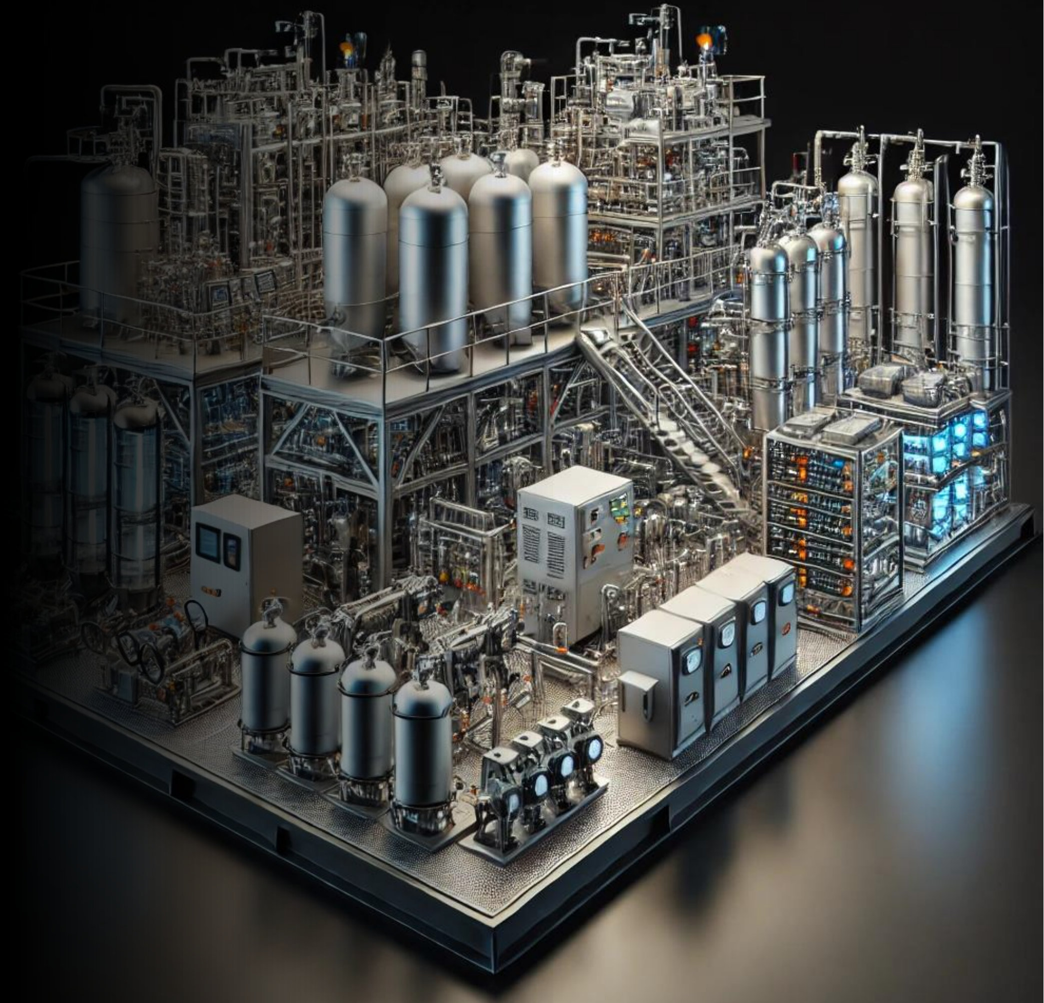
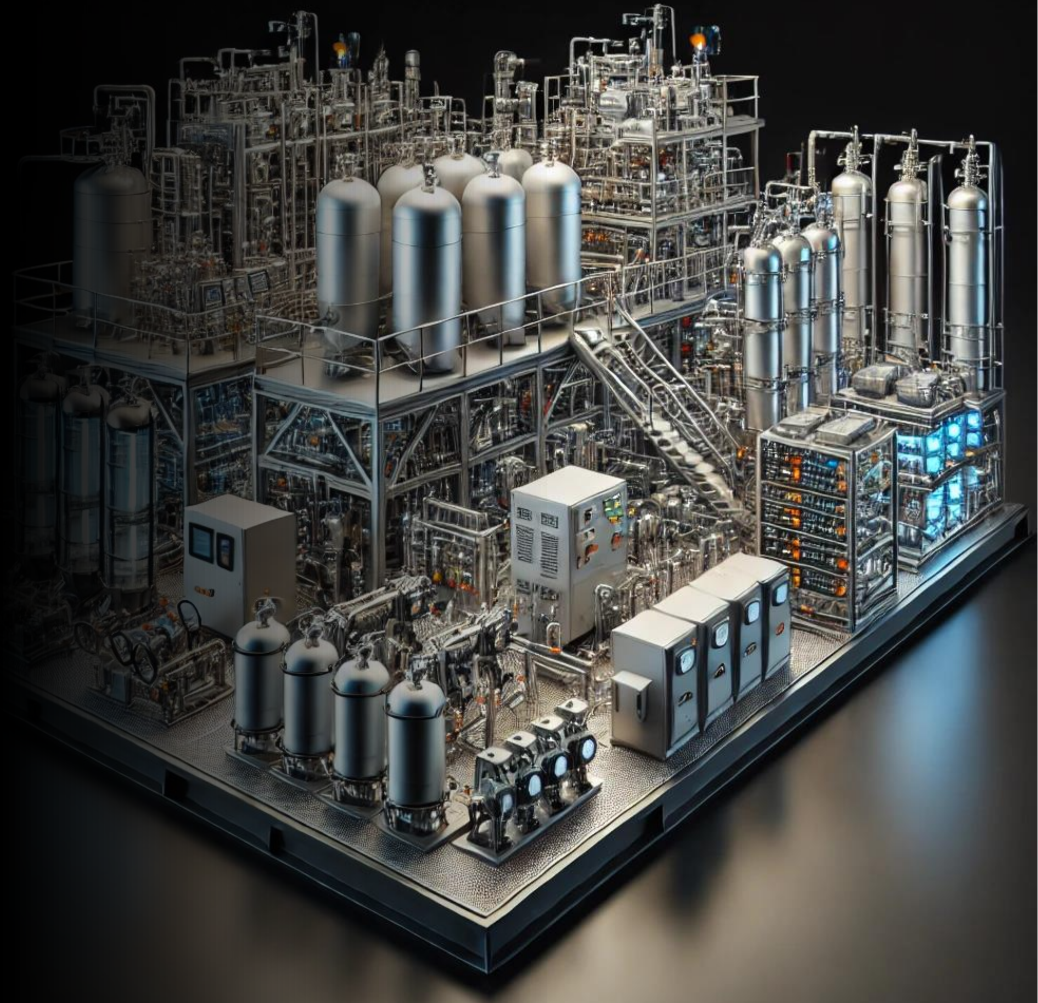
Socotec Technical Consulting

HAZOP Report

Études de Risques et la Sécurité du Skid Hydrogène



20241009_ SEGULA_ HAZOP Report_Études de Risques et la Sécurité du Skid Hydrogène_V01



1 – Introduction

This document presents the Hazard & Operability Study (HAZOP) report performed for the XL Pilot electrolyzer, consisting of stacks, to manage risks during normal operation and operability aspects, including startup, shutdown (hot and cold stand-by), and maintenance.

The aim is to assess the risks of one (1) module of the XL Pilot electrolyzer and evaluate the prevention and mitigation measures.

The study was conducted by SEGULA, with SOCOTEC leading the HAZOP. McPhy, as the final user, participated in all the workshops.

Objectives of the HAZOP:

- Identify process deviations that may lead to risks concerning safety, the environment, and assets.
- Assess the identified risks.
- Analyze the prevention and mitigation measures for each risk scenario.
- Evaluate the residual risk and, where necessary, propose improvements to achieve ALARP (As Low As Reasonably Practicable) or acceptable risk levels.

The review covers the electrolyzer stacks, separators, gas and electrolyte coolers, condensate pots, filters, and pumps. It excludes the Power Distribution Unit (PDU), venting system, draining system, and utilities such as the chilled water system, cooling water system, instrument air, and nitrogen system.

This HAZOP analysis for the XL Pilot electrolyzer is primarily based on the analysis conducted for the ML3200 model.

The HAZOP was carried out using P&ID – Revision A as a reference. A list of actions was issued, and the HAZOP was updated accordingly. The report is updated based on the P&ID included in the Reference Documents section.

Conseil et assistance

2 - Reference Documents

# REFERENCE	Référence
[1]	DOC-D-0235 IEC 61511 – Guideline (McPhy internal guideline)
[2]	MO472-01-PRO-BOD-017 Process description Rev0
[3]	MO472-01-PRO-PFD-001-00
[4]	MO472-01-PRO-PID-004-Cell stack Rev00
[5]	MO472-01-PRO-PID-005-Chilled water-Rev00
[6]	MO472-01-PRO-PID-006-Cooling water-Rev00
[7]	MO472-01-PRO-PID-007-00-Demineralization water
[8]	MO472-01-PRO-PID-008-00 Electrolyte pump & cooler-Rev00
[9]	MO472-01-PRO-PID-010-00 H2 separator-Rev00
[10]	MO472-01-PRO-PID-011-Instrument Air Distribution-Rev00
[11]	MO472-01-PRO-PID-012-00- Interconnecting
[12]	MO472-01-PRO-PID-013-NITROGEN SYSTEM -Rev00
[13]	MO472-01-PRO-PID-014-00 O2 separator-Rev00
[14]	MO472-01-PRO-PID-compilation for review
[15]	[M31] DE-RE2220-BQB-HAZ-HAZOP Report-C

Table 1 – Reference documents

3 – Acronyms

3 – 1 Acronyms

ALARP	As Low As Reasonably Practicable
DCS	Basic Process Control System
CCPS	Center for Chemical Process Safety
DCS	Distributed Control System
DP	Design Pressure
DT	Design Temperature
HAZOP	HAZard OPerability
IEC	International Electrotechnical Commission
LFL	Lower Flammability Limit
IPL	Independent Protection Layer
P&ID	Piping & Instrumentation Diagram
PFDavg	Average Probability of Failure on Demand
PLC	Programmable Logic Control
PSV	Pressure Safety Valve
RRF	Risk Reduction Factor
SIF	Safety Integrity Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System (S-PLC)

4 - Executive Summary

A HAZOP was conducted for the XL Pilot system, focusing on identifying potential risks and determining the necessary prevention and mitigation measures. Over the course of nine (9) workshops, various risk scenarios were analyzed, and a list of associated actions has been generated. Some of these actions remain open and must be addressed to complete the analysis of all scenarios and to ensure that the risk levels are reduced to acceptable levels (see Appendix D – List of Actions).

The safeguards identified during the review are detailed in Appendix C – Safeguards Without Safety Instrumented Functions (SIF) and in Appendix C – List of SIF. The total number of safeguards identified is as follows:

- 21 control function (DCS)
- 2 PSV
- 2 alarms for operator action
- 34 SIF

5 - HAZOP Methodology

The HAZOP has been conducted using Excel, in accordance with McPhy's internal guideline (Ref. [1]), which was approved by McPhy's top management. The analysis was based on, and updated with, the results from the previous HAZOP conducted for the XL Module McLyzer 3200 (Ref. [15]).

The methodology begins by identifying potential causes and consequences of process deviations using guidewords, as outlined in Table 2 – Parameters and Deviations. For each identified scenario, the independent protection layers (see Table 5 – Safeguards RRF) that prevent or mitigate the associated hazards are documented. Afterward, the risk is calculated and analyzed to determine whether additional risk reduction measures are required.

The next slide explains in detail how the risk is evaluated and how the need for further risk reduction is assessed.

5 - HAZOP Methodology

Parameter	Guideword
Flow	More
	Less / No
	Reverse
	Misdirected
Pressure	More
	Less
Temperature	More
	Less
Level	High
	Low
Composition	Change
Concentration (KOH)	Change
Utilities	Loss
Current/Voltage	More
	Less
Operation	Start-up
	Maintenance

Table 2 – Parameters and deviations

Conseil et assistance

5 - HAZOP Methodology

5 – 1 Risk Matrix

The following risk matrix is used, with three (3) color-coded regions corresponding to different approaches for addressing the risk:

- The green region represents risks that can be accepted without the need for further investigation.
- The yellow region corresponds to the ALARP zone, where the risk should be reduced to As Low As Reasonably Practicable.
- The red region indicates unacceptable risks that must be reduced to at least the ALARP zone or preferably to an acceptable level.

SEVERITY	CONSEQUENCES		LIKELIHOOD				
	Environment	Assets	1	2	3	4	5
			Very unlikely	Unlikely	Rare	Probable	Frequent
5	Catastrophic effect	Loss of facility					
4	Major effect	Loss of unit Long term SD					
3	Moderate effect	Loss of critical eqpt Middle term SD					
2	Minor effect	Eqpt damage Short term SD					
1	Slight effect	Minor effect					

Figure 1 – Safety matrix for environment and assets

SEVERITY	CONSEQUENCES	LIKELIHOOD				
	People	1	2	3	4	5
		Very unlikely	Unlikely	Rare	Probable	Frequent
5	> 3 fatalities					
4	1 to 3 fatalities					
3	Major injury					
2	Minor injury					
1	Slight injury					

Figure 2 – Risk matrix for people

5 - HAZOP Methodology

5 – 2 Risk Acceptance Criteria

The risk is considered acceptable if one of the following criteria is met:

- The risk falls within the acceptable region (green zone).
- The risk falls within the ALARP region (yellow zone) and affects only the environment or assets.
- The risk falls within the ALARP region (yellow zone) and affects people with a severity level of S4 or S5.

