shutdown, depressurization of unit. BPCS.	V		Operational interlock loop, electronic DCS or single loop, automatic action (includes sensing, logic and Control valve)	1.0E-01																									

Node: 2. O2 Water Loop -600

Deviation	Cause	Consequence	Hazard Register	RAM Score				SIF	Barriers						SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations								Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y/N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
2.1. Flow No/Less	2.1.2. CP-600A/B stopped Consequence: 2.18.2.2	2.1.2.1. No flow through the stacks leading damage to the membrane due to stacks overheating, ultimately resulting in LOPC of stacks creating an explosive mixture with potential for ignition and explosion.	Hydrogen	P	5	A	5A	Y	PAL-600		PT-600 Low Pressure Alarm auto start-up of other pump. Only valid if pump failure is cause.	V		Pump - Backup (spare); non-positive displacement	1.0E-01	FALL-600	Pump, General: Stops Running	2.0E-01	N/A	1.0E+00	2.0E-01	4.0E-05	8.0E-06	Control of Ignition not claimed	1.E+00	1.0E+00	8.0E-06	9.8E-05	1.0E-04	Y										9.8E-05	PHA Team considers this scenario to be ALARP and that adding additional barriers would be grossly disproportionate to the risk reduction achieved. There are additional non valid barriers e.g. alarm, BPCS switches and a non-rated SIL which have not been claimed in the LOPA. Considering these additional barriers, the scenario is considered ALARP.
				A	4	B	4B		FALL-600		FT-600 Low Low Flow Trip will trigger IS 1. IS 1 will de-energise the stacks(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	4.0E-03														1.0E-03	Y											
				C	4	B	4B		TAH-601/2/3/4/5/6/7/8		TT-601/2/3/4/5/6/7/8 High Temperature Alarm with insufficient time for operator action. Temperature rises rapidly.	NV																1.0E-03	Y											
				E	3	B	3B		TAHH-601/2/3/4/5/6/7/8		TT-601/2/3/4/5/6/7/8 High High Temperature Trip will trigger a major fault leading to a soft shutdown, depressurization of unit. BPCS	V		Operational interlock loop, electronic DCS or single loop, automatic action (includes sensing, logic and Control valve)	1.0E-01													1.0E-02	Y											
									CAH-610		HIOD-610A/B/C 2oo3 High Hydrogen in Oxygen stream above ST-600. Not considered valid for this scenario as likely to develop before Alarm activated.	NV																													
									CAHH-610		HIOD-610A/B/C 2oo3 High High Hydrogen in Oxygen stream above ST-600. Trips of IS 1(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)). Not considered valid for this scenario as likely to develop before Alarm activated.	NV																													
		2.1.7.2. Downstream: No make-up water from DG-640 to the O2 Loop leading to low level in ST-600 resulting in	Hydrogen	P	5	A	5A	Y	LAL-600		LT-600 Low Level Alarm with operator action to perform a soft shutdown. Not	NV				FALL-600	Control Loop (Electronic	1.0E-01	N/A	1.0E+00	1.0E-01	4.0E-04	4.0E-05		1.E+00	1.0E+00	4.0E-05	9.8E-05	1.0E-04	Y										9.8E-05	PHA Team considers this scenario to be ALARP and that adding additional barriers would be grossly

