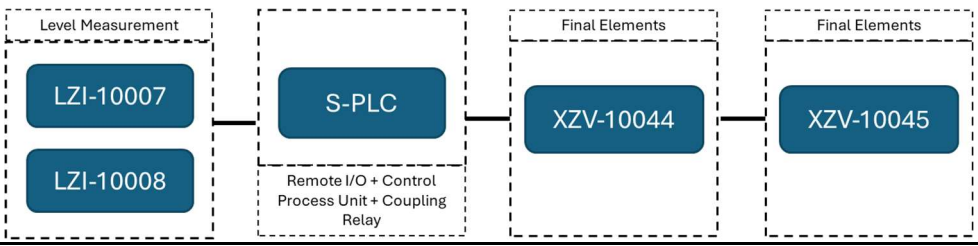
Scénario N°	Description du scénario	Equipement	Réf. MMR	Description MMR			Nature	NC	Type de sécurité	Testabilité / maintenabilité
				Détection	Traitement	Action				
3	Explosion interne du séparateur O_2 et H_2	Séparateur O_2 /H_2	1	Pression différentielle élevée capteur PDIC- 10010	Automate de conduite	Ouverture vanne PCV 14017 et PCV 10200	Technique	1	Active	Oui
3	Explosion interne du séparateur O_2 et H_2	Séparateur O_2 /H_2	2	Niveau très très bas capteurs LZI-10007 & LZI-10008	Automate de conduite	Fermeture les vannes XZV-10044 et XZV-10045	Technique	2	Active	Oui
3 et 4	Explosion interne du séparateur O_2 et H_2 Explosion pneumatique du séparateur O_2 et H_2	Séparateur O_2 /H_2	3	Niveau très très haut capteurs LZI-14007 & LZI-14008	Automate de conduite	Fermeture les vannes XZV-14039 et XZV-14041	Technique	2	Active	Oui
3 et 4	Explosion interne du séparateur O2 et H2 Explosion pneumatique du séparateur O2 et H2	Séparateur O_2 /H_2	4	Niveau bas ou haut capteurs : LZT-10007/8 (H2) & LZT-14007/8 (O2)	Automate de conduite	Arrêt du redresseur (rectifier)	Technique	1	Active	Oui
3	Explosion interne du séparateur O_2 et H_2	Séparateur O_2 /H_2	5	Pression élevée capteurs : PZI-10005 & PZI-14005	Automate de conduite	Arrêt du redresseur (rectifier)	Technique	2	Active	Oui
3	Explosion interne du séparateur O_2 et H_2	Séparateur O_2 /H_2	6	Niveau bas LIC-10032	Automate de conduite	Arrêt du redresseur (rectifier)	Technique	1	Active	Oui
3	Explosion interne du séparateur O_2 et H_2	Séparateur O_2 /H_2	7	Niveau élevé HTO/OTH	Alarme	Alarme pour action d'operateur	Technique et organisationnelle	1	Active	Oui

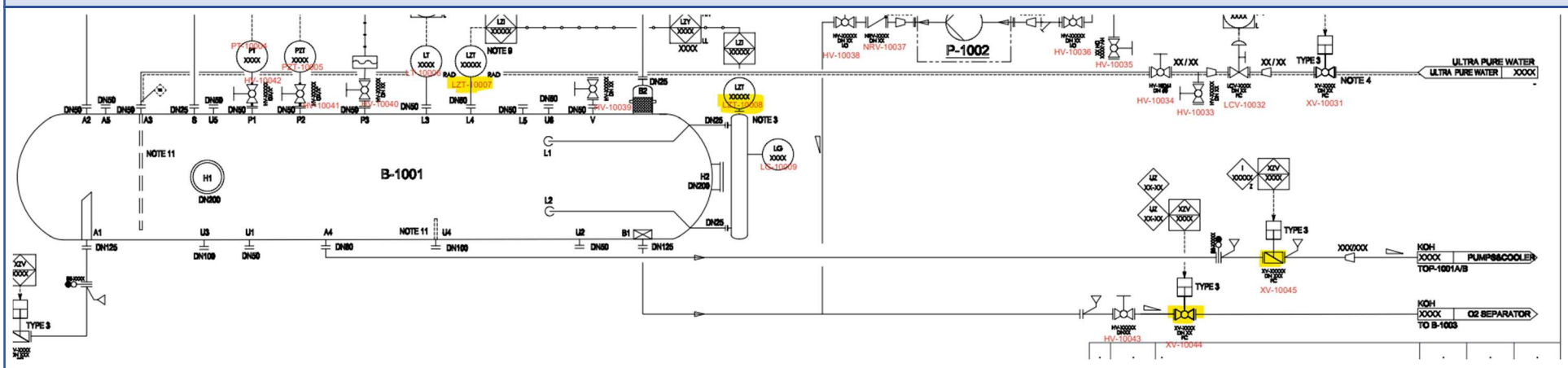
Scénario N°	Description du scénario	Equipement	Réf. MMR	Description MMR			Nature	NC	Type de sécurité	Testabilité / maintenabilité
				Détection	Traitement	Action				
3	Explosion interne du séparateur O_2 et H_2	Séparateur O_2 /H_2	8	Détection courant faible : CZS-04022	Automate de conduite	Arrêt du redresseur (rectifier)	Technique	1	Active	Oui