5 – 3 Frequency

The risk matrix is divided into five (5) frequency categories:

Likehood	1	2	3	4	5
Definition	Very unlikely	Unlikely	Rare	Probable	Frequent
Design	Risk already well know and covered and fully addressed in the design	Risk well know and covered but not yet fully addressed in the design	Risk not expected but possible, not yet addressed in the design	Risk possible	Risk expected
Frequency	$F \leq 10^{-5}/y$	$10^{-5}/y < F \leq 10^{-4}/y$	$10^{-4}/y < F \leq 10^{-3}/y$	$10^{-3}/y < F \leq 10^{-2}/y$	F> 10-2/year
Historical	Never heard of in the industry	Has already occurred in industry but many corrective actions have been taken	Has already occurred in industry but corrective action has been taken	Has already occurred on similar facility	Has already occurred several times on several facility

Figure 3 – Frequency categories

Conseil et assistance

5 - HAZOP Methodology

5 – 3 Frequency

Next, the event frequency is evaluated based on the main event frequencies considered during the HAZOP, as follows:

Initiating Event	Frequency (per year)	Reference
Safety valve opens spuriously	10^{-2}	[15]
Pressure Safety valve opens spuriously	10^{-4}	[15]
DCS instrument loop failure	10^{-1}	[15]
Check valve failure	10^{-1}	[15]
Filter plugged	10^{-1}	[15]
Filter plugged on hydrogen pipe	10^{-2}	[15]
Exchanger pin hole	10^{-2}	[15]
Tube rupture inside heat exchanger	10^{-2}	[15]
Pump or blower failure	10^{-1}	[15]
Operator error during nonroutine task following written procedure	10^{-2}	[15]

5 - HAZOP Methodology

5 – 4 Severity

The severity is quoted according to the following table:

Severity	Definition	PEOPLE	Environment	ASSET
5	Disaster	1 fatality outside boundaries Multiple fatalities inside boundaries	Catastrophic effect External massive, irreversible	Loss of the facility Extensive damage Abandon
4	Catastrophic	1 to 3 fatalities inside boundaries Severe injuries inside boundaries Injuries outside the boundaries	Major effect External massive, reversible External large, irreversible	Major damage Loss of 1 unit Long term shutdown
3	Major	Major Injuries Irreversible disabilities	Moderate effect External large, reversible Internal irreversible	Localized damage Loss of one equipment Middle term shutdown
2	Significant	Injuries Reversible disabilities	Minor effect Limited discharge above limit value Internal reversible	Equipment internal damages Significant maintenance Short term shutdown
1	Minor	Slight disturbance	Slight effect	Minor Effects Slight damage Maintenance issue

5 - HAZOP Methodology

5 – 4 Severity

In order to evaluate the severity, the following considerations were used:

- **Sp=5, Se=3** and **Sa=5** for an explosion inside the separator
- **Sp=4 a**nd **Sa=4** for the loss of the chilled water system (tube rupture inside heat exchanger). A failure of the heat exchanger leads to the overpressure and rupture of the chilled water system. This scenario leads to a hydrogen leakage, jet fire and potential explosion and fatality
- **Sa=4** for the loss of the cooling water system (pin hole inside heat exchanger). Cooling water contaminated with electrolyte with H_2/O_2 degassing and overpressure of the cooling water system (No piping corrosion)
- **Sp=3**, **Se=2** and **Sa=3** for the overheating scenarios of the stack. Insufficient cooling of the stack exceeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O_2/H_2 leading to operator exposure to hot and corrosive stream
- **Se=2** for the loss of containment scenarios given the presence of the draining system designed to collect the total capacity of the KOH
- **Sa=2** for the loss of efficiency or loss of production

5 - HAZOP Methodology

5 – 5   Safeguards RRF

The following table provides the main safeguards and Risk Reduction Factor (RRF):

Safeguard	RRF	Reference
PSV	100	[15]
DCS	10	[15]
SIF - SIL 1	10	[15]
SIF - SIL 2	100	[15]
SIF - SIL 3	1000	[15]

C o n s e i l   e t   a s s i s t a n c e

5 - HAZOP Methodology

5 – 6   Main Assumptions and Exclusions

5 – 6 – 1 Assumptions

To carry out the HAZOP, the following main assumptions are considered.

Ref	Assumption
A1	Lines, equipment, and material are specified and designed to withstand Normal Operating Conditions of stresses, temperature, pressure, humidity and other parameter expecting during start-up, shut-down, normal, test and maintenance operations. Environmental conditions of the operating location, of the factory, assembly, tests, and maintenance locations and during transport between these locations are also covered.
~~A2~~	~~Operators are trained and have knowledge of the installation. Frequency of mistakes due to operator is 1/100 per year.~~
~~A3~~	~~Maintenance, inspection, verification and tests are well led in the specified period and in the expected way.~~
A4	When a control or on/off valve is identified as a cause of the scenario, the DCS control loop failure from sensor to actuator is considered since the scenario could be the result of the valve itself or the sensor or the PLC.
A5	Consequences were reviewed without any safeguards but considering design itself.
A7	DCS as protection layer It is possible to consider the DCS as a protection layer if the inputs, outputs are independent from the initiating source for the demand of the risk scenario, provided the maintenance on the DCS is performed by trained and qualified personnel.
A8	DCS as an initiating event: PFDavg $= 10^{-1}$ (Ref. [15]). Indeed, the maintenance on the DCS is carried out by trained and qualified personnel/operators only. With this consideration, DCS cannot be accounted as a safeguard in the scenario.
~~A9~~	~~Failures coming from upstream utilities such as the cooling water system (Sc. 1.5.3.1), chilled water system (Sc. 4.5.4.1, 5.5.4.1), instrument air (Sc. 1.14.1.2) and demineralized water plant (Sc. 4.2.6.1) are assumed to be a DCS failure.~~
~~A10~~	~~Low/high current is assumed to be a DCS failure (Sc 1.16.1.1, 2.15.1.1, 2.16.1.1).~~
~~A11~~	~~Change in composition of the Demin water is assumed to be a failure of the DCS (Sc. 4.11.1.1).~~
~~A12~~	~~Human error scenarios on padlocked and capped valves are not considered in the HAZOP.~~

5 - HAZOP Methodology

5 – 6 Main Assumptions and Exclusions

5 – 6 – 2 Exclusions

The following events are not considered in the HAZOP. They are part of the client Risk/HAZID/Vulnerability analysis.

Ref	Exclusions
E1	Intentional mistakes, errors or sabotages.
E2	Simultaneously jeopardizes.
E3	Cyberattacks or malware.
E4	Gasket or line leaks without identified cause.
E5	Damages caused by lightning and thunder, earthquakes, fire at proximity, natural or technologic disaster and any damage caused by an external source.

Conseil et assistance

6 – Review team

The review team, led by SOCOTEC, included experts from SEGULA, responsible for conducting the study, and representatives from the final client, MCPHY, who will ultimately be the end user. Each team was composed of professionals knowledgeable and experienced in their respective fields. However, all the safety workshops were coordinated and managed by SOCOTEC.

First name / Last name	Société	contact
Vinay KURUP	MCPHY	vinay.kurup@mcphy.com
Hady NESBAY	MCPHY	hady.nesbay@mcphy.com
Frederic STAINE	MCPHY	frederic.staine@mcphy.com
Christophe GAVELLE	MCPHY	christophe.gavelle-ext@mcphy.com
Valentin VOILLAUME	MCPHY	valentin.voillaume@mcphy.com
Frank KENGNE	MCPHY	frank.kengne-ext@mcphy.com
Adeline Lecesne	MCPHY	a.lecesne@mcphy.com
Mustapha AZMAL	MCPHY	mustapha.azmal-ext@mcphy.com
Cyril George	MCPHY	cyril.george@mcphy.com
Jean-Charles FAVERGER	MCPHY	jean-charles.faverger@mcphy.com
Navid SOHRABI	MCPHY	navid.sohrabi@mcphy.com
Daniel FRIESE	MCPHY	daniel.friese@mcphy.com
jacek.papina	MCPHY	jacek.papina@mcphy.com
Alexandre SERPOLLIER	MCPHY	alexandre.serpollier@mcphy.com
LEBRUN SERGE	SEGULA	SERGE.LEBRUN@segula.fr
Loic Delabrousse	SEGULA	loic.delabrousse-ext@segula.fr
Viviane BENEZETH	SEGULA	viviane.benezeth@segula.fr
David BAELEN	SEGULA	david.baelen@segula.fr
Damien RIVAL	SEGULA	damien.rival@segula.fr
Ali EL OUAZZANI	SOCOTEC	ali.elouazzani@socotec.com
Regis BODIGUEL	SOCOTEC	regis.bodiguel@socotec.com

7 - Conclusions

7 – 1 HAZOP Scenarios

The results of the HAZOP analysis are documented in the worksheets found in Appendix E – HAZOP Worksheet.

These sheets outline all the scenarios that were discussed and approved by the participants during the review, detailing the causes, consequences, safeguards, and associated risk rankings.

In total, 200 scenarios were reviewed.

7 – 2 HAZOP actions

During the HAZOP review, actions were identified and assigned to the relevant parties for the following reasons:

- When the risk was not mitigated to an acceptable level
- When the existing safeguards were deemed inadequate
- When further information was required to finalize the scenario

Appendix D – List of Actions, contains the complete list of 28 actions assigned during the review process.

Conseil et assistance

7 - Conclusions

7 – 4 List of safeguards without SIF

All the safeguards are deemed sufficient enough to reduce the risk were recorded during the HAZOP review and listed in Appendix C – Safeguards. The safeguards are classified as follow:

- 21 control function (DCS)
- 2 PSV
- 2 alarms for operator action

8 – 5 List of SIF

All the SIF deemed sufficient to reduce the risk were recorded during the HAZOP review and listed in Appendix D – List of SIF. The list includes 34 SIF.

8 - Appendix A – Nodes (1/4)

Node	Design Intent	Drawings / References	Rev | date	Document Title	Tag	Description	Pressure (barg)		Temperature (°C)		Other
							Pop	Pdes	Top	Tdes	
1. ELECTROLYTE CIRCULATION	To control the circulating overall flow, cool down, heat (for low ambient temperature condition) and filter (10% of the flow through the filter) the electrolyte that will feed anolyte and catholyte to the stacks.	MO472-01-PRO-PID-004	00 | 02/08/24	Cell Stack	P-1001 A/B	Electrolyte Circulation Pump	Suction = 28 discharge = 30.8	40	57 / 85	-20 / 100	190 m3/h
		MO472-01-PRO-PID-012-00	00 | 06/08/24	Interconnecting	F-1001	Electrolyte Slipstream Filter	30,8	40	57 / 85	-20 / 100	19 m3/h
		MO472-01-PRO-PID-010	00 | 31/07/24	Hydrogen Separation	B-1001	Heat Exchanger	28,0	33	inlet : 85 outlet: 75	-20 / 100	190 m3/h
		MO472-01-PRO-PID-014	00 | 31/07/24	Oxygen Separation	B-1003	Heater	33,8	39	inlet : 10 outlet: 20	-20 / 100	10 m3/h
		MO472-01-PRO-PID-008-00		Electrolyte Pumps and Cooler							
2. CATHOLYTE CIRCULATION	To control the catholyte flow to the stacks using temperature transmitter. To produce H2 sent to H2 separator	MO472-01-PRO-PID-004	00 | 02/08/24		P1001 A/B	Cell Stack	29.5 / 31	34 (1st phase) 37 (2de phase)	85 / 57	-20 / 100	H2 = 200 Nm3/h
		MO472-01-PRO-PID-012-00	00 | 06/08/24	Interconnecting	F-1001	Hydrogen Separator	28,0	33	57 / 85	-20 / 100	H2 = 800 Nm3/h
		MO472-01-PRO-PID-010	00 | 31/07/24	Hydrogen Separation							

8 - Appendix A – Nodes (2/4)

Node	Design Intent	Drawings / References	Rev | date	Document Title	Tag	Description	Pressure (barg)		Temperature (°C)		Other
							Pop	Pdes	Top	Tdes	
2.1 Network (H2 / KOH) / Half production (2/4 of 1 MW stacks)	To control the catholyte flow to the stacks temperature transmitter. To produce H2 sent to H2 separator	MO472-01-PRO-PID-004	00 | 02/08/24	Cell Stack	P1001 A/B	Cell Stack	29.5 / 31	34 (1st phase) 37 (2de phase)	85 / 57	-20 / 100	H2 = 200 Nm3/h
		MO472-01-PRO-PID-012-00	00 | 06/08/24	Interconnecting	F-1001	Hydrogen Separator	28,0	33	57 / 85	-20 / 100	H2 = 800 Nm3/h
		MO472-01-PRO-PID-010	00 | 31/07/24	Hydrogen Separation							
3. ANOLYTE CIRCULATION	To control the anolyte flow to the clusters using temperature transmitter. To produce O2 sent to O2 separator	MO472-01-PRO-PID-004	00 | 02/08/24	Cell Stack	P1001 A/B	Cell Stack Cluster 1 (4MW)	29.5 / 31	34	85 / 57	-20 / 100	O2 = 400 Nm3/h
		MO472-01-PRO-PID-012-00	00 | 06/08/24	Interconnecti ng	F-1001						
		MO472-01-PRO-PID-014	00 | 31/07/24	Oxygen Separation		Oxygen Separator	28,0	33	57 / 85	-20 / 100	O2 = 400 Nm3/h
3.1. Network (O2 / KOH) / Half production (2/4 of 1 MW stacks) U1003/4 operating and U1005/6 shutdown	To control the anolyte flow to the clusters using temperature transmitter. To produce O2 sent to O2 separator	MO472-01-PRO-PID-004	00 | 02/08/24	Cell Stack	P1001 A/B	Cell Stack Cluster 1 (4MW)	29.5 / 31	34	85 / 57	-20 / 100	O2 = 400 Nm3/h
		MO472-01-PRO-PID-012-00	00 | 06/08/24	Interconnecti ng	F-1001						
		MO472-01-PRO-PID-014	00 | 31/07/24	Oxygen Separation		Oxygen Separator	28,0	33	57 / 85	-20 / 100	O2 = 400 Nm3/h

8 - Appendix A – Nodes (3/4)

Node	Design Intent	Drawings / References	Rev | date	Document Title	Tag	Description	Pressure (barg)		Temperature (°C)		Other
							Pop	Pdes	Top	Tdes	
4. HYDROGEN SEPARATION	To separate H2 from the catholyte and send it OSBL. To control the H2 pressure using the absolute pressure, or the differential pressure between the H2 and O2 separator (DP override the absolute pressure). To maintain the level between both separators using the balancing line. To control the level by feeding ultra pure water.	MO472-01-PRO-PID-012-00	00 | 06/08/24	Interconnecting		Hydrogen Separator	28,0	33	57 / 85	-20 / 100	H2 = 800 Nm3/h
		MO472-01-PRO-PID-010	00 | 31/07/24	Hydrogen Separation		Hydrogen Gas Cooler	28,0	33	inlet : 85 outlet: 30	-20 / 100	H2 = 800 Nm3/h
5. OXYGEN SEPARATION	To separate O2 from the anolyte and send it OSBL. To control the H2 pressure using the absolute pressure, or the differential pressure between the H2 and O2 separator (DP override the absolute pressure). To maintain the level between both separators using the balancing line. To control the level by feeding ultra pure water in the H2 separator.	MO472-01-PRO-PID-012-00	00 | 06/08/24	Interconnecting		Oxygen Separator	28,0	33	57 / 85	-20 / 100	O2 = 400 Nm3/h
		MO472-01-PRO-PID-014	00 | 31/07/24	Oxygen Separation		Oxygen Gas Cooler	28,0	33	inlet : 85 outlet: 30	-20 / 100	O2 = 400 Nm3/h
6. Cell stack HOT STAND-BY MODE	Cell stack Stand-by for system turn down (max 10%, 3 clusters out of 4) 30,9 barg opearting pressure : - Rectifier stopped										

8 - Appendix A – Nodes (4/4)

Node	Design Intent	Drawings / References	Rev | date	Document Title	Tag	Description	Pressure (barg)		Temperature (°C)		Other
							Pop	Pdes	Top	Tdes	
7. MODULE HOT STAND-BY MODE	Module Stand-by for plant turn down and fast ramp up (30.9 barg operating pressure): - All rectifiers stopped - Ultra pure water isolated - All PV outlet closed - Cooling stopped - Pump stopped										
8. H2 COLD STAND-BY MODE	Modules cold stand-by from hot stand-by mode or after a DCS shutdown (8 barg operating pressure): - Depressurization by PV1111B & PV1211B - All rectifiers stopped - Ultra pure water isolated - All PV outlet closed - Cooling stopped - Pump stopped										
9. N2 COLD STAND-BY MODE	Modules cold stand-by from stop and used to ramp up: - All rectifiers stopped - Ultra pure water isolated - All PV outlet closed - Cooling stopped - Pump stopped										

9 - Appendix B – Safeguards Without SIF(1/6)

Safeguard Tag	Safeguard Description	Safeguard Category	Place(s) Used
FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow trip to stop the rectifier	Control (DCS)	1.1.2.1. ; 1.2.2.1. ; 1.2.3.1. ;1.2.4.1. ; 1.2.5.1. ;1.2.5.1. 1.2.6.1. ; 1.2.9.1. ; 3.1.1.1.
TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	High temperature trip to stop the rectifier (not independant from the above)	Control (DCS)	1.1.2.1. ; 1.2.2.1. ; 1.2.3.1. ; 1.2.6.1.
FT-08002	Flow meter with an alarm	Control (DCS)	1.2.8.1.
TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014		Control (DCS)	1.2.11.2.
TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	High temperature to stop the rectifier	Control (DCS)	1.5.1.1. ; 1.5.2.1. ; 1.6.3.1.
TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	Low temperature to reduce the electrolyte flow to the stacks	Control (DCS)	1.6.1.1.
FT-04005 & FT-04007 TT-04011 & TT-04012 & TT-04014	High flowrate Low delta T between both inlet / outlet to stop the rectifier	Control (DCS)	2.1.1.1.
FT-04005 & FT-04007	Low flow trip to stop the rectifier	Control (DCS)	2.1.2.1.
TT-04011 & TT-04012 & TT-04014	High temperature trip to stop the rectifier (not independant from the cause)	Control (DCS)	2.1.3.1. ; 2.2.1.2. ; 2.2.2.1.