Node: 2. O2 Water Loop -600

Deviation	Cause	Consequence	Hazard Register	RAM Score				LOPA	Barriers						SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations							Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y/N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
	2.1.7. FIC-640 control loop failure closing PV-640 Consequence: 2.10.1.1 Consequence: 2.18.2.1	CP-600A/B running dry causing pump damage. Results in no flow of make-up water to Electrolyser leading to stacks overheating, ultimately resulting in LOPC of stacks creating an explosive mixture with potential for ignition and explosion.									valid as same sensor as LALL-600.						): Fails to danger							Control of Ignition not claimed																disproportionate to the risk reduction achieved. There are additional non valid barriers e.g. alarm, BPCS switches and a non-rated SIL which have not been claimed in the LOPA. Considering these additional barriers, the scenario is considered ALARP.
				A	4	B	4B		LALL-600		LT-600 Low Low Level Controlled Shutdown will trigger a major fault leading to a soft shutdown, depressurization of unit. BPCS	V		Operational interlock loop, electronic DCS or single loop, automatic action (includes sensing, logic and Control valve)	1.0E-01												1.0E-03	Y											
				C	4	B	4B		LASLL-600		LSL-600 Low Low Level Switch will trigger a major fault leading to a soft shutdown, depressurization of unit. SIS	V		SIL0 - Non SIL rated IPF	1.0E+00												1.0E-03	Y											
				E	3	B	3B		FALL-600		FT-600 Low Low Flow Trip will trigger IS 1. IS 1 will de-energise the stacks(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	4.0E-03												1.0E-02	Y											
									TAH-601/2/3/4/5/6/7/8		TT-601/2/3/4/5/6/7/8 High Temperature Alarm with insufficient time for operator action. Temperature rises rapidly.	NV																											
									TAHH-601/2/3/4/5/6/7/8		TT-601/2/3/4/5/6/7/8 High High Temperature Trip will trigger a major fault leading to a soft shutdown, depressurization of unit. Not valid as third BPCS.	NV																											
2.2. Flow More	2.2.4. LIC640/FX-642/FIC642 control loop failure closing PV642	2.2.4.2. Upstream: Gradual build up of H2 gas in DG-640 resulting in release of gas contents of DG-640 into ST-600, explosive mixture with potential for ignition and explosion. Based on calculations from Elogen, the amount of H2 that is flashed in DG-640 is insufficient to result in a flammable mixture in ST-600. H2 in O2 content will not exceed 50%LFL. Internal explosion is no longer considered credible.						Y	LSLL-641		LSLL-641 Low Low Level trip will trigger IS 3. IS 3 will close PV-641 (Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	9.0E-04											9.0E-04													
									CAH-610		HIOD-610A/B/C 2oo3 High Hydrogen in Oxygen stream above ST-600. Not considered valid for this scenario.	NV																											

Node: 2. O2 Water Loop -600

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers							SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations							Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y/N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
		Consequence: 4.2.9.2							CAHH-610		HIOD-610A/B/C 2oo3 High High Hydrogen in Oxygen stream above ST-600. Trips of IS 1(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)). Not considered valid for this scenario.	NV																														
2.3. Flow Misdirected	2.3.2. Failure of membrane in Stack gradual degradation Consequence: 4.3.1.1	2.3.2.1. Gradual increase of H2 content into O2 loop overtime minor decrease in efficiency and increased H2 content of O2 in ST-600. Potential to create flammable atmosphere within ST-600, fire and explosion within ST-600.	Hydrogen	P	5	A	5A	Y	CAH-610		HIOD-610A/B/C 2oo3 High Hydrogen in Oxygen stream above ST-600.	V				CAHH-610													1.0E-04												The design life of the stacks is 10 years assuming continuous stable load, and degradation of the stacks overtime is anticipated. As current safeguard, there is H2 in O2 detection (HIOD) with an alarm (Valid), which will give sufficient time for operations to shut down the system. In addition, there is 2oo3 SIL2 SIF which shutsdown the electrolyser at 50%LEL. There is also continuous monitoring of stack voltage which might indicate degradation, however it is not considered valid. With all of the barriers considered, therefore this scenario is considered tolerable if ALARP.
				A	4	B	4B		CAHH-610		HIOD-610A/B/C 2oo3 High High Hydrogen in Oxygen stream above ST-600. Trips of IS 1(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V																	1.0E-03												
				C	4	B	4B		VI-001/2/3/4/5/6/7/8		Continuous monitoring of stack voltage might indicate degradation, however it is not considered valid.	NV																	1.0E-03												
				E	3	B	3B																						1.0E-02											