SRS sheet	Title : **Low Low level for isolating valves XZV-10044/10045** **Niveau très très bas pour fermeture des vannes XZV-10044 et XZV-10045**	PID number : MO472-01-PRO-PID-010	Name : LZI-10007/10008 Rev0

SAFETY FUNCTION PRESENTATION

Detailed description	In case of low low level of LZI-10007/08 on the H2 separator. - XZV-10044 valve is closed - XZV-10045 valve is closed, isolating the separator 	**Required SIL** 2
Fail safe status of the process	Valves XZV-10044 and XZV-10045 are closed and separator is isolated. This prevents H2/O2 mixture formation due to the balancing line.	**Response Time** 5s **Calculated SIL** 2

Location on P&ID



	Tag	Description	Type	Failure treatment (FS / NFS)	Redundancy Monitoring	Undetected failure rate λdu (h-1)	Override
SENSOR	LZI – 10007/08	Level Transmitter	Endress & Hauser – FMP51	FS	1oo2	2E-07	NA

Note : MOS for maintenance override ; OOS for operation overrides.

	Tag	Description	Type		Failure treatment (FS/NFS)	Undetected failure rate λdu (h-1)			
SOLVER	F-CPU	Safety PLC	SIEMENS 6ES71366AA000CA1		FS	1,00E-09			

Note : FS for Fail Safe ; NFS for Non Fail Safe.

	Tag	Description	Type	Failure treatment (FS/NFS)	Undetected failure rate λdu (h-1)	Action	Redundancy Monitoring	Specific requirements (Tight shut off / Energy needs)
ACTUATORS	XZV-10044	Solenoid valve	COAX -Type MK 20 560141	FS	8.26E-9	Close	1oo1	/
	XZV-10045	Solenoid valve	COAX -Type MK 20 560141	FS	8.26E-9	Close	1oo1	

Note : FS for Fail Safe ; NFS for Non Fail Safe.

EFFICIENCY

EFFICIENCY	**Equipment sizing Threshold value**	A time delay (0s by default) is available to delay warning/trip triggering if required (prevent false alarms by ignoring spurious sound peaks not generated by a leak).
	Environmental conditions Specific constraints	Temperature from -20°C to +40 °C. Specific constraints coming from the manipulation of H2 have been taken into account when implementing sensors and actuators
	Resist to accidental conditions (e.g. fire…)	The instrumentation is adapted to the ambient conditions.
	Failure tolerance	If sensors fails, the function trip.
	Equipment availability for a safety purpose	No element can prevent the running of the safety function.

OPERATION

OPERATION	**SPL trip signalisation**	Trip message is displayed on station HMI and dispenser HMI.
	Safety function manual shutdown	Not applicable
	Reseting after trip	SIF must be reset in the control room with the ESD reset push button (located on the main cabinet). Remote ESD reset on station HMI is possible (After visual inspection only)
	Automatic override	Not applicable
	Compensating actions (in case of a failure or a MOS)	No compensating actions
	Specific operating cases (e.g. blowing, flushing…)	Not applicable

MAINTENANCE

MAINTENANCE	**Test periods**	SIF must be tested from the sensor to the actuator every year
	Equipment maintenance	See "Installation operation and maintenance" manual

CHANGE HISTORY

Name	Change description	Date	Révision

COMMENTS

SRS sheet	Title : Low Low level for isolating valves XZV-10044/10045 Niveau très très bas pour fermeture des vannes XZV-10044 et XZV-10045	PID number : MO472-01-PRO-PID-010	Name : LZI-10007/10008 Rev0