9 - Appendix B – Safeguards Without SIF (2/6)

Safeguard Tag	Safeguard Description	Safeguard Category	Place(s) Used
FT-04005 & FT-04007	Low flow to stop the rectifier (not independant from the cause)	Control (DCS)	2.2.1.2.
FT-04005 & FT-04007	Low flow to stop the rectifier and interlock the sequences	Control (DCS)	2.2.2.1.
PSV-10002	PSV on the separators with 132% pressure	PSV	2.15.1.1. ; 2-1.15.1.
CZS-04021	High current detection to stop the rectifier	Control (DCS)	2.15.1.1. ; 2-1.15.1. ; 3.15.1.1. ; 3-1.15.1.
CZS-04021	Protection against overcurrent from the primary current of the transformer to trip the MV breaker	Control (DCS)	2.15.1.1. ; 2-1.15.1. ; 3.15.1.1. ; 3-1.15.1.
AT-10011	Alarm in case of High OTH/HTO for operator action	Alarm (DCS)	2.16.1.1. ; 2-1.16.1.
CZS-04021	Low current detection to stop the rectifier automtically	Control (DCS)	2.16.1.1. ; 2-1.16.1.1 ; 3.16.1.1. 3-1.16.1.1.
FT-04005 TT-04011	High flowrate Low delta T between both inlet / outlet	Control (DCS)	2-1.1.2.1
TT-04011	High temperature trip to stop the rectifier (not independant from the cause)	Control (DCS)	2-1.1.4.1 ; 2-1.2.1.2 ; 2-1.2.2.1

9 - Appendix B – Safeguards Without SIF (3/6)

Safeguard Tag	Safeguard Description	Safeguard Category	Place(s) Used
FT-04005	Low flow to stop the rectifier (not independant from the cause)	Control (DCS)	2-1.2.1.2
FT-04005	Low flow to stop the rectifier and interlock the sequences	Control (DCS)	2-1.2.2.1
?	High delta T between both TT to stop the rectifier	Control (DCS)	3.2.1.2.
FT-04001 & FT-04003	Low flow to stop the rectifier (not independant from the cause)	Control (DCS)	3.2.1.2.
TT-04009 & TT-04010 & TT-04013	High temperature trip to stop the rectifier (not independant from the cause)	Control (DCS)	3.2.1.2. ; 3.2.2.1.
FT-04001 & FT-04003	Low flow to stop the rectifier and shutdown the pump	Control (DCS)	3.2.2.1.
PSV-14002	PSV on the separators with 132% pressure	PSV	3.15.1.1. ; 3-1.15.1.
AT-10010	Alarm in case of High OTH/HTO for operator action	Alarm (DCS)	3.16.1.1. ; 3-1.16.1.
FT-04001 TT-04009	High flowrate Low delta T between both inlet / outlet	Control (DCS)	3-1.1.2.1

9 - Appendix B – Safeguards Without SIF (4/6)

Safeguard Tag	Safeguard Description	Safeguard Category	Place(s) Used
TT-04009	High temperature trip to stop the rectifier (not independant from the cause)	Control (DCS)	3-1.1.4.1 ; 3-1.2.1.2 ; 3-1.2.2.1
FT-04001	Low flow to stop the rectifier (not independant from the cause)	Control (DCS)	3-1.2.1.2
FT-04001	Low flow to stop the rectifier and interlock the sequences	Control (DCS)	3-1.2.2.1
LT- 10006/LT-10004	High level to stop the rectifier	Control (DCS)	4.1.4.1. ; 5.1.4.1. ; 6.1.3.1. ; 7.1.2.1.
LIC-10032	High level to stop the rectifier (not independant from the cause)	Control (DCS)	4.1.4.1. ; 5.1.4.1. ; 6.1.3.1. ; 7.1.2.1.
LT- 10006/LT-14006	Low level to stop the rectifier	Control (DCS)	4.2.2.1. ; 5.2.2.1. ; 5.7.1.1. ; 5.8.1.1.
LIC-10032	Low level to stop the rectifier (not independant from the cause)	Control (DCS)	4.2.2.1. ; 5.2.2.1.
PSV-10002	Pressure safety valve setpoint is 33Barg. PDU is at 27 Barg will never reach 33 Barg, that means the PSV will not open	PSV	4.3.1.1.
PT-13001	Low pressure alaram in the N2 distribution	Control (DCS)	4.3.2.1.

9 - Appendix B – Safeguards Without SIF (5/6)

Safeguard Tag	Safeguard Description	Safeguard Category	Place(s) Used
PDIC- 10010	High differential pressure to open production line on oxygen side (to open PCV-14017)	Control (DCS)	4.4.1.1.
PT-13001	High pressure alarm in N2 distribution	Control (DCS)	4.4.2.1.
TIC-10012	High temperature to stop the rectifier (not independent from the cause)	Control (DCS)	4.5.2.1.
TIC-10012	High temperature to stop the rectifier	Control (DCS)	4.5.3.1.
LIC-10032	Low level to stop the rectifier	Control (DCS)	4.7.2.1.
LIC-10032	High level to stop the rectifier	Control (DCS)	4.8.1.1.
PT-13007	Low pressure alaram in the N2 distribution	Control (DCS)	5.3.2.1.
PDIC- 10010	High differential pressure to open production line on Hydrogen side (to open PCV-10017 and PCV-10020)	Control (DCS)	5.4.1.1.
TIC-14026	High temperature to stop the rectifier (not independant from the cause)	Control (DCS)	1.2.6.1.
TIC-14026	High temperature to stop the rectifier	Control (DCS)	5.5.3.1.

9 - Appendix B – Safeguards Without SIF (6/6)

Safeguard Tag	Safeguard Description	Safeguard Category	Place(s) Used
PSV- 14002 & PSV-10002	PSV on the separators with 33 set pressure	PSV	6.1.1.1.
PT- 10004 & PT-14004	High pressure to open the vents on both separators.	Control (DCS)	6.1.1.1.
TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	Feedback from the rectifier to stop the electrolyzer and depressurize	Control (DCS)	6.1.1.2.

10 - Appendix C – List of SIF (1/5)

SIF Tag	Number of SIF	SIF Description	Safeguard Category	Place(s) Used
FZS-08001	1	FZI low low flow to stop the pump	SIS - SIL 2	1.1.1.1.
FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	4	Low low flow to stop the rectifier	SIS - SIL 2	1.1.2.1. ; 1.2.2.1. ; 1.2.3.1. 1.2.9.1.
TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	6	Low low temperature trip to stop the rectifier	SIS - SIL 2	1.1.2.1. ; 1.2.2.1. ; 1.2.3.1.
FZS-08007 & FZS-08006	2	FZI low low flow to stop the pump	SIS - SIL 2	1.2.1.1.
FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	4	Low low flow to stop the rectifier & the pump		1.2.4.1.
FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	4	Low low flow to stop the rectifier & the pump	SIS - SIL 2	1.2.5.1.
FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	4	Low low flow to stop the rectifier & the pump	SIS - SIL 2	1.2.6.1.
TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	6	Low low temperature to trip the rectifier & pump	SIS - SIL 2	1.2.6.1.
FZS-08005	1		NA	1.2.11.1.

10 - Appendix C – List of SIF (2/5)

SIF Tag	Number of SIF	SIF Description	Safeguard Category	Place(s) Used
TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	6	Low low temperature to stop the pumps P-1001A & P-1001B	SIS - SIL 2	1.2.11.2.
TSV-08002	1	TSV arround the both valves	SIS - SIL 2	1.2.11.3
TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	6	High high temperature to stop the rectifier	SIS - SIL 2	1.5.1.1. ; 1.5.2.1. ; 1.6.3.1.
TZS-04017 & TZS-04018 & TZS-04020	3	High high temperature to stop the rectifier (not independent from the above)		2.1.3.1. ; 2.2.1.2. ; 2.2.2.1.
FZS-04006 & FZS-04008	2	Low low flow to stop the rectifier	SIS - SIL 2	2.2.1.2. ; 2.2.2.1.
CZS-04022	1	High high current detection to stop the rectifier	SIS - SIL 2	2.15.1.1. ; 2-1.15.1. ; 3.15.1.1. ; 3-1.15.1.
CZS-04022	1	IIC Low Low current detection with a timer delay (3 mins) to stop the rectifier	SIS - SIL 2	2.16.1.1. ; 2-1.16.1. ; 3.16.1.1. ; 3-1.16.1.

10 - Appendix C – List of SIF (3/5)

SIF Tag	Number of SIF	SIF Description	Safeguard Category	Place(s) Used
TZS-04017	1	High high temperature to stop the rectifier (not independent from the above)	SIS - SIL 2	2-1.1.4.1 ; 2-1.2.1.2 ; 2-1.2.2.1
FZS-04006	1	Low low flow to stop the rectifier	SIS - SIL 2	2-1.2.1.2. ; 2-1.2.2.1.
TZI-1001A	1	High high temperature to stop the rectifier	SIS - SIL 2	3.2.1.2.
FZS-04002 & FZS-04004	2	Low low flow to stop the rectifier	SIS - SIL 2	3.2.1.2. ; 3.2.2.1.
TZS-04015 & TZS-04016 & TZS-04019	3	High high temperature to stop the rectifier	SIS - SIL 2	3.2.1.2. ; 3.2.2.1.
TZS-04015	1	High high temperature to stop the rectifier	SIS - SIL 2	3-1.1.4.1 ; 3-1.2.1.2. ; 3-1.2.2.1.
FZS-04002	1	Low low flow to stop the rectifier	SIS - SIL 2	3-1.2.1.2 ; 3-1.2.2.1

10 - Appendix C – List of SIF (4/5)

SIF Tag	Number of SIF	SIF Description	Safeguard Category	Place(s) Used
LZT-10007/8 & LZT-14007/8	2	High high level trip to isolate the demin water feeding line (to close XZV-10031)	SIS - SIL 2	4.1.4.1. ; 5.1.4.1. ; 6.1.3.1. ; 7.1.2.1. ; 8.1.2.1.
LZT-10007/8 (H2) & LZT-14007/8 (O2)	2	Low low level trip to stop the rectifier	SIS - SIL 2	4.2.2.1. ; 5.2.2.1.
LZI-10007 & LZI-1008	2	High high level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045)	SIS - SIL 2	4.4.1.1. ; 4.4.3.1. ; 4.8.1.1. ; 5.7.1.1. ; 8.1.3.1. ; 8.4.1.1.
LZI-14007 & LZI-14008	2	Low low level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2	4.4.1.1. ; 4.4.3.1. ; 4.8.1.1. ; 5.7.1.1. ; 8.1.3.1. ; 8.4.1.1.
TZT-10018	1	High high trip temperature to stop the rectifier	SIS - SIL 2	4.5.2.1. ; 4.5.3.1.
LZI-10007 & LZI-1008	2	Low Low level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045)	SIS - SIL 2	4.7.2.1. ; 5.4.1.1. ; 5.4.2.1. ; 5.8.1.1. ; 8.1.4.1. ; 8.4.2.1.
PZT-10005	1	High high pressure trip to stop the rectifier	SIS - SIL 2	4.7.2.1. ; 8.4.2.1.

10 - Appendix C – List of SIF (5/5)

SOCOTEC

SIF Tag	Number of SIF	SIF Description	Safeguard Category	Place(s) Used
LZI-14007 & lzi-14008	2	High high level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2	4.7.2.1. ; 5.4.1.1. ; 5.4.2.1. ; 5.8.1.1. ; 8.1.4.1. ; 8.4.2.1.
TZT-10013	1	High high temperature to stop the rectifier	SIS - SIL 2	1.2.6.1. ; 5.5.3.1.
PZI-10005 & PZI-14005	2	High high pressure to stop the rectifier	SIS - SIL 2	6.1.1.1.
TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	6	High high temperature to stop the rectifier	SIS - SIL 2	6.1.1.2.