Node: 3. O2 Production - 610

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers							SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations							Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y/N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
3.2. Flow More	3.2.1. PV-900 Driven open by PI-610	3.2.1.1. Normal operation: Operating pressure of ST-600 is greater then N2 supply pressure potential back flow of O2 into N2 system. Potential for flammable atmosphere to be formed within ST-620 or DG-640 or H2 panel. Potential for explosion within unit when purging.	Hydrogen	P	5	A	5A	Y	CV-900/901		CV-900/901 Dissimilar Check Valves	V																	1.0E-04												ALARP by HSSE Standards and Practices. Assessment based on DEP 31.38.01.25 for the N2 utility lineup
				A	4	B	4B		PAH-910		PT-910 High Pressure Alarm with operator action to stop production and vent O2 and H2. Not valid as same sensing element.	NV																	1.0E-03												

Node: 3. O2 Production - 610

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers							SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations							Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y/N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
				C	4	B	4B		PAHH-910		PT-910 High High Pressure Trip will trigger a major fault leading to a soft shutdown, depressurization of unit.	V																1.0E-03														
				E	3	B	3B		PKA-900		PT-900 High Pressure Downstream of PV-900 Alarm with operator action to stop production and vent O2 and H2. Not valid as third BPCS.	NV																1.0E-02														
	3.2.5. MPV-611 driven open failure of RDPC-001/PT-610	3.2.5.1. depressurization of the O2 Loop resulting in a 30 bar differential pressure across the stack membranes resulting in failure of stack membranes. H2 into O2 Loop creating a flammable atmosphere and potential explosion in ST-600.	Hydrogen	P	5	A	5A	Y	PDAH-001		PT-610 and PT-630 High Differential Pressure Alarm between O2 loop and H2 loop. Not valid as part of IE.	NV				PDAHH-002	Control Loop (Electronic): Fails to danger	1.0E-01	N/A	1.0E+00	1.0E-01	4.2E-03	4.2E-04	Control of Ignition not claimed	1.E+00	1.0E+00	4.2E-04	4.2E-04	1.0E-04	N	4	2. Ensure scenario is managed to a tolerable frequency considering the following options: 1. Refine the IEF by looking at the failures that result in a high differential pressure. 2. Review the SIL calculation which currently includes secondary final elements, and is there for a conservative value. 3. Review the SIL calculation to increase the test interval and reduce the PFD. 4. Review operating philosophy to ensure no personnel is in the vicinity when the electrolyser is in operation.		DOT						4.2E-04	PHA Team considers this scenario, after implementation of recommendations, to be ALARP and that adding additional barriers would be grossly disproportionate to the risk reduction achieved. Additional barriers considered: Installing additional trips.
				A	4	B	4B		PDAHH-001		PT-610 and PT-630 High High Differential Pressure trip between O2 loop and H2 loop will trigger a major fault leading to a soft shutdown, depressurization of unit. Not valid as part of IE.	NV																1.0E-03	Y													
				C	4	B	4B		PDAHH-002		PT-611 and PT-631 High Differential Pressure trips of IS 1 (Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	4.2E-03													1.0E-03	Y													
				E	3	B	3B		CAH-610		HIOD-610A/B/C 2oo3 High Hydrogen in Oxygen stream above ST-600. Not valid insufficient time.	NV																1.0E-02	Y													
									CAHH-610		HIOD-610A/B/C 2oo3 High High Hydrogen in Oxygen stream above ST-600. Trips of IS 1(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)). Not valid insufficient time.	NV																													
									GDA-611		Position sensor on MPV-611 warning. Not valid as insufficient time for operator action as ST-600 will be depressurized	NV																													

Node: 3. O2 Production - 610

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers							SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations								Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y/N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
											before action is taken.																														