Conseil et assistance

11 - Appendix D – List of Actions (1/3)

SOCOTEC

Actions	Place(s) Used	Responsibility
1. The safety Temperture transmitter has to be added in the P&ID	consequeces 1.1.2.1.	SEGULA
2. To design ventilation system in a way to avoid H2 accumulation due to LOC of the stack consequently avoidin an exploison. In addition to monitoring system for the ventilation to stop the XL PILOT in case the ventilation is not working. 2. Investigate the critical component in the stack following an overheating scenario (cells stack, end flange , flexible hoses)	consequeces 1.2.2.1.	SEGULA
3. Check the maximum pump shut off head at maximum speed 3600 RPM	consequeces 1.2.3.2.	Segula
4. Unclogging the mesh from the maintenance service	consequeces 1.2.4.1.	SEGULA
5. Confirm the consequences of operting the stack below 5 degres	consequeces 1.2.11.2.	SEGULA / MCPHY
6. Is the control automatic back up?	consequeces 1.4.1.1.	SEGULA
7. Confirm the consequences of operting the stack below 5 degres	consequeces 1.6.3.1.	SEGULA
8. Check about the safeguards for the cooling system	consequeces 1.7.3.1.	SEGULA
9. To define the startup and shutdown philosphy	consequeces 1.13.1.1.	SEGULA

/ / / CONFIDENTIAL / / /

11 - Appendix D – List of Actions (3/3)

Actions	Place(s) Used	Responsibility
10. to define the draining and filling procedure and think about a keying feature To remove a human errors, to think about a safe design (interlocks…)	consequeces 1.13.2.1	SEGULA
11. To define each valve which are condisered during the design	consequeces 1.14.1.1.	SEGULA
12. The safety Temperature transmitter must be added in the P&ID	consequeces 2.1.3.1 ; 2-1.1.4.1 ; 3.1.3.1. ; 3-1.1.4.1	SEGULA
13. Issues regarding the interlocking	consequeces 2.4.1.1	SEGULA
14. Issue regarding the flexible hose's connection	consequeces 2.4.1.2	SEGULA
15. To identify the worse case, Control de Max current of the rectifier if the protection is lost	consequeces 2.15.1.1. ; 2-1.15.1. ; 3.15.1.1. ; 3-1.15.1.	SEGULA
16. To confirm with rectifier's supplier to stop it automatically in case of low current detection	consequeces 2.16.1.1. ; 2-1.16.1. ; 3.16.1.1. ; 3-1.16.1.	SEGULA/MCPHY
17. The distance must be studied in HAZAN scenario to reduce the severity. To check with the supplier what can be the reason behind this low current to see if we must reduce the frequency	consequeces 2.16.1.1. ; 2-1.16.1. ; 3.16.1.1. ; 3-1.16.1.	SEGULA
18. Check the pressure drop btween stacks 5/6 on H2 side and H2 separator	consequeces 2-1.1.2.1	SEGULA
19. To design the pipe supports to withstand the production lines filled with liquid in order to avoid mechanical pipe rupture. Thus, we can reduce Sp to 0 and Sa to 0.	consequeces 4.1.4.1.	SEGULA

11 - Appendix D – List of Actions (2/3)

SOCOTEC TECHNICAL CONSULTING

Actions	Place(s) Used	Responsibility
20. Calculate the reaction time and make sure it will be lower than the process time (the time when the PSV will open and then will escalate until it will reach the unwanted event which is liquid unbalanced, potential H2 O2 mixture.)	consequence 4.4.3.1.	SEGULA
21. Investigate the necessity to have a SIF (high high pressure in case if H2/O2 is inside the chilled water system.)	consequence 4.5.1.1.	SEGULA
22. Make sure that H2 will not leak following the pump damaged (To avoid the exploison in case the H2 will be inside the chiller)	consequeces 4.5.4.5. ; 4.7.1.1.	SEGULA
23. Investigate the possibility to havean online conductivity measurment to stop the rectifier	consequence 4.13.1.1.	SEGULA
24. To design the pipe supports in order to withstand the production lines filled with liquid in order to avoid mechanical pipe rupture. Thus, we can reduce Sp to 0 and Sa to 0.	consequeces 5.1.4.1. ; 6.1.3.1. ; 7.1.2.1. ; 8.1.2.1.	SEGULA
25. Calculate the reaction time and make sure it will be lower than the process time (the time when the PSV will open and then will escalate until it will reach the unwanted event which is liquid unbalanced, potential H2 O2 mixture.)	consequeces 5.4.2.1.	SEGULA
26. Investigate the necessity to have a safeguard in case of H2/O2 is inside the chilled water system.	consequence 5.5.1.1.	SEGULA
27. Investigate the consequences on the PDU	consequence 1.2.6.1.	SEGULA
28. Investigate the possibility to add a high high pressure monitoring on the cooling side to close XZV- 14015/XZV-14028	consequence 5.5.3.1.	SEGULA

12 - Appendix E – HAZOP Worksheet (1/12)

Node: 1. ELECTROLYTE CIRCULATION
Drawings / References : MO472-01-PRO-PID-004 Cell Stack ; MO472-01-PRO-PID-012-00 Interconnecting ; MO472-01-PRO-PID-010 Hydrogen Separation ; MO472-01-PRO-014 Oxygen Separation ; MO472-01-PRO-PID-008-00 Electrolyte pump & cooler-Rev00

Deviations	Causes	Consequences	Initial Fi	S p	S e	S a	RRp	RRe	RRa	Safeguards without SIF: Tag	Description	CAT	Risk without SIF: RR F	RR p	RR e	R Ra	Safety Instrumented Functions: Tag	Description	CAT	Actions	Responsibility	Remarks
1. More flow	1. Both pumps are runing together	1.1.1.1. More flow inside the minimum flow line on FCV-08016 which are not designed for flow leading to more pressure below the design pressure, Less flow rate through the pump leading to damage of both pumps.	1.0E-01			2			2			NA				2	FZS-08001	FZI low low flow to stop the pump	SIS - SIL 2			
	1. Control valves FCV- 08016 fails open (control loop failure)	1.1.2.1. More flow to the pump mini flow line and Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-01	3	2	3	3	2	3	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow trip to stop the rectifier	Control (DCS)	10	2	2	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier	SIS - SIL 2			
										TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	High temperature trip to stop the rectifier (not independant from the above)	Control (DCS)	10				TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	Low low flow to stop the rectifier	SIS - SIL 2	1. The safety Temperture transmitter has to be added in the P&ID	SEGULA	
	3. Pump variable speed drive is opareted at the maximum	1.1.3.1																				To be integrated at more pressure deviation scenario
2. No or less flow	1. Control valves FCV- 08016 fails closed (control loop failure)	1.2.1.1. Minimum flow line is used because the flow rate oof the stacks are below the minimum flow rate of the pump. If the control valve fails closed, the remaining flow rate will be below of the minimum flow rate of the pump, the the pump will be damaged	1.0E-01			2			2								FZS-08007 & FZS-08006	FZI low low flow to stop the pump	SIS - SIL 2			
	2. Failure of the pump P- 1001A/B	1.2.2.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-01	3	2	3	3	2	3	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow trip to stop the rectifier	Control (DCS)	10	2	2	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier	SIS - SIL 2	2. To design ventilation system in a way to avoid H2 accumulation due to LOC of the stack consequently avoidin an explosion. In addition to	SEGULA	
										TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	High temperature trip to stop the rectifier (not independant from the above)	Control (DCS)	10				TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	Low low temperature to trip the rectifier	SIS - SIL 2			
	3. Manual valves (pump suction and discharge lines) left closed (operator error during non routine task following written procedure)	1.2.3.1. Less flow to the stacks leading to unsufficient cooling of the stack exceeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-02	3	2	3	3	2	3	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow trip to stop the rectifier	Control (DCS)	10	2	1	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier	SIS - SIL 2			
										TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	High temperature trip to stop the rectifier (not independant from the above)	Control (DCS)	10				TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	Low low temperature to trip the rectifier	SIS - SIL 2			
		1.2.3.2. pressure increase downstream the pump without exceeding the design pressure of the piping (40barg) since the PSV setpoint on the seperators and the pump shut-off pressure were adjusted to meet the design pressure of the piping, equipment is less than the pipe design safety consequences. There is no safeguards to foresee																		3. Check the maximum pump shut off head at maximum speed 3600 RPM	SEGULA	
	4. Clogged strainers	1.2.4.1. Refer to the scenario 1.2.3.1	1.0E-01	3	2	3	3	2	3	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow trip to stop the rectifier	Control (DCS)	10	2	1	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier & the pump		4. Unclogging the mesh from the maintenance service	MCPHY	
											Low flow trip to stop pump											
	5. Check valve stuck closed downstream the pump	1.2.5.1. Refer to the consequences of scenario 1.2.3.1	1.0E-01	3	2	3	3	2	3	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow to stop the rectifier	Control (DCS)	10	2	2	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier & the pump	SIS - SIL 2			
											Low flow trip to stop pump											
	6. Manual valve downstream the heat exchanger left closed (operator error during non routine task following written procedure)	1.2.6.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-02	2	2	2	2	2	2	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow to stop the rectifier	Control (DCS)	10	2	1	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier & the pump	SIS - SIL 2			
										TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	High temperature trip to stop the rectifier (not independant from the above)	NA	1				TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	Low low temperature to stop the rectifier & the pump	SIS - SIL 2			
	7. Clogged filter F-1001	1.2.7.1. Less flow on the pump and more pressure but no consequences	1.0E-02			1			1		Delta Pressure with alarm to clean the filter	NA	1			1						
	8. Manual valves upstream/downstream the filter left closed (operator error during non routine task following written procedure)	1.2.8.1. Refer to the scenario 1.2.7.1								FT-08002	Flow meter with an alarm											
	9. The valve XZV-1001 closes spuriously	1.2.9.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-02	3	2	3	2	2	2	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow to stop the rectifier	Control (DCS)	10	2	1	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier	SIS - SIL 2			
	10. Control valves FCV- 1001A A fail closed (control loop failure)	1.2.10.1. Refer to node 2 scenarios: 2.2.1.1/2.2.1.2																				
		1.2.10.2. Refer to node 3 scenarios: 3.2.1.1/3.2.1.2																				
	11. Manual valve inlet/outlet of the heater left closed during low ambient temperature (operator error during non routine task following written procedure)	1.2.11.1. Heater will turn on by the control loop TIC-1006 leading to the overheating of the heater since there is no electrolyte flow	1.0E-02			3			2			Control (DCS)	10			1	FZS-08005		NA			FZS be shift between blocked valve & heater
		1.2.11.2. Stack operated below 5°C design temperature leading to damage of the stack and potential leakages. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-02	3	2	3	2	2	2	TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014		NA	1	2	2	2	TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	Low low temperature to stop the pumps P-1001A & P-1001B	SIS - SIL 2	5. Confirm the consequences of operting the stack below 5 degres	MCPHY	1. The safeguards in place will avoid the stack leakages but will not avoid the stack damage since the stack will be damaged in low ambient temperature conditions even if it is not in operation
		1.2.11.3 Liquid trapped between both valves and can generate overpressure	1.0E-02	3	2	3	2	2	2								TSV-08002	TSV arround the both valves	SIS - SIL 2			
3. Reverse flow	1. Check valves blocked open	1.3.1.1 Discharge pressure of the pump leading to damage the upstream	1.0E-			3			3		Pump upstream line should have the					1						

12 - Appendix E – HAZOP Worksheet (2/12)

Node: 1. ELECTROLYTE CIRCULATION
Drawings / References : MO472-01-PRO-PID-004 Cell Stack ; MO472-01-PRO-PID-012-00 Interconnecting ; MO472-01-PRO-PID-010 Hydrogen Separation ; MO472-01-PRO-PID-014 Oxygen Separation ; MO472-01-PRO-PID-008-00 Electrolyte pump & cooler-Rev00

Deviations	Causes	Consequences	Initial Fi	Sp	Se	Sa	RRp	RRe	RRa	Safeguards without SIF: Tag	Description	CAT	RRF	Risk without SIF: RRp	RRe	RRa	Safety Instrumented Functions: Tag	Description	CAT	Actions	Responsibility	Remarks
1. More flow	1. Both pumps are runing together	1.1.1.1. More flow inside the minimum flow line on FCV-08016 which are not designed for flow leading to more pressure below the design pressure, Less flow rate through the pump leading to damage of both pumps.	1.0E-01			2			2			NA				2	FZS-08001	FZI low low flow to stop the pump	SIS - SIL 2			
	1. Control valves FCV- 08016 fails open (control loop failure)	1.1.2.1. More flow to the pump mini flow line and Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-01	3	2	3	3	2	3	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow trip to stop the rectifier	Control (DCS)	10	2	2	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier	SIS - SIL 2			
										TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	High temperature trip to stop the rectifier (not independant from the above)	Control (DCS)	10				TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	Low low flow to stop the rectifier	SIS - SIL 2	1. The safety Temperture transmitter has to be added in the P&ID	SEGULA	
	3. Pump variable speed drive is opareted at the maximum	1.1.3.1																				To be integrated at more pressure deviation scenario
2. No or less flow	1. Control valves FCV- 08016 fails closed (control loop failure)	1.2.1.1. Minimum flow line is used because the flow rate oof the stacks are below the minimum flow rate of the pump. If the control valve fails closed, the remaining flow rate will be below of the minimum flow rate of the pump, the the pump will be damaged	1.0E-01			2			2								FZS-08007 & FZS-08006	FZI low low flow to stop the pump	SIS - SIL 2			
	2. Failure of the pump P- 1001A/B	1.2.2.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-01	3	2	3	3	2	3	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow trip to stop the rectifier	Control (DCS)	10	2	2	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier	SIS - SIL 2	2. To design ventilation system in a way to avoid H2 accumulation due to LOC of the stack consequently avoidin an exploison. In addition to	SEGULA	
										TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	High temperature trip to stop the rectifier (not independant from the above)	Control (DCS)	10				TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	Low low temperature to trip the rectifier	SIS - SIL 2			
	3. Manual valves (pump suction and discharge lines) left closed (operator error during non routine task following written procedure)	1.2.3.1. Less flow to the stacks leading to unsufficient cooling of the stack exceeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-02	3	2	3	3	2	3	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow trip to stop the rectifier	Control (DCS)	10	2	1	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier	SIS - SIL 2			
										TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	High temperature trip to stop the rectifier (not independant from the above)	Control (DCS)	10				TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	Low low temperature to trip the rectifier	SIS - SIL 2			
		1.2.3.2. pressure increase downstream the pump without exceeding the design pressure of the piping (40barg) since the PSV setpoint on the seperators and the pump shut-off pressure were adjusted to meet the design pressure of the piping, equipment is less than the pipe design safety consequences. There is no safeguards to foresee																		3. Check the maximum pump shut off head at maximum speed 3600 RPM	SEGULA	
	4. Clogged strainers	1.2.4.1. Refer to the scenario 1.2.3.1	1.0E-01	3	2	3	3	2	3	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow trip to stop the rectifier	Control (DCS)	10	2	1	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier & the pump		4. Unclogging the mesh from the maintenance service	MCPHY	
											Low flow trip to stop pump											
	5. Check valve stuck closed downstream the pump	1.2.5.1. Refer to the consequences of scenario 1.2.3.1	1.0E-01	3	2	3	3	2	3	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow to stop the rectifier	Control (DCS)	10	2	2	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier & the pump	SIS - SIL 2			
											Low flow trip to stop pump											
	6. Manual valve downstream the heat exchanger left closed (operator error during non routine task following written procedure)	1.2.6.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-02	2	2	2	2	2	2	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow to stop the rectifier	Control (DCS)	10	2	1	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier & the pump	SIS - SIL 2			
										TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014	High temperature trip to stop the rectifier (not independant from the above)	NA	1				TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	Low low temperature to stop the rectifier & the pump	SIS - SIL 2			
	7. Clogged filter F-1001	1.2.7.1. Less flow on the pump and more pressure but no consequences	1.0E-02			1			1		Delta Pressure with alarm to clean the filter	NA	1			1						
	8. Manual valves upstream/downstream the filter left closed (operator error during non routine task following written procedure)	1.2.8.1. Refer to the scenario 1.2.7.1								FT-08002	Flow meter with an alarm											
	9. The valve XZV-1001 closes spuriously	1.2.9.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-02	3	2	3	2	2	2	FT-04001 & FT-04003 & FT-04005 & FT-04007	Low flow to stop the rectifier	Control (DCS)	10	2	1	2	FZS-04002 & FZS-04004 & FZS-04006 & FZS-04008	Low low flow to stop the rectifier	SIS - SIL 2			
	10. Control valves FCV- 1001A A fail closed (control loop failure)	1.2.10.1. Refer to node 2 scenarios: 2.2.1.1/2.2.1.2																				
		1.2.10.2. Refer to node 3 scenarios: 3.2.1.1/3.2.1.2																				
	11. Manual valve inlet/outlet of the heater left closed during low ambient temperature (operator error during non routine task following written procedure)	1.2.11.1. Heater will turn on by the control loop TIC-1006 leading to the overheating of the heater since there is no electrolyte flow	1.0E-02			3			2			Control (DCS)	10			1	FZS-08005		NA			FZS be shift between blocked valve & heater
		1.2.11.2. Stack operated below 5°C design temperature leading to damage of the stack and potential leakages. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-02	3	2	3	2	2	2	TT-04009 & TT-04010 & TT-04011 & TT-04012 & TT-04013 & TT-04014		NA	1	2	2	2	TZS-04015 & TZS-04016 & TZS-04017 & TZS-04018 & TZS-04019 & TZS-04020	Low low temperature to stop the pumps P-1001A & P-1001B	SIS - SIL 2	5. Confirm the consequences of operting the stack below 5 degres	MCPHY	1. The safeguards in place will avoid the stack leakages but will not avoid the stack damage since the stack will be damaged in low ambient temperature conditions even if it is not in operation
		1.2.11.3 Liquid trapped between both valves and can generate overpressure	1.0E-02	3	2	3	2	2	2								TSV-08002	TSV arround the both valves	SIS - SIL 2			
3. Reverse flow	1. Check valves blocked open	1.3.1.1 Discharge pressure of the pump leading to damage the upstream	1.0E-			3			3		Pump upstream line should have the					1						

12 - Appendix E – HAZOP Worksheet (3/12

Drawings / References: MO472-01-PRO-PID-004 Cell Stack ; MO472-01-PRO-PID-012-00 Interconnecting ; MO472-01-PRO-PID-010 Hydrogen Separation

Deviations	Causes	Consequences	Initial Risk: Fi	People Sp	Enviro Se	Asset Sa	RRp	RRe	RRa	Safeguards without SIF: Tag	Description	CAT	RRF	Risk without SIF: RRp	RRe	RRa	Safety Instrumented Functions: Tag	Description	CAT	Actions: Actions	Responsibility	Remarks
1. More flow	1. Control valve FCV-04024 & FCV-04029 fails fully open	2.1.1.1. More catholyte flow to the stack leading to loss of efficency	1.0E-01			1			1	FT-04005 & FT-04007 TT-04011 & TT-04012 & TT-04014	High flowrate Low delta T between both inlet / outlet to stop the rectifier	Control (DCS)	10			1			NA		Responsibility	
	2. Refer to node 1 deviation more flow scenarios : 1.1.1.1 and 1.1.1.2	2.1.2.1.								FT-04005 & FT-04007	Low flow trip to stop the rectifier											
	3. Refer to node 2 deviation more current scenario 2.15.1.1	2.1.3.1.								TT-04011 & TT-04012 & TT-04014	High temperature trip to stop the rectifier (not independant from the cause)						TZS-04017 & TZS-04018 & TZS-04020	High high temperature to stop the rectifier (not independent from the above)		12. The safety Temperture transmitter has to be added in the P&ID	SEGULA	
	3. Pump variable speed drive is opareted at the maximum	2.1.3.1 refer to (node 1) 1.1.3.1																				To be integrated at mire pressure deviation scenario
2. No or less flow	1. Control valve FCV-04024 & FCV-04029 fails closed	2.2.1.1. Pressure build up upstream the control valve without safety consequences because the piping is designed for the maximum pump head pressure.																				
		2.2.1.2. Less flow to the stacks leading to unsufficient cooling of the stack exceeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.		3	2	3	3	2	3	FT-04005 & FT-04007	Low flow to stop the rectifier (not independant from the cause)	Control (DCS)	1	2	1	2	FZS-04006 & FZS-04008	Low low flow to stop the rectifier	SIS - SIL 2			
										TT-04011 & TT-04012 & TT-04014	High temperature trip to stop the rectifier (not independant from the cause)	Control (DCS)	1				TZS-04017 & TZS-04018 & TZS-04020	High high temperature to stop the rectifier	SIS - SIL 2			
	2. Manual valves upstream the stack left closed	2.2.2.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure	1.0E-02	3	2	3	2	2	2	FT-04005 & FT-04007	Low flow to stop the rectifier and interlock the sequences	Control (DCS)	10	1	1	2	FZS-04006 & FZS-04008	Low low flow to stop the rectifier	SIS - SIL 2			
										TT-04011 & TT-04012 & TT-04014	High temperature trip to stop the rectifier (not independant from the cause)	NA	1				TZS-04017 & TZS-04018 & TZS-04020	High high temperature to stop the rectifier				
	3. Refere to node 1 no or less flow scenarios:1.2.2.1/1.2.3.1/1.2.4.1/1.2. 5.1/1.2.8.1/1. 2.9.1	2.2.3.1																				
3. Reverse flow	No causes identified																					
4. Misdirected flow	1.	2.4.1.1																		13. Issues regarding the interlocking	SEGULA/MCPHY	
	2.	2.4.1.2																		14. Issue regarding the flexible hoses connection	SEGULA/MCPHY	
5. More temperature	1. Refer to node 1 scenarios : 1.1.2.1/1.2.2.1/1.2.3.1/1.2.4.1/1.2.5.1/1.2.6.1/1.2.7.1/1.2.8.1/1.2.9.1/1.210.1/1.5.1.1/1.5.2.1/1.5.3.1/1.5.4.1/1.6.1.1/1.14.1.2	2.5.1.1.																				
	2. Refer to node 2 scenarios: 2.2.1.2/2.2.2.1/2.3.1.1	2.5.2.1.																				
6. Less temperature	1. Refer to node 1 scenarios: 1.2.11.2/1.6.1.1/1.6.2.1	2.6.1.1.																				
7. More pressure	1. No causes identified																					
8. Less pressure or vacuum	1. No causes identified																					
9. High liquid level	1. No causes identified																					
10. Low or no liquid level	1. No causes identiifed																					
11. Change in composition	1. No causes identifed																					
12. Change in KOH concentration	1. Refer to node 1 scenario 1.12.1.1																					
	2. Refer to node 4 scenarios: 4.1.4.1/4.2.2.1/4.2.3.1	1.2.11.2.																				
13. Startup, maintenance and shutdown	1. No causes identified																					
14. Loss of utilities	1. Loss of instrument air	2.14.1.1. FCV-04024 & FCV-04029 fail in open position. Refer to scenario 2.1.1.1, 2.4.1.1																				
15. More current/voltage	1. Failure of DC current limiter in the rectifier	2.15.1.1. 10% more current than expected. More production than expected without overpressure inside the separators since the outlet	1.0E-01			2			2	PSV- 10002 CZS-04021 CZS-04021	PSV on the separators with 132% pressure High current detection to stop the rectifier Protection against overcurrent from	PSV Control (DCS) Control	100 10 10			1	CZS-04022	High high current detection to stop the rectifier	SIS - SIL 2	15. To identify the worse case Control de Max current of the	SEGULA	
16. Less current/voltage	1. Less current than the minimum turndown rate (20% per stack)	2.16.1.1. Improper gas quality O2 into H2 / H2 into O2 leading to potential explosion inside separators	1.0E-01	5	3	5	5	3	5	AT-10011	Alarm in case of High OTH/HTO for operator action	Alarm (DCS)	10	3	2	3	CZS-04022	IIC Low Low current detection with a timer delay (3 mins) to stop the rectifier	SIS - SIL 2	16. To confirm with rectifier's supplier to stop it automatically in case of low current detection	SEGULA	
										CZS-04021	Low current detection to stop the rectifier automtically	Control (DCS)	10							17. The distance has to be studied in HAZAN scenarii to reduce the severity. To check with the supplier what can be the reason behind this low current to see if if we have to reduce the frenquency	SEGULA	
17. Other	1. No causes identified																					

12 - Appendix E – HAZOP Worksheet (4/12)

Node: 2.1. Network (H2 / KOH) / Half production (2/4 of 1 MW stacks)
Drawings / References: MO472-01-PRO-PID-004 Cell Stack ; MO472-01-PRO-PID-012-00 Interconnecting ; MO472-01-PRO-PID-010 Hydrogen Separation

Deviations	Causes	Consequences	Initial Risk							Safeguards without SIF				Risk without SIF			Safety Instrumented Functions			Actions		Remarks
			Fi	S p (People)	S e (Enviro)	S a (Asset)	RRp	RRe	RRa	Tag	Description	CAT	RR F	RR p	RR e	R Ra	Tag	Description	CAT	Actions	Responsibility	
1. More flow	1. Control valve FCV-04024 fails fully open	2-1.1.1.1. More catholyte flow to the stack leading to loss of efficency	1.0E-01			1			1										NA			
1. More flow	2. Control valve FCV-04029 fails fully open	2-1.1.2.1. More catholyte flow to the stack leading	1.0E-01			1			1	FT-04005 TT-04011	High flowrate Low delta T between both inlet / outlet	Control (DCS)	10			1			NA	18. Check the pressure drop btween stacks 5/6 on H2 side and H2 separator	SEGULA	
1. More flow	3. Refer to node 1 deviation more flow scenarios : 1.1.1.1 and 1.1.1.2	2-1.1.3.1.									Low flow trip to stop the rectifier											
1. More flow	4. Refer to node 2 deviation more current scenario 2.15.1.1	2-1.1.4.1.								TT-04011	High temperature trip to stop the rectifier (not independant from the cause)	Control (DCS)	1				TZS-04017	High high temperature to stop the rectifier (not independent from the above)	SIS - SIL 2	12. The safety Temperture transmitter has to be added in the P&ID	SEGULA	
2. No or less flow	1. Control valve FCV-04024 fails closed	2-1.2.1.1. Pressure build up upstream the control valve without safety consequences because the piping is designed for the maximum pump head pressure.																				
2. No or less flow	1. Control valve FCV-04024 fails closed	2-1.2.1.2. Less flow to the stacks leading to unsufficient cooling of the stack exceeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.		3	2	3	3	2	3	FT-04005	Low flow to stop the rectifier (not independant from the cause)	Control (DCS)	1	2	1	2	FZS-04006	Low low flow to stop the rectifier	SIS - SIL 2			
2. No or less flow										TT-04011	High temperature trip to stop the rectifier (not independant from the cause)	Control (DCS)	1				TZS-04017	High high temperature to stop the rectifier	SIS - SIL 2			
2. No or less flow	2. Manual valve upstream the stack left closed	2-1.2.2.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure	1.0E-02	3	2	3	2	2	2	FT-04005	Low flow to stop the rectifier and interlock the sequences	Control (DCS)	10	2	1	2	FZS-04006	Low low flow to stop the rectifier	SIS - SIL 2			
2. No or less flow										TT-04011	High temperature trip to stop the rectifier (not independant from the cause)	Control (DCS)	1				TZS-04017	High high temperature to stop the rectifier	SIS - SIL 2			
2. No or less flow	3. Refere to node 1 no or less flow scenarios:1.2.2.1/1.2.3.1/1.2.4.1/1.2. 5.1/1.2.8.1/1. 2.9.1	2-1.2.3.1.																				
3. Reverse flow	No causes identified																					
4. Misdirected flow	1. Refer to node 2 scenarios: 2.4.1.1	2-1.4.1.1																				
4. Misdirected flow	2. Refer to node 2 scenarios: 2.4.1.2	2-1.4.1.2																				
5. More temperature	1. Refer to node 1 scenarios : 1.1.2.1/1.2.2.1/1.2.3.1/1.2.4.1/1.2.5.1/1.2.6.1/1.2.7.1/1.2.8.1/1.2.9.1/1.210.1/1.5.1.1/1.5.2.1/1.5.3.1/1.5.4.1/1.6.1.1/1.14.1.2	2-1.5.1.1.																				
5. More temperature	2. Refer to node 2 scenarios: 2.2.1.2/2.2.2.1/2.3.1.1	2-1.5.2.1.																				
6. Less temperature	1. Refer to node 1 scenarios: 1.2.11.2/1.6.1.1/1.6.2.1	2-1.6.1.1.																				
7. More pressure	1. No causes identified																					
8. Less pressure or vacuum	1. No causes identified																					
9. High liquid level	1. No causes identified																					
10. Low or no liquid level	1. No causes identiifed																					
11. Change in composition	1. No causes identifed																					
12. Change in KOH concentration	1. Refer to node 1 scenario 1.12.1.1	2-1.12.1.1																				
12. Change in KOH concentration	2. Refer to node 4 scenarios: 4.1.4.1/4.2.2.1/4.2.3.1	2-1.2.12.2. Stack operated below 5°C design temperature leading to damage of the stack and potential leakages. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.																				
13. Startup,	1. No causes identified																					
14. Loss of utilities	1. Loss of instrument air	2-1.14.1.1. FCV-04024 & FCV-04029 fail in open position. Refer to scenario 2.1.1.1, 2.4.1.1																				
15. More current/voltage	1. Failure of DC current limiter in the rectifier	2-1.15.1.1. 10% more current than expected. More production than expected without overpressure inside the separators since the outlet	1.0E-01			2			2	PSV- 10002 CZS-04021 CZS-04021	PSV on the separators with 132% pressure High current detection to stop the rectifier Protection against overcurrent from	PSV Control (DCS) Control (DCS)	100 10 10			1	CZS-04022	High high current detection to stop the rectifier	SIS - SIL 2	15. To identify the worse case Control de Max current of the	SEGULA	
16. Less current/voltage	1. Less current than the minimum turndown rate (20% per stack)	2-1.16.1.1. Improper gas quality O2 into H2 / H2 into O2 leading to potential explosion inside separators	1.0E-01	5	3	5	5	3	5	AT-10011	Alarm in case of High OTH/HTO for operator action	Alarm (DCS)	10	3	2	3	CZS-04022	IIC Low Low current detection with a timer delay (3 mins) to stop the rectifier	SIS - SIL 2	16. To confirm with rectifier's supplier to stop it automatically in case of low current detection	SEGULA	
16. Less current/voltage										CZS-04021	Low current detection to stop the rectifier automtically	Control (DCS)	10							17. The distance has to be studied in HAZAN scenarii to reduce the severity. To check with the supplier what can be the reason behind this low current to see if if we have to reduce the frenquency	SEGULA	
17. Other	1. No causes identified																					