Node: 4. H2 Water Loop - 620

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers							SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations								Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y/N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
4.1. Flow No/Less	4.1.8. PRV-640 fails closed	4.1.8.3. Downstream: No make-up water from DG-640 to the O2 Loop leading to low level in ST-600 resulting in CP-600A/B running dry causing pump damage. Results in no flow of make-up water to Electrolyser leading to stacks overheating, ultimately resulting in LOPC of stacks creating an explosive mixture with potential for ignition and explosion.	Hydrogen	P	5	A	5A	Y	LAL-600		LT-600 Low Level Alarm with operator action to perform a soft shutdown. Not valid as same sensor as LALL-600.	NV				FALL-600	Regulators, Flow and Pressure: All Failure Modes Summed	1.8E-02	N/A	1.0E+00	1.8E-02	4.0E-04	7.2E-06	Control of Ignition not claimed	1.E+00	1.0E+00	7.2E-06	9.8E-05	1.0E-04	Y										9.8E-05	
				A	4	B	4B		LALL-600		LT-600 Low Low Level Controlled Shutdown will trigger a major fault leading to a soft shutdown, depressurization of unit.	V		Operational interlock loop, electronic DCS or single loop, automatic action (includes sensing, logic and Control valve)	1.0E-01													1.0E-03	Y											
				C	4	B	4B		LASLL-600		LSL-600 Low Low Level Switch will trigger a major fault leading to a soft shutdown, depressurization of unit. SIS	V		SIL0 - Non SIL rated IPF	1.0E+00													1.0E-03	Y											
				E	3	B	3B		FALL-600		FT-600 Low Low Flow Trip will trigger IS 1. IS 1 will de-energise the stacks(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	4.0E-03													1.0E-02	Y											
									TAH-601/2/3/4/5/6/7/8		TT-601/2/3/4/5/6/7/8 High Temperature Alarm with insufficient time for operator action. Temperature rises rapidly.	NV																													
									TAHH-601/2/3/4/5/6/7/8		TT-601/2/3/4/5/6/7/8 High High Temperature Trip will trigger a major fault leading to a soft shutdown,	NV																													

Node: 4. H2 Water Loop - 620

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers						SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations								Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y/N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk
											depressurization of unit. BPCS. Not valid as same final element as LALL-600.																												
	4.1.10. PV-641 fails closed Consequence: 4.18.1.1	4.1.10.2. Downstream: No make-up water from DG-640 to the O2 Loop leading to low level in ST-600 resulting in CP-600A/B running dry causing pump damage. Results in no flow of make-up water to Electrolyser leading to stacks overheating, ultimately resulting in LOPC of stacks creating an explosive mixture with potential for ignition and explosion.	Hydrogen	P	5	A	5A	Y	LAL-600		LT-600 Low Level Alarm with operator action to perform a soft shutdown. Not valid as same sensor as LALL-600.	NV				FALL-600	On/off Valves, All failure modes summed	6.7E-03	N/A	1.0E+00	6.7E-03	4.0E-04	2.7E-06	Control of Ignition not claimed	1.E+00	1.0E+00	2.7E-06	9.8E-05	1.0E-04	Y										9.8E-05	
				A	4	B	4B		LALL-600		LT-600 Low Low Level Controlled Shutdown will trigger a major fault leading to a soft shutdown, depressurization of unit.	V		Operational interlock loop, electronic DCS or single loop, automatic action (includes sensing, logic and Control valve)	1.0E-01													1.0E-03	Y											
				C	4	B	4B		LASLL-600		LSL-600 Low Low Level Switch will trigger a major fault leading to a soft shutdown, depressurization of unit. SIS	V		SIL0 - Non SIL rated IPF	1.0E+00													1.0E-03	Y											
				E	3	B	3B		FALL-600		FT-600 Low Low Flow Trip will trigger IS 1. IS 1 will de-energise the stacks(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	4.0E-03													1.0E-02	Y											
									TAH-601/2/3/4/5/6/7/8		TT-601/2/3/4/5/6/7/8 High Temperature Alarm with insufficient time for operator action. Temperature rises rapidly.	NV																											
									TAHH-601/2/3/4/5/6/7/8		TT-601/2/3/4/5/6/7/8 High High Temperature Trip will trigger a major fault leading to a soft shutdown, depressurization of unit. Not valid as third BPCS.	NV																											
4.2. Flow More	4.2.2. FIC-640 Control loop failure, opening PV-640	4.2.2.1. Water from the hydrogen loop will flow via DG-640 to ST-600. The level in ST-620 will reduce leading to emptying of ST-620 and	Hydrogen	P	5	A	5A	Y	LAL-620		LT-620 Low Level Alarm with insufficient time for operator action.	NV				LASLL-641	Control Loop (Electronic	1.0E-01	N/A	1.0E+00	1.0E-01	8.7E-05	8.7E-06	Control of Ignition not claimed	1.E+00	1.0E+00	8.7E-06	1.7E-05	1.0E-04	Y		3. Confirm the actual PFD of LSLL-620 based on finalisation of the SIL calculation of Elogen, and assess whether the LOPA scenario is still		DOT						1.7E-05	PHA Team considers this scenario, after implementation of recommendations, to be ALARP and that adding