Conseil et assistance

12 - Appendix E – HAZOP Worksheet (5/12)

Node: 3. Network (O2/KOH)
Drawings / References: MO472-01-PRO-PID-004 Cell Stack ; MO472-01-PRO-PID-012-00 Interconnecting ; MO472-01-PRO-PID-014 Oxygen Separation

Deviations	Causes	Consequences	Initial Risk							Safeguards without SIF				Risk without SIF			Safety Instrumented Functions			Actions		Remarks
			Fi	People Sp	Environm Se	Asset Sa	RRp	RRe	RRa	Tag	Description	CAT	RRF	RRp	RRe	RRa	Tag	Description	CAT	Actions	Responsibility	
1. More flow	1. Control valve FCV-04014 & FCV-04019 fails fully open	3.1.1.1. More anolyte flow to the stack leading to loss of efficency	1.0E-01			2			2	FT-04001 & FT-04003 TT-04009 & TT-04010 & TT-04013	High flowrate Low delta T between both inlet / outlet to stop the rectifier	Control (DCS)	10			1			NA		Responsibility	
	2. Refer to node 1 deviation more flow scenarios : 1.1.1.1 and 1.1.1.2	3.1.2.1.																				
	3. Refer to node 2 deviation more current scenario 2.15.1.1	3.1.3.1.																	SIS - SIL 2	12. The safety Temperture transmitter has to be added in the P&ID	SEGULA	
	4. Pump variable speed drive is opareted at the maximum	1.1.4.1 refer to (node 1) 1.1.3.1																				To be integrated at more pressure deviation scenario
2. No or less flow	1. Control valve FCV-04014 & FCV-04019 fails closed	3.2.1.1. Pressure build up upstream the control valve without safety consequences because the piping is designed for the maximum pump head pressure																				
		3.2.1.2. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure.	1.0E-01	3	2	3	3	2	3	?	High delta T between both TT to stop the rectifier	Control (DCS)	10	2	2	2	TZI-1001A	High high temperature to stop the rectifier	SIS - SIL 2			
										FT-04001 & FT-04003	Low flow to stop the rectifier (not independant from the cause)	NA	1				FZS-04002 & FZS-04004	Low low flow to stop the rectifier	SIS - SIL 2			
										TT-04009 & TT-04010 & TT-04013	High temperature trip to stop the rectifier (not independant from the cause)	NA	1				TZS-04015 & TZS-04016 & TZS-04019	High high temperature to stop the rectifier	SIS - SIL 2			
	2. Manual valves upstream the cluster left closed	3.2.2.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure.	1.0E-02	3	2	3	2	2	2	FT-04001 & FT-04003	Low flow to stop the rectifier and shutdown the pump	Control (DCS)	10	2	1	2	FZS-04002 & FZS-04004	Low low flow to stop the rectifier	SIS - SIL 2			
										TT-04009 & TT-04010 & TT-04013	High temperature trip to stop the rectifier (not independant from the cause)	NA	1				TZS-04015 & TZS-04016 & TZS-04019	High high temperature to stop the rectifier	SIS - SIL 2			
	3. Refere to node 1 no or less flow scenarios:1.2.2.1/1.2.3.1/1.2.4.1/1.2. 5.1/1.2.8.1/1. 2.9.1	3.3.3.1.																				
3. Reverse flow	No causes identified																					
4. Misdirected flow																						
5. More temperature	1. Refer to node 1 scenarios : 1.1.2.1/1.2.2.1/1.2.3.1/1.2.4.1/1.2.5.1/1.2.6.1/1.2.7.1/1.2.8.1/1.2.9.1/1.210.1/1.5.1.1/1.5.2.1/1.5.3.1/1.5.4.1/1.6.1.1/1.14.1.2	3.5.1.1.																				
	2. Refer to node 3 scenarios: 3.2.1.2/3.2.2.1/3.3.1.1	3.5.2.1.																				
6. Less temperature	1. Refer to node 1 scenarios: 1.2.11.2/1.6.1.1/1.6.2.1	3.6.1.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.																				
7. More pressure	1. No causes identified																					
8. Less pressure or vacuum	1. No causes identified																					
9. High liquid level	1. No causes identified																					
10. Low or no liquid level	1. No causes identiifed																					
11. Change in composition	1. No causes identiifed	3.11.1.1. Stack operated below 5°C design temperature leading to damage of the stack and potential leakages. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.																				
12. Change in KOH concentration	1. Refer to node 1 scenario 1.12.1.1	3.12.1.1.																				
	2. Refer to node 4 scenarios: 4.1.4.1/4.2.2.1/4.2.3.1	3.12.2.1. Stack operated below 5°C design temperature leading to damage of the stack and potential leakages. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.																				
13. Startup, maintenan ce and shutdown	1. No causes identified																					
14. Loss of utilities	1. Loss of instrument air	3.14.1.1. FCV-04024 & FCV-04029 fail in open position. Refer to scenario 2.1.1.1, 2.4.1.1																				
15. More current/vol tage	1. Failure of DC current limiter in the rectifier	3.15.1.1. 10% more current than expected. More production than expected without overpressure inside the separators since the outlet	1.0E-01			2			2	PSV-14002	PSV on the separators with 132% pressure	PSV	100			1	CZS-04022	High high current detection to stop the rectifier	SIS - SIL 2	15. To identify the worse case Control de Max current of the	SEGULA	
										CZS-04021	High current detection to stop the rectifier	Control (DCS)	10									
										CZS-04021	Protection against overcurrent from the primary current of the transformer to trip the MV breaker	Control (DCS)	10									
16. Less current/vol tage	1. Less current than the minimum turndown rate (20% per stack)	3.16.1.1. Improper gas quality O2 into H2 / H2 into O2 leading to potential explosion inside separators	1.0E-01	5	3	5	5	3	5	AT-10010	Alarm in case of High OTH/HTO for operator action	Alarm (DCS)	10	3	2	3	CZS-04022	IIC Low Low current detection with a timer delay (3 mins) to stop the rectifier	SIS - SIL 2	16. To confirm with rectifier's supplier to stop it automatically in case of low current detection	SEGULA	
										CZS-04021	Low current detection to stop the rectifier automtically	Control (DCS)	10							17. The distance has to be studied in HAZAN scenarii to reduce the severity. To check with the supplier what can be the reason behind this low current to see if if we have to reduce the frenquency	SEGULA	
17. Other	1. No causes identified																					

12 - Appendix E – HAZOP Worksheet (6/12)

SOCOTEC TECHNICAL CONSULTING

Node: 3.1. Network (O2 / KOH) / Half production (2/4 of 1 MW stacks) U1003/4 operating and U1005/6 shutdown
Drawings / References: MO472-01-PRO-PID-004 Cell Stack ; MO472-01-PRO-PID-012-00 Interconnecting ; MO472-01-PRO-PID-014 Oxygen Separation

Deviations	Causes	Consequences	Initial Risk: Fi	People: S p	Enviro: S e	Asset: S a	RRp	RRe	RRa	Safeguards without SIF: Tag	Description	CAT	RR F	Risk without SIF: RR p	RR e	R Ra	Safety Instrumented Functions: Tag	Description	CAT	Actions: Actions	Responsibility	Remarks
1. More flow	1. Control valve FCV-04014 fails fully open	2-1.1.1.1. More catholyte flow to the stack leading to loss of efficency	1.0E-01			1			1										NA			
	2. Control valve FCV-04019 fails fully open	3-1.1.2.1. More catholyte flow to the stack leading	1.0E-01			1			1	FT-04001 TT-04009	High flowrate Low delta T between both inlet / outlet	Control (DCS)	10			1			NA			
	3. Refer to node 1 deviation more flow scenarios : 1.1.1.1 and 1.1.1.2	3-1.1.3.1									Low flow trip to stop the rectifier											
	4. Refer to node 2 deviation more current scenario 2.15.1.1	3-1.1.4.1								TT-04009	High temperature trip to stop the rectifier (not independant from the cause)						TZS-04015	High high temperature to stop the rectifier (not independent from the above)	SIS - SIL 2	12. The safety Temperture transmitter has to be added in the P&ID	SEGULA	
2. No or less flow	1. Control valve FCV-04024 fails closed	3-1.2.1.1. Pressure build up upstream the control valve without safety consequences because the piping is designed for the maximum pump head pressure.																				
		3-1.2.1.2. Less flow to the stacks leading to unsufficient cooling of the stack exceeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.		3	2	3	3	2	3	FT-04001	Low flow to stop the rectifier (not independant from the cause)	Control (DCS)	1	2	1	2	FZS-04002	Low low flow to stop the rectifier	SIS - SIL 2			
										TT-04009	High temperature trip to stop the rectifier (not independant from the cause)	Control (DCS)	1				TZS-04015	High high temperature to stop the rectifier	SIS - SIL 2			
	2. Manual valve upstream the stack left closed	3-1.2.2.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure	1.0E-02	3	2	3	2	2	2	FT-04001	Low flow to stop the rectifier and interlock the sequences	Control (DCS)	10	2	1	2	FZS-04002	Low low flow to stop the rectifier	SIS - SIL 2			
										TT-04009	High temperature trip to stop the rectifier (not independant from the cause)	Control (DCS)	1				TZS-04015	High high temperature to stop the rectifier	SIS - SIL 2			
	3. Refere to node 1 no or less flow scenarios:1.2.2.1/1.2.3.1/1.2.4.1/1.2. 5.1/1.2.8.1/1. 2.9.1	3-1.2.1.1.																				
3. Reverse flow	No causes identified																					
4. Misdirected flow		3-1.4.1.1.																				
		3-1.4.2.1.																				
5. More temperature	1. Refer to node 1 scenarios : 1.1.2.1/1.2.2.1/1.2.3.1/1.2.4.1/1.2.5.1/1.2.6.1/1.2.7.1/1.2.8.1/1.2.9.1/1.210.1/1.5.1.1/1.5.2.1/1.5.3.1/1.5.4.1/1.6.1.1/1.14.1.2	3-1.5.1.1.																				
	2. Refer to node 2 scenarios: 2.2.1.2/2.2.2.1/2.3.1.1	3-1.5.2.1.																				
6. Less	1. Refer to node 1 scenarios: 1.2.11.2/1.6.1	3-1.6.1.1.																				
7. More pressure	1. No causes identified																					
8. Less pressure or vacuum	1. No causes identified																					
9. High liquid level	1. No causes identified																					
10. Low or no liquid level	1. No causes identiifed																					
11. Change in composition	1. No causes identifed																					
12. Change in KOH concentration	1. Refer to node 1 scenario 1.12.1.1	3-1.6.1.1.																				
	2. Refer to node 4 scenarios: 4.1.4.1/4.2.2.1/4.2.3.1	3-1.6.2.1. Stack operated below 5°C design temperature leading to damage of the stack and potential leakages. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.																				
13. Startup, maintenance and shutdown	1. No causes identified																					
14. Loss of utilities	1. Loss of instrument air	3-1.14.1.1. FCV-04024 & FCV-04029 fail in open position. Refer to scenario 2.1.1.1, 2.4.1.1																				
15. More current/voltage	1. Failure of DC current limiter in the rectifier	3-1.15.1.1. 10% more current than expected. More production than expected without overpressure inside the separators since the outlet valves are designed to evacuate the additional production. No safety	1.0E-01			2			2	PSV- 14002	PSV on the separators with 132% pressure	PSV	100			1	CZS-04022	High high current detection to stop the rectifier	SIS - SIL 2	15. To identify the worse case Control de Max current of the rectifier if the protection is lost	SEGULA	
										CZS-04021	High current detection to stop the rectifier	Control (DCS)	10									
										CZS-04021	Protection against overcurrent from	Control	10									
16. Less current/voltage	1. Less current than the minimum turndown rate (20% per stack)	3-1.16.1.1. Improper gas quality O2 into H2 / H2 into O2 leading to potential explosion inside separators	1.0E-01	5	3	5	5	3	5	AT-10010	Alarm in case of High OTH/HTO for operator action	Alarm (DCS)	10	3	2	3	CZS-04022	IIC Low Low current detection with a timer delay (3 mins) to stop the rectifier	SIS - SIL 2	16. To confirm with rectifier's supplier to stop it automatically in case of low current detection	SEGULA	
										CZS-04021	Low current detection to stop the rectifier automtically	Control (DCS)	10							17. The distance has to be studied in HAZAN scenarii to reduce the severity. To check with the supplier what can be the reason behind this low current to see if if we have to reduce the frenquency	SEGULA	
17. Other	1. No causes identified																					

12 - Appendix E – HAZOP Worksheet (7/)

Node: 4. LYE HYDROGEN SEPARATION
Drawings / References: MO472-01-PRO-PID-012-00 Interconnecting ; MO472-01-PRO-PID-010 Hydrogen Separation