Node: 4. H2 Water Loop - 620

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers						SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations							Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y/N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
		gas blow-by of H2 into ST-600. Ultimately resulting in an explosive mixture of H2 and O2 ST-620 potential for ignition and an explosion.		A	4	B	4B		LALL-620		LT-620 Low Low Level will trigger a major fault leading to a soft shutdown, depressurization of unit. BPCS	V		Operational interlock loop, electronic DCS or single loop, automatic action (includes sensing, logic and Control valve)	1.0E-01		): Fails to danger											1.0E-03	Y		tolerable. Reassess the scenario if it is not tolerable.									additional barriers would be grossly disproportionate to the risk reduction achieved.
				C	4	B	4B		LSLL-620		LSL-620 Low Low Level will initiate IS-5 (Stops the rectifiers & pumps & trigger IS1 (Safety Stop)).	V		SIL a	1.0E+00													1.0E-03	Y											
				E	3	B	3B		LSLL-641		LSL-641 Low Low Level trip will trigger IS 3. IS 3 will close PV-641 (Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	8.7E-04													1.0E-02	Y											
									CAHH-610		HIOD-610A/B/C 2oo3 High High Hydrogen in Oxygen stream above ST-600. Trips of IS 1(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)). Not considered valid for this scenario.	NV																											
	4.2.5. MV-640 set incorrectly at commissioning	4.2.5.1. Shorter residence time of Hydrogenated water in DG-640 leading to higher H2 concentration in ST-600 resulting in a flammable atmosphere of H2 and O2 in ST-600 potential for ignition and an explosion.	Hydrogen	P	5	A	5A	Y	FAHH-640		FAHH-640 High Flow Trip will trigger IS-3 will close PV-641 and Safety Stop(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	1.0E-03	FAHH-640	5.1.9.1. Human Error Probability (with procedure): HEP * number of critical steps * opportunities/yr * 1E-03 1E-03*1*0.5=5E-04	5.0E-04	N/A	1.0E+00	5.0E-04	1.0E-03	5.0E-07	Control of Ignition not claimed	1.E+00	1.0E+00	5.0E-07	5.0E-07	1.0E-04	Y		1. Provide a lock on MV-640/642 after putting the valve in position to ensure the valve cannot be manipulated.		DOT						5.0E-07	PHA Team considers this scenario, after implementation of recommendations, to be ALARP and that adding additional barriers would be grossly disproportionate to the risk reduction achieved. Adding a lock on the valve, in addition to the trip is considered ALARP.
				A	4	B	4B		CAH-610		HIOD-610A/B/C 2oo3 High Hydrogen in Oxygen stream above ST-600.	NV																1.0E-03	Y											
				C	4	B	4B		CAHH-610		HIOD-610A/B/C 2oo3 High High Hydrogen in Oxygen stream above ST-600. Trips of IS 1(Safety Stop, requires the main breaker to be reset to start-up system(manual	NV																1.0E-03	Y											
				E	3	B	3B																						1.0E-02	Y											

Node: 4. H2 Water Loop - 620

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers							SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations							Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y / N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
											operation offshore)).																														
	4.2.7. LIC-630 control loop failure opening PV-620	4.2.7.1. Downstream: Loss of level in CS-630, leading to 30barg H2 breakthrough to DG-640. Pressure build up of H2 in DG-640 resulting in H2 gas from DG-640 into ST-600, explosive mixture with potential for ignition and explosion.	Hydrogen	P	5	A	5A	Y	FIC-642/LIC-640		FIC-642/LIC-640 control loop Opening PV-642, valid as sufficient capacity (due to RO-620)	V		Operational interlock loop, electronic DCS or single loop, automatic action (includes sensing, logic and Control valve)	1.0E-01	LASLL-641	Control Loop (Electronic): Fails to danger	1.0E-01	N/A	1.0E+00	1.0E-01	8.7E-05	8.7E-06	Control of Ignition not claimed	1.E+00	1.0E+00	8.7E-06	1.7E-05	1.0E-04	Y										1.7E-05	
				A	4	B	4B		LSLL-641		LSL-641 Low Low Level trip will trigger IS 3. IS 3 will close PV-641 (Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	8.7E-04														1.0E-03	Y											
				C	4	B	4B		CAHH-610		HIOD-610A/B/C 2oo3 High High Hydrogen in Oxygen stream above ST-600. Trips of IS-1(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)). Not considered valid for this scenario.	NV																	1.0E-03	Y											
				E	3	B	3B																							1.0E-02	Y											

Node: 5. H2 Production - 630

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers							SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations							Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y / N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
5.1. Flow No/Less	5.1.9. MV-642 set incorrectly at commissioning	5.1.9.1. Upstream: Gradual build up of H2 in DG-640 resulting in release of gas contents of DG-640 into ST-600, explosive mixture with potential for ignition and explosion. Based on calculations from Elogen, the amount of H2 that is flashed in DG-640 is insufficient to result in a flammable mixture in ST-600.						Y	LASLL-641		LSL-641 Low Low Level trip will trigger IS 3. IS 3 will close PV-641 (Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	9.0E-04							9.0E-04										1. Provide a lock on MV-640/642 after putting the valve in position to ensure the valve cannot be manipulated.		DOT								
									CAH-610		HIOD-610A/B/C 2oo3 High Hydrogen in	NV																															

Node: 5. H2 Production - 630

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers						SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations							Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y / N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD		Residual Risk	
		H2 in O2 content will not exceed 50%LFL. Internal explosion is no longer considered credible.									Oxygen stream above ST-600.																												
									CAHH-610		HIOD-610A/B/C 2oo3 High High Hydrogen in Oxygen stream above ST-600. Trips of IS 1(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	NV																										
	5.1.11. PV-632 Fails to open when required	5.1.11.1. Upstream: PV-633 closes, blocked outlet of HPP. High pressure in ST-620 potential overpressure ST-620. LOPC of H2 and explosion upon ignition.	Hydrogen	P	5	A	5A	Y	PAHH-630		PT-630 High High Pressure will trigger a major fault leading to a soft shutdown, depressurization of unit. BPCS	V		Operational interlock loop, electronic DCS or single loop, automatic action (includes sensing, logic and Control valve)	1.0E-01	PAHH-631	Control Loop (Electronic): Fails to danger	1.0E-01	N/A	1.0E+00	1.0E-01	4.0E-07	4.0E-08	Control of Ignition not claimed	1.E+00	1.0E+00	4.0E-08	4.0E-08	1.0E-04	Y										4.0E-08	ALARP by HSSE Standards and Practices. Assessment based on: Overpressure DEP 80.45.10.11 (2021)
				A	4	B	4B		PAH-631		PT-631 High Pressure Alarm. Not valid as same sensing element.	NV																1.0E-03	Y											
				C	4	B	4B		PAHH-631		PT-631 High High Pressure will trigger IS 1. IS 1 will de-energise the stacks(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	4.0E-03												1.0E-03	Y											
				E	3	B	3B		PSV-630		Pressure Relief valve with a set point of 36 barg. Designed for this case.	V		RV or Vacuum Breaker (fail mode:fail to open)	1.0E-02														1.0E-02	Y											
									PSV-631		Pressure Relief valve with a set point of 36 barg. Designed for this case.	V		Second set of RV or Vacuum Breaker (fail mode:fail to open)	1.0E-01																										
	5.1.13. MV-632 set incorrectly at commissioning	5.1.13.2. Upstream: PV-633 closes, blocked outlet of HPP. High pressure in ST-620 potential overpressure ST-620. LOPC of H2 and explosion upon ignition.	Hydrogen	P	5	A	5A	Y	PAHH-630		PT-630 High High Pressure will trigger a major fault leading to a soft shutdown, depressurization of unit.	V		Operational interlock loop, electronic DCS or single loop, automatic action (includes sensing, logic and Control valve)	1.0E-01	PAHH-631	Human Error Probability (with procedure): HEP * number of critical steps * opportunities/yr * 1E-03	5.0E-04	N/A	1.0E+00	5.0E-04	4.0E-07	2.0E-10	Control of Ignition not claimed	1.E+00	1.0E+00	2.0E-10	4.0E-08	1.0E-04	Y										4.0E-08	ALARP by HSSE Standards and Practices. Assessment based on: Overpressure DEP 80.45.10.11 (2021)
				A	4	B	4B		PAH-631		PT-631 High Pressure Alarm. Not	NV																1.0E-03	Y											