Deviations	Causes	Consequences	Initial Risk: Fi	People Sp	Environment Se	Asset Sa	RRp	RRe	RRa	Safeguards without SIF: Tag	Description	CAT	RR F	Risk without SIF: RR p	RR e	R Ra	Safety Instrumented Functions: Tag	Description	CAT	Actions: Actions	Responsibility	Remarks
1. More flow	1. Refer to node 2 scenario: 2.1.1.1	4.1.1.1.																				
	2. Refer to node 1 deviation more flow scenarios : 1.1.1.1 and 1.1.1.2	4.1.2.1.																				
	3. Refer to node 2 deviation more current scenario 2.15.1.1	4.1.3.1.																				
	4. Control valve LCV-10032 fails open (control loop failure)	4.1.4.1. More ultra pure demin water flow inside the separator leading to high level in both separators (due to the balancing line). Liquid flow in the gas production lines OSBL leading to pipe rupture, loss of containment and potential jet fire.	1.0E-01	3	2	3	3	2	3	LT- 10006/LT-10004 LIC-10032	High level to stop the rectifier High level to stop the rectifier (not independant from the cause)	Control (DCS) NA	10 1	2	2	2	LZT-10007/8 & LZT-14007/8	High high level trip to isolate the demin water feeding line (to close XZV-10031)	SIS - SIL 2	19. To design the pipe supports in order to withstand the production lines filled with liquid in order to avoid mechanical pipe rupture. Thus, we can reduce Sp to 0 and Sa to 0.	SEGULA	
	5. Refer to scenarios 4.8.1.1/4.8.2.1	4.1.5.1.																				
2. No or less flow	1. Refer to scenarios 4.7.1.1/4.7.2.1	4.2.1.1.																				
	2. Control valve LCV-10032 fails closed	4.2.2.1. Consumption of water from the electrolyte solution continues. Gradual increase of concentration of KOH leading to higher viscosity and	1.0E-01	3	2	3	3	2	3	LT- 10006/LT-14006 LIC-10032	Low level to stop the rectifier Low level to stop the rectifier (not	Control (DCS) NA	10 1	2	2	2	LZT-10007/8 (H2) & LZT-	Low low level trip to stop the rectifier	SIS - SIL 2			
	3. Clogged strainers refer to node 1 scenario 1.2.3.1	4.2.3.1.																				
	4. The valve XZV-10023 closes spuriously	4.2.4.1. PCV-10017 will evacuate the total production without safety consequences.																				
	5. No ultra pure demin water flow from OSBL	4.2.5.1. Refer to the scenario 4.2.2.1																				
	6. The pump P-1040 failure from the ultra pure demin water supply	4.2.6.1. Refer to the scenario 4.2.2.1																				
	7. Check valve on the nitrogen feeding line stuck closed	4.2.7.1. Purging with nitrogen is not possible, resulting in delays to change of stuck.	1.0E-01			1			2			NA	1			2			NA			1. The production cannot start if pressure cycles during purging are not accomplished
3. Reverse flow	1. Control valve PCV-10020 fails open when the system is in low pressure mode (startup,standby,stop)	4.3.1.1. There is no KOH flow in standby, and stop mode . Blow by from PDU system to H2 separator. The low low trip pressure is inhibited								PSV-10002	Pressure safety valve setpoint is 33Barg. PDU is at 27 Barg will never reach 33 Barg, that means the PSV will not open											
	2. Check valve NRV-10008 on the nitrogen feeding separtor opened	4.3.2.1. XZV-10007 is already open during H2 purging. A contamination with H2 in N2 distribution	1.0E-01			2			2	PT-13001	Low pressure alaram in the N2 distribution	Control (DCS)	1			1			NA			
4. Misdirected flow	1. The depressurization valve XZV-10004 opens spuriously	4.4.1.1. Pressure release inside the separator leading to level unbalance between both separators. O2 H2 mixture inside hydrogen separator, due to the balanicng line, leading to explosion inside the separator.	1.0E-02	5	3	5	3	3	3	PDIC- 10010	High differential pressure to open production line on oxygen side (to open PCV-14017)	Control (DCS)	10	3	2	3	LZI-10007/8 LZI-14007/8	High high level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045) Low low level to isolate the oxygen	SIS - SIL 2 SIS -			
	2. The valve XZV-10007opens spuriously	4.4.2.1. Refer to scenario 4.3.2.1				2			2	PT-13001	High pressure alarm in N2 distribution	Control (DCS)	1			1			NA			
	3. The valve PSV-10002	4.4.3.1. Less flow to the stacks leading to unsufficient cooling of the stack exeeding the design temperature. Degradation of the membrane and cell frame failure.	1.0E-04	2	1	2	2	1	2			NA	1	2	1	2	LZI-10007/8 LZI-14007/8	High high level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045) Low low level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2 SIS - SIL 2	20. Calculate the reaction time and make sure it will be lower than the process time I the time when the PSV	SEGULA	
5. More temperature	1. Tube rupture in gas cooler E-1001	4.5.1.1. H2 leakage in chilled water network without overpressure since the heat exchanger is designed according to 10/13 API521 rule. Chilled water contaminated with H2 gas.	1.0E-02	3		3	3		3			NA	1	3		3			NA	21. Investigate the necessity to have a SIF (high high pressure in case if H2/O2 is inside the chilled water system.)	SEGULA	
	2. Control valve TCV-10028 fails closed (control loop failure)	4.5.2.1. No more chilled water to cool down the hydrogen gas leading to	1.0E-01			2			2	TIC-10012	High temperature to stop the	NA	1			2	TZT-10018	High high trip temperature to stop the rectifier	SIS -			
	3. The valves XZV-10015/XZV-10030 close spuriously	4.5.3.1. No more chilled water to cool down the hydrogen gas leading to high gas temperature to PDU. Potential damage of the PDU.	1.0E-01			2			2	TIC-10012	High temperature to stop the rectifier	Control (DCS)	10			2	TZT-10018	High high trip temperature to stop the rectifier	SIS - SIL 2			
	4. No chilled water from upstream	4.5.4.1. Refer to scenario 4.5.3.1																				
	5.Leak of the chiller exchanger towards the chill water system	4.5.4.5 H2 inside the closed-loop circulation and pump cavitation																		22. Make sure that H2 will not leak following the pump damaged (To avoid the exploison in case the H2 will be inside the chiller)	SEGULA	
6. Less temperature	1. Control valve TCV-10028 fails open (control loop failure)	4.6.1.1. Overcooling of the hydrogen gas without safety consequenses																				
7. More pressure	1. Control valve PCV-10020 fails closed (control loop failure) while PCV-10017 is closed	4.7.1.1. PCV-10017 will open to evacuate the total production without safety consequences.																		22. Investigate the consequences on the PDU	SEGULA	
	2. Control valve PCV-10017 fails closed (control loop failure) while PCV-10020 is closed	4.7.2.1. Pressure build up inside the H2 separator leading to level	1.0E-01	5	3	5	3	3	3	LIC-10032	Low level to stop the rectifier	Control	10	3	2	3	LZI-10007/8 PZT 10005 LZI-14007/8	Low Low level to isolate the hydrogen separator (to close XZV-10044 and High high pressure trip to stop the rectifier High high level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIS - SIL 2 SIS - SIL 2			
	3. Control valves PCV- 10020 and PCV-10017 fail closed	4.7.3.1. Refer to the scenario 4.7.2.1																				

Conseil et assistance

12 - Appendix E – HAZOP Worksheet (8/12)

8. Less pressure or vacuum	1. Control valve PCV-10020 fails fully open (control loop failure)	4.8.1.1. Pressure release inside the separator leading to level unbalance between both separators. O2 H2 mixture inside hydrogen separator, due to the balanicng line, leading to explosion inside the separator.	1.0E-01	5	3	5	3	3	3	LIC-10032	High level to stop the rectifier	Control (DCS)	10	3	2	3	LZI-10007/8 LZI-14007/8	High high level to isolate the hydrogen separator (to close XZV-10044 liquid outlet and XZV-10045 balancing line) Low low level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2 SIS - SIL 2			
	2. Control valve PCV-10017 fails open (control loop failure)	4.8.2.1. Refer to the scenario 4.8.1.1																				
	3. Control valves PCV- 10017 and PCV-10020 fail open(control loop failure)	4.8.3.1. Refer to the scenario 4.8.1.1																				
	4. Refer to node 4 scenarios 4.4.1.1/4.4.2.1/4.4.3.1	4.8.4.1.																				
9. High liquid level	1. Refer to node 4 scenarios 4.4.1.1/4.4.2.1/4.4.3.1	4.9.1.1.																				
	2. Refer to node 5 scenarios 5.7	4.9.2.1.																				
10. Low or no liquid level	1. Refer to node 4 scenarios 4.7	4.10.1.1.																				
	2. Refer to node 5 scenarios 5.8	4.10.2.1.																				
11. Change in composition	1. Refer to node 4 scenario 4.7.3.1/4.2.2.1 /4.2.3.1/4.2.6 .1/4.3.1.1	4.11.1.1.																				
	2. Refer to node 5 scenarios 5.4.1.1/5.8.1.1	4.11.2.1. Loss of efficency without safety consequences																				
12. Change in KOH concentrati on	1. Refer to node1 scenario1.12.1.1	4.12.1.1.																				
	2. Refer to node 4 scenarios: 4.1.4.1/4.2.2.1/4.2.3.1	4.12.2.1.																				
13. Startup, maintenance and shutdown	1. Bad ultra pure water quality from upstream	4.13.1.1.																		23. Investigate the possibility to havean online conductivity measurment to stop the rectifier	SEGULA	
	2. Refer to node 2 scenario 2.16.1.1	4.13.2.1																				
	3. Wrong calibration of the gas analyzer.	4.13.3.1.																				
14. Loss of utilities	1. Loss of instrument air	4.14.1.1. The control LCV-10032 fails in closed position TCV-10028 fails in open position PCV-10020 & PCV-10017 fail in closed position XZV-10015 & XZV-10030 fails in closed position XZV-10004 fails in open position XZV-10007 fails in closed position XZV-10023 fails in closed position. XZV-10045 & XZV-10044 fails in closed position.																				
15. More current/voltage	1. No causes identified																					
16. Less current/voltage	1. No causes identified																					
17. Other	1. No causes identified																					
17. Other	1. No causes identified																					

Conseil et assistance

12 - Appendix E – HAZOP Worksheet (9/12)

Node: 5. LYE OXYGEN SEPARATION
Drawings / References: MO472-01-PRO-PID-012-00 Interconnecting ; MO472-01-PRO-PID-014 Oxygen Separation

Deviations	Causes	Consequences	Initial Risk: Fi	Sp (People)	Se (Environment)	Sa (Asset)	RRp	RRe	RRa	Safeguards without SIF: Tag	Description	CAT	Risk without SIF: RRF	RRp	RRe	RRa	Safety Instrumented Functions: Tag	Description	CAT	Actions: Actions	Responsibility	Remarks
1. More flow	1. Refer to node 3 scenario: 3.1.1.1	5.1.1.1																				
	2. Refer to node 1 deviation more flow scenarios : 1.1.1.1 and 1.1.1.2	5.1.2.1																				
	3. Refer to node 3 deviation more current scenario 3.15.1.1	5.1.3.1																				
	4. Pump variable speed drive is opareted at th maximum	5.1.4.1																				To be integrated at mire pressure deviation scenario
	5. Control valve LCV-10032 fails open (control loop failure)	5.1.4.1. More ultra pure demin water flow inside the separator leading to high level in both separators (due to the balancing line). Liquid flow in the gas production lines OSBL leading to pipe rupture, loss of containment and potential jet fire.	1.0E-01	3	2	3	3	2	3	LT- 10006/LT-10004 LIC-10032	High level to stop the rectifier High level to stop the rectifier (not independant from the cause)	Control (DCS) NA	10 1	2	2	2	LZT-10007/8 & LZT-14007/8	High high level trip to isolate the demin water feeding line (to close XZV-10031)	SIS - SIL 2	24. To design the pipe supports in order to withstand the production lines filled with liquid in order to avoid mechanical pipe rupture. Thus, we can reduce Sp to 0 and Sa to 0.	SEGULA	
	6. Refer to less pressure scenarios 5.8.1.1/5.8.2.1	5.1.5.1.																				
2. No or less flow	1. Refer to more pressure scenarios 5.7.1.1/5.7.2.1	5.2.1.1																				
	2. Control valve LCV-10032 fails closed	5.2.2.1. Consumption of water from the electrolyte solution continues. Gradual increase of concentration of KOH leading to higher viscosity and	1.0E-01	3	2	3	3	2	3	LT- 10006/LT-14006 LIC-10032	Low level to stop the rectifier Low level to stop the rectifier (not	Control (DCS) NA	10 1	2	2	2	LZT-10007/8 (H2) & LZT-14007/8	Low low level trip to stop the rectifier	SIS - SIL 2			
	3. Clogged strainers refer to node 1 scenario 1.2.4.1	5.2.3.1.																				
	4. The valve XZV-10023 closes spuriously	5.2.4.1. PCV-10017 will evacuate the total production without safety consequences.																				
	5. No ultra pure demin water flow from OSBL	5.2.5.1. Refer to the scenario 5.2.2.1																				
	6. The pump P-1040 failure from the ultra pure demin water supply	5.2.6.1. Refer to the scenario 5.2.2.1																				
	3. Check valve on the nitrogen feeding line stuck closed	5.2.7.1. Purging with nitrogen is not possible, resulting in delays to change of stuck.	1.0E-01			1			2			NA	1			2			NA			1. The production cannot start if pressure cycles during purging are not accomplished
3. Reverse flow	1. to refer to 4.3.1.1	5.3.1.1.																				
	2. Check valve NRV-10008 on the nitrogen feeding separtor opened	5.3.2.1. XZV-14007 is already open during O2 purging. A contamination with H2 in O2 distribution	1.0E-01			2			2	PT-13007	Low pressure alaram in the N2 distribution	Control (DCS)	1			1			NA			
4. Misdirected flow	1. The valve XZV-14004 opens spuriously	5.4.1.1. Pressure release inside the separator leading to level unbalance between both separators. O2 H2 mixture inside oxygen separator, due to the balanicng line, leading to explosion inside the separator.	1.0E-02	5	3	5	3	2	3	PDIC- 10010	High differential pressure to open production line on Hydrogen side (to oepn PCV-10017 and PCV-	Control (DCS)	10	3	2	3	LZI-14007/8 LZI-10007/8	High high level to isolate the oxygen separator (to close XZV-14039 and XZV-14041) Low Low level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045)	SIS - SIL 2 SIS - SIL 2			1. A vent seal drum is provided for the vent OSBL
	2. The valve PSV-14002 opens spuriously	5.4.2.1. Refer to the consequences of scenario 5.4.1.1	1.0E-04	5	3	5	2	1	2			NA	1	2	1	2	LZI-10007/8 LZI-14007/8	Low Low level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045) High high level to isolate the oxygen	SIS - SIL 2 SIS -	25. Calculate the reaction time and make sure it will be lower than the process time (the time when the PSV	Segula	
5. More temperature	1. Tube rupture in gas cooler E-1002	5.5.1.1. O2 leakage in chilled water network without overpressure since the heat exchanger is designed according to 10/13 API521 rule. Chilled water contaminated with O2 gas.	1.0E-02	4		4	3		3			NA	1	3		3			NA	26. Investigate the necessity to have a safeguard in case of H2/O2 is inside the chilled water system.	SEGULA	
	2. Control valve TCV-14026 fails closed (control loop failure)	1.2.6.1. Less flow to the stacks leading to unsufficient cooling of the stack exceeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-01			2			2	TIC-14026	High temperature to stop the rectifier (not independant from the cause)	NA	1			2	TZT-10013	High high temperature to stop the rectifier	SIS - SIL 2	27. Investigate the consequences on the PDU	SEGULA / MCPHY	
	3. The valves XZV-14015/XZV-14028 close spuriously	5.5.3.1. No more chilled water to cool down the oxygen gas leading to high gas temperature sent to OSBL and filled with KOH. Potential damage of the PDU.	1.0E-01			2			2	TIC-14026	High temperature to stop the rectifier	Control (DCS)	10			2	TZT-10013	High high temperature to stop the rectifier	SIS - SIL 2	28. Investigate the possibility to add a high high pressure monitoring on the cooling side to close XZV-14015/XZV-14028	SEGULA	
	4. No chilled water from upstream	5.5.4.1. Refer to scenario 5.5.3.1																				
6. Less temperature	1. Control valve TCV-14026 fails open (control loop failure)	5.6.1.1. Overcooling of the oxygen gas without safety consequens																				
7. More pressure	1. Control valve PCV-14017 fails closed (control loop failure)	5.7.1.1. Pressure build up inside the O2 separator leading to level unbalance between both separators. O2 H2 mixture inside Hydrogen separator. due to the balancing line. leading to explosion inside the	1.0E-01	5	3	5	3	3	3	LT- 10006/LT-14006	Low level to stop the rectifier	Control (DCS)	10	3	2	3	LZI-10007/8 LZI-14007/8	High high level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045) Low low level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2 SIS - SIL 2			
8. Less	1. Control valve PCV-14017 fails open (control loop	5.8.1.1. Pressure release inside the separator leading to level unbalance between both separators. O2 H2 mixture inside oxygen separator, due to the balanicng line, leading to explosion inside the separator.	1.0E-	5	3	[illegible]	3	3	3	LT- 10006/LT-14006	High level to stop the rectifier	Control (DCS)	10	3	2	3	LZI-14007/8	High high level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2			