Node: 5. H2 Production - 630

Deviation	Cause	Consequence	Hazard Register	RAM Score					Barriers						SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations								Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR		Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.				CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y / N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD			Residual Risk
											valid as same sensing element.						1E-03*1*0.5=5E-04																							
				C	4	B	4B		PAHH-631		PT-631 High High Pressure will trigger IS 1. IS 1 will de-energise the stacks(Safety Stop, requires the main breaker to be reset to start-up system(manual operation offshore)).	V		SILx - Real PFD	4.0E-03												1.0E-03	Y											
				E	3	B	3B		PSV-630		Pressure Relief valve with a set point of 36 barg. Designed for this case.	V		RV or Vacuum Breaker (fail mode:fail to open)	1.0E-02												1.0E-02	Y											
									PSV-631		Pressure Relief valve with a set point of 36 barg. Designed for this case.	V		Second set of RV or Vacuum Breaker (fail mode:fail to open)	1.0E-01																								
5.2. Flow More	5.2.1. PV-920 Driven open	5.2.1.1. Normal operation: Operating pressure of ST-620 is greater then N2 supply pressure potential back flow of H2 into N2 system. Potential for flammable atmosphere to be formed within ST-600. Potential for explosion within unit when purging.	Hydrogen	P	5	A	5A	Y	CV-920/921		CV-920/921 Dissimilar Check Valves	V														1.0E-04												ALARP by HSSE Standards and Practices. Assessment based on DEP 31.38.01.25 for the N2 utility lineup
				A	4	B	4B		PAH-920		PT-920 High Pressure Alarm with operator action to stop production and vent O2 and H2. Not valid as same sensing element.	NV														1.0E-03												
				C	4	B	4B		PAHH-920		PT-920 High High Pressure Trip will trigger a major fault leading to a soft shutdown, depressurization of unit.	V														1.0E-03												
				E	3	B	3B		PKA-920		PT-920 High Pressure Downstream of PV-920 Alarm with operator action to stop production and vent O2 and H2. Not valid as third BPCS.	NV														1.0E-02												

Node: 6. H2 Purification - 700

Deviation	Cause	Consequence	Hazard Register	RAM Score						Barriers						SIF Summation - Threat	IE Type	IE Frequency	EFs		Total Event Frequency	Barrier Total PFD	MEF (/yr)	Conditional Modifiers (right-hand side barriers)			Scenario Residual Risk Frequency	Threat Res. Risk Freq.	Tolerable?			Recommendations							Res. Risk Freq. After Recs	SIF Summation - Threat	ALARP Determination
				R	S	L	RR			Barrier Tag	SCE Tag	Barrier Description	Barrier Validity	Prevents SIF Demand?	Protective Layer Description	PFD				EF Description	EF Prob.			CM Description	CM Probability	Total CM PFD			Freq (/yr)	Y / N	Gap (RRF)	Recommendation	Interim Measure	Resp.	HAZOP/LOPA Action	Protective Layer Description	PFD improvement	Total PFD			Residual Risk
6.2. Flow More	6.2.2. Failure of PIC-630 driving MPV-630 open	6.2.2.1. Loss of back pressure on ST-620. Reversal of differential pressure on stack membranes. Damage to stack membranes. Potential oxygen migration into hydrogen system. Potential explosion within hydrogen system.	Hydrogen	P	5	A	5A	Y	N	RDPC-001		PT-610 and PT-630 Low Pressure Differential Alarm between O2 and H2 loop with a set point of -0.1 bar with operator action.	NV					Control Loop (Electronic): Fails to danger	1.0E-01	N/A	1.0E+00	1.0E-01	4.2E-03	4.2E-04	N/A	1.E+00	1.0E+00	4.2E-04		1.0E-04	N	4	2. Ensure scenario is managed to a tolerable frequency considering the following options: 1. Refine the IEF by looking at the failures that result in a high differential pressure. 2. Review the SIL calculation which currently includes secondary final elements, and is there for a conservative value. 3. Review the SIL calculation to increase the test interval and reduce the PFD. 4. Review operating philosophy to ensure no personnel is in the vicinity when the electrolyser is in operation.		DOT							PHA Team considers this scenario, after implementation of recommendations, to be ALARP and that adding additional barriers would be grossly disproportionate to the risk reduction achieved. Additional barriers considered: Installing additional trips.
				A	4	B	4B			RDPC-001		PT-610 and PT-630 Low Low Pressure Differential between O2 and H2 loop with a set point of -0.5 bar. It will trigger a major fault leading to a soft shutdown, depressurization of unit. BPCS	NV															1.0E-03	Y													
				C	4	B	4B			PDSLL-002		PT-631 and PT-611 Low Low Pressure Differential between O2 and H2 loop with a set point of -0.5 bar. It will trigger IS 1, IS 1 is a safety fault leading to a hard shutdown, depressurization of unit.	V		SILx - Real PFD	4.2E-03												1.0E-03	Y													
				E	3	B	3B			CAHH-800		FX-800 diverts flow to vent closing PV-633 (FC) and opening PV-632 (FO). Flow through PV-632 is through MV-632 which restricts flow creating back pressure on ST-620. BPCS	NV															1.0E-02	Y													

Appendix B.2 Fuel Cell LOPA

HOLD1

APPENDIX C LOPA RECOMMENDATIONS

Appendix Table C-1: LOPA Recommendations

LOPA Rec No.	Recommendation	Responsible Discipline/ Person	Place(s) Used
1	Provide a lock on MV-640/642 after putting the valve in position to ensure the valve cannot be manipulated.	DOT	Consequences: 4.2.5.1, 5.1.9.1
2	Ensure scenario is managed to a tolerable frequency considering the following options: 1. Refine the IEF by looking at the failures that result in a high differential pressure. 2. Review the SIL calculation which currently includes secondary final elements, and is therefore a conservative value. 3. Review the SIL calculation to increase the test interval and reduce the PFD. 4. Review operating philosophy to ensure no personnel is in the vicinity when the electrolyser is in operation.	DOT	Consequences: 3.2.5.1, 6.2.2.1
3	Confirm the actual PFD of LSLL-620 based on finalisation of the SIL calculation of Elogen, and assess whether the LOPA scenario is still tolerable. Reassess the scenario if it is not tolerable.	DOT	Consequences: 4.2.2.1

APPENDIX D PHAPRO FILES

Electrolyzer

Fuel Cell

[HOLD]