12 - Appendix E – HAZOP Worksheet (9/12)

pressure or vacuum	1. Control valve PCV-14017 fails open (control loop		01										10				LZI-10007/8	Low Low level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045)	SIS - SIL 2			
	4. Refer to node 5 scenarios 5.4.1.1/5.4.2.1	5.8.2.1.																				
9. High liquid level	1. Refer to node 5 scenarios 5.1.4.1//5.4.1.1/5.4.2.1/5.8.1.1	5.9.1.1.																				
	2. Refer to node 4 scenarios 4.7.1.1. / 4.7.2.1. / 4.7.3.1./ 4.3.1.1	5.9.2.1.																				
10. Low or no liquid level	1. Refer to node 5 scenarios 5.7.1.1	5.10.1.1.																				
	2. Refer to node 4 scenarios 4.8	5.10.2.1.																				
11. Change in composition	1. Refer to node 4 scenario 4.11.1.1	5.11.1.1.																				
	2. Refer to node 2 scenario 2.16.1.1	5.11.2.1.																				
12. Change in KOH	1. Refer to node1 scenario 1.12.1.1	5.12.1.1.																				
	2. Refer to node 4 scenarios: 4.1.4.1/4.2.2.1/4.2.3.1	5.12.2.1.																				
13. Startup, maintenance and shutdown	1. Refer to node 4 scenario 4.13.1.1	5.13.1.1.																				
14. Loss of utilities	1. Loss of instrument air	5.14.1.1. The control TCV-14026 fails in open position PCV-14017 fail in closed position XZV-14015 & XZV-14028 fails in closed position XZV-14004 fails in open position XZV-14007 fails in closed position XZV-14021 fails in closed position. XZV-10041 & XZV-10039 fails in closed position.																				
15. More current/vol tage	1. No causes identified																					
16. Loss current/vol tage	1. No causes identified																					
17. Other	1. No causes identified																					

Conseil et assistance

12 - Appendix E – HAZOP Worksheet (10/12)

SOCOTEC TECHNICAL CONSULTING

Node: 6. Overall HOT STAND-BY MODE
Drawings / References:

Deviations	Causes	Consequences	Initial Risk: Fi	People: Sp	Environment: Se	Asset: Sa	RRp	RRe	RRa	Safeguards without SIF: Tag	Safeguards without SIF: Description	Safeguards without SIF: CAT	Safeguards without SIF: RRF	Risk without SIF: RRp	Risk without SIF: RRe	Risk without SIF: RRa	Safety Instrumented Functions: Tag	Safety Instrumented Functions: Description	Safety Instrumented Functions: CAT	Actions: Actions	Actions: Responsibility	Remarks
1. More flow	1. Fail to turn off the rectifier	6.1.1.1. Gas production leading to pressure build up inside the system and potential stack burst. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-01	3	2	3	3	2	3	PSV- 14002/PSV-10002	PSV on the separators with 33 set pressure	PSV	100	1	1	1	PZI-10005/PZI-14005	High high pressure to stop the rectifier	SIS - SIL 2		Responsibility	
										PT- 10004/PT-14004	High pressure to open the vents on both separators.	Control (DCS)	10									
		6.1.1.2. Overheating of the stacks leading to unsufficient cooling exeeding the design temperature. Degradation of the membrane and cell frame failure. Medium leakage of electrolyte with O2/H2 leading to operator exposure to hot and corrosive stream.	1.0E-01	3	2	3	3	2	3	TT-04009 / TT-04010 TT-04011/ TT-04012/ TT-04013 / TT-04014	Feedback from the rectifier to stop the electrolyzer and depressurize	Control (DCS)	10	2	2	2	TZS-04015 / TZS-04016 / TZS-04017 / TZS-04018 / TZS-04019 / TZS-04020	High high temperature to stop the rectifier	SIS - SIL 2			
	2. Pump turns on spuriously	6.1.2.1. KOH flow inside the system without safety consequences																	NA			
	3. Control valve LCV-10032 opens spuriously	6.1.3.1. More ultra pure demin water flow inside the separator leading to high level in both separators (due to the balancing line). Liquid flow in the gas production lines leading to pipe rupture, loss of containment and potential jet fire.	1.0E-01	3	2	3	3	2	3	LT- 10006/LT-10004	High level to stop the rectifier	Control (DCS)	10	2	2	2	LZT-10007/8 & LZT-14007/8	High high level trip to isolate the demin water feeding line (to close XZV-10031)	SIS - SIL 2	24. To design the pipe supports in order to withstand the production lines filled with liquid in order to avoid mechanical pipe rupture. Thus, we can reduce Sp to 0 and Sa to 0.	SEGULA	
										LIC-10032	High level to stop the rectifier (not independant from the cause)	NA	1									
	4. Control valve PCV-10020 fails open (control loop failure)	6.1.4.1. Refer to scenario 4.3.1.1																				
	5. Control valve upstream the stacks fails open	6.1.5.1. There is no flow without safety consequences																				
	6. Pump variable speed drive is opareted at the maximum	6.1.6.1 No safety consequences																				To be integrated at more pressure deviation scenario
2. No or less flow	1. No causes identified																					
3. Reverse flow	1. No causes identified																					
4. Misdirected flow	1. No causes identified																					
5. More temperature	1. Refer to to 6.1.1.2	6.5.1.1.																				
6. Less temperature	1. Cooling water system turns on spuriously	6.6.1.1. No safety concequences since no flow																				
	2. Chilled water system turns on spuriously	6.6.1.2. Refer to the consequences of scenario 1.2.3.1																				
7. More pressure	1. No causes identified																					
8. Less pressure or vacuum	1. No causes identified																					
9. High liquid level	1. No causes identified																					
10. Low or no liquid level	1. No causes identified																					
11. Change in compositio n	1. No causes identified																					
12. Change in KOH concentrati on	1. No causes identified																					
13. Startup, maintenan ce and shutdown	1. No causes identified																					
14. Loss of utilities	1. No causes identified																					
15. More current/vol tage	1. No causes identified																					
16. Less current/vol tage	1. No causes identified																					
17. Other	1. No causes identified																					

12 - Appendix E – HAZOP Worksheet (11/12)

Node: 7. N2 COLD STAND-BY MODE
Drawings / References:

Deviations	Causes	Consequences	Initial Risk							Safeguards without SIF				Risk without SIF			Safety Instrumented Functions			Actions		Remarks
			Fi	People Sp	Environment Se	Asset Sa	RRp	RRe	RRa	Tag	Description	CAT	RRF	RRp	RRe	RRa	Tag	Description	CAT	Actions	Responsibility	
1. More flow	1. Refer to node 6 deviation more flow, scenarios: 6.1.1.1/.1.1. 2/6.1.2.1	7.1.1.1.																				
	2. Control valve LCV-10032 opens spuriously	7.1.2.1. More ultra pure demin water flow inside the separator leading to high level in both separators (due to the balancing line). Liquid flow in the gas production lines OSBL leading to pipe rupture, loss of containment	1.0E-01	3	2	3	3	2	3	LT- 10006/LT-10004	High level to stop the rectifier	Control (DCS)	10	2	2	2	LZT-10007/8 & LZT-14007/8	High high level trip to isolate the demin water feeding line (to close XZV-10031)	SIS - SIL 2	24. To design the pipe supports in order to withstand the production lines filled with liquid in order to avoid mechanical pipe rupture. Thus, we can reduce Sp to 0 and Sa to 0.	SEGULA	
										LIC-10032	High level to stop the rectifier (not independant from the cause)	Control (DCS)	10									
	3. Control valve PCV-10017 fails open (control loop failure) H2 separator side	7.1.3.1. Pressure release inside the separator leading to level unbalance between both separators. O2 H2 and N2 mixture inside hydrogen separator, due to the balanicng line, without safety consequences																				
	4. Control valve PCV-14017 fails open (control loop failure) O2 Separator side	7.1.4.1. Pressure release inside the separator leading to level unbalance between both separators. O2 H2 and N2 mixture inside Oxygen separator, due to the balanicng line, without safety consequences																				
	5. Pump variable speed drive is opareted at the maximum	7.1.5.1.																				To be integrated at mire pressure deviation scenario
2. No or less flow	1. No causes identified																					
3. Reverse flow	1. No causes identified																					
4. Misdirected flow	1. XZV-14007 opens spuriously for O2 Separator	7.4.1.1. back pressure from the N2 system (more than 8 barg, less than 30 barg) leading to level unbalance between both separators. Gas mixture inside oxygen separator, due to the balanicng line, without safety consequences																				
	2. XZV-10007 opens spuriously H2 separator	7.4.2.1. back pressure from the N2 system (more than 8 barg, less than 30 barg) leading to level unbalance between both separators. Gas mixture inside hydrogen separator, due to the balanicng line, without safety consequences																				
5. More temperature	1. No causes identified																					
6. Less temperature	1. No causes identified																					
7. More pressure	1. No causes identified																					
8. Less pressure or vacuum	1. No causes identified																					
9. High liquid level	1. No causes identified																					
10. Low or no liquid level	1. No causes identified																					
11. Change in composition	1. No causes identified																					
12. Change in KOH concentration	1. No causes identified																					
13. Startup, maintenance and shutdown	1. No causes identified																					
14. Loss of utilities	1. No causes identified																					
15. More current/voltage	1. No causes identified																					
16. Less current/voltage	1. No causes identified																					
17. Other	1. No causes identified																					

Conseil et assistance

12 - Appendix E – HAZOP Worksheet (12/12)

Node: 8. H2 COLD STAND-BY MODE
Drawings / References:

Deviations	Causes	Consequences	Initial Risk							Safeguards without SIF				Risk without SIF			Safety Instrumented Functions			Actions		Remarks
			Fi	People Sp	Environment Se	Asset Sa	RRp	RRe	RRa	Tag	Description	CAT	RRF	RRp	RRe	RRa	Tag	Description	CAT	Actions	Responsibility	
1. More flow	1. Refer to node 6 deviation more flow, scenarios: 6.1.1.1/.1.1. 2/6.1.2.1	8.1.1.1.																				
	2. Control valve LCV-10032 opens spuriously	8.1.2.1. More ultra pure demin water flow inside the separator leading to high level in both separators (due to the balancing line). Liquid flow in the gas production lines OSBL leading to pipe rupture, loss of containment	1.0E-01	3	2	3	3	2	3	LT- 10006/LT-10004	High level to stop the rectifier	Control (DCS)	10	2	2	2	LZT-10007/8 & LZT-14007/8	High high level trip to isolate the demin water feeding line (to close XZV-10031)	SIS - SIL 2	24. To design the pipe supports in order to withstand the production lines filled with liquid in order to avoid mechanical pipe rupture. Thus, we can reduce Sp to 0 and Sa to 0.	SEGULA	
										LIC-10032	High level to stop the rectifier (not independant from the cause)	Control (DCS)	10									
	3. Control valve PCV-10017 fails open (control loop failure) H2 separator side	8.1.3.1. Pressure release inside the separator leading to level unbalance between both separators. O2 H2 mixture inside hydrogen separator, due to the balanicng line, leading to explosion inside the separator.	1.0E-01	5	3	5	3	3	3	LIC-10032	High level to stop the rectifier	Control (DCS)	10	3	2	3	LZI-10007/8	High high level to isolate the hydrogen separator (to close XZV-10044 liquid outlet and XZV-10045 balancing line)	SIS - SIL 2			
																	LZI-14007/8	Low low level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2			
	4. Control valve PCV-14017 fails open (control loop failure) O2 Separator side	8.1.4.1. Pressure release inside the separator leading to level unbalance between both separators. O2 H2 mixture inside oxygen separator, due to the balanicng line, leading to explosion inside the separator.	1.0E-01	5	3	5	3	3	3	LT- 10006/LT-14006	High level to stop the rectifier	Control (DCS)	10	3	2	3	LZI-14007/8	High high level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2			
																	LZI-10007/8	Low Low level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045)	SIS - SIL 2			
	5. Pump variable speed drive is opareted at the maximum	8.1.5.1.																				To be integrated at mire pressure deviation scenario
3. Reverse flow	1. No causes identified																					
4. Misdirected flow	1. XZV-14007 opens spuriously for O2 Separator	8.4.1.1. back pressure from the N2 system (more than 8 barg, less than 30 barg) leading to level unbalance between both separators. O2 H2 mixture inside oxygen separator, due to the balanicng line, leading to	1.0E-01	5	3	5	3	3	3	LT- 10006/LT-14006	Low level to stop the rectifier	Control (DCS)	10	3	2	3	LZI-10007/8	High high level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045)	SIS - SIL 2			
																	LZI-14007/8	Low low level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2			
	2. XZV-10007 opens spuriously H2 separator	8.4.2.1. back pressure from the N2 system (more than 8 barg,less than 30 barg) leading to level unbalance between both separators. O2 H2 mixture inside hydrogen separator, due to the balanicng line, leading to explosion inside the separator.	1.0E-01	5	3	5	3	3	3	LIC-10032	Low level to stop the rectifier	Control (DCS)	10	3	2	3	LZI-10007/8	Low Low level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045)	SIS - SIL 2			
																	PZT 10005	High high pressure trip to stop the rectifier	SIS - SIL 2			
																	LZI-14007/8	High high level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2			
5. More temperature	1. No causes identified																					
6. Less temperature	1. No causes identified																					
7. More pressure	1. No causes identified																					
8. Less pressure or vacuum	1. No causes identified																					
9. High liquid level	1. No causes identified																					
10. Low or no liquid level	1. No causes identified																					
11. Change in compositio n	1. No causes identified																					
12. Change in KOH concentrati on	1. No causes identified																					
13. Startup, maintenan ce and shutdown	1. No causes identified																					
14. Loss of utilities	1. No causes identified																					
15. More current/vol tage	1. No causes identified																					
16. Less current/vol tage	1. No causes identified																					
17. Other	1. No causes identified																					

Thank you for this exchange

Your contacts:

Ali EL OUAZZANI
Project manager
SOCOTEC Technical Consulting
ali.elouazzani@socotec.com

A generic STC email:
Technical_consulting@socotec.com