JUSTIFICATION OF SIL LEVEL

1/ RESULT

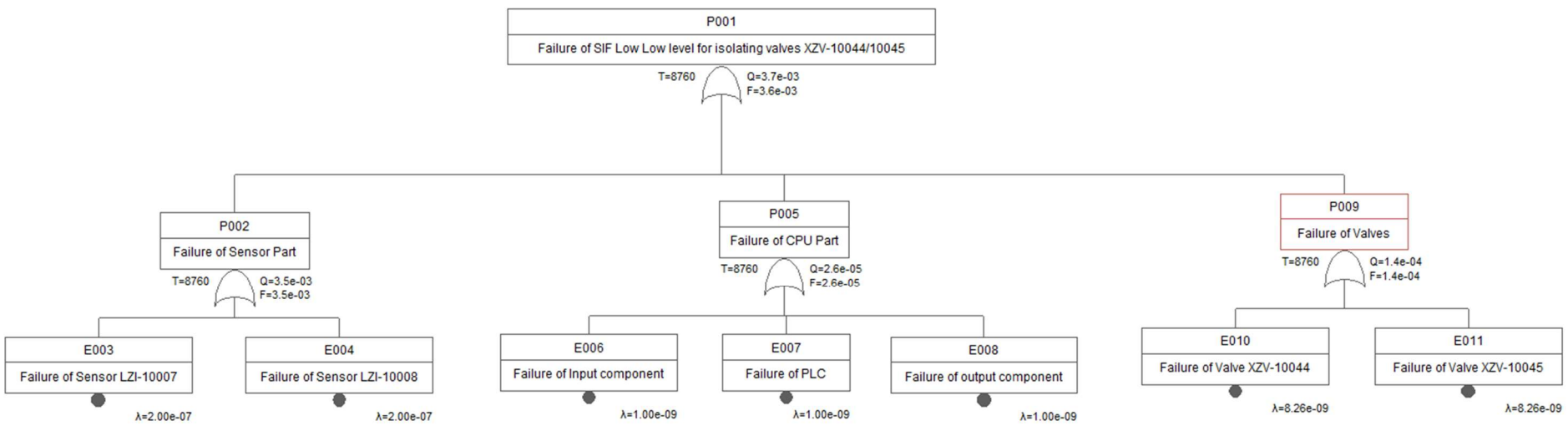
Description SIF	PFD Average	SIL achieved with architectural constraints	SIL Achieved with PFD	Targeted SIL	SIL Met
Low Low level for isolating valves XV-10044/10045 Niveau très très bas pour fermeture des vannes XZV-10044 et XZV-10045	3.6E-03	SIL 2	SIL 2	SIL 2	SIL 2 (NC2)

Calculation assumptions:

The calculations are performed on a 1-year lifecycle or 8760 hours.
The proof test frequency is 1 year or 8760 hours.
All the safety functions operate in "low demand mode".
All components follow Route 1H of IEC 61508.
The PFD average is defined from λd, as per IEC 61508.
All equipment is considered repairable, and each piece of equipment has its own specific MTTR.

2/ FAULT TREE

The SIF architecture used in the calculations are shown below:



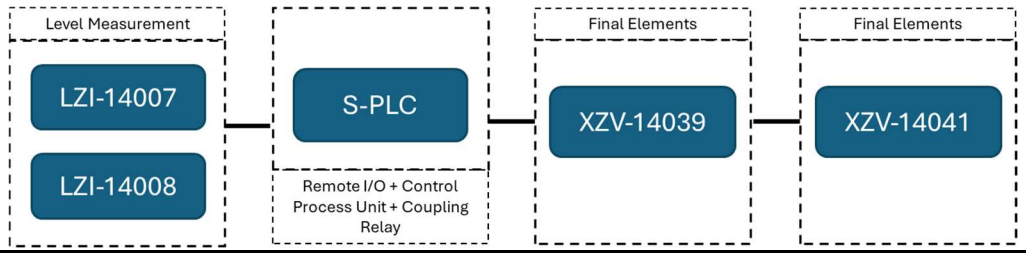
Hazard & risk assessment

Source document : XL Pilot Hazop report
Version : v1
Date : 10/03/2025
Node Number : 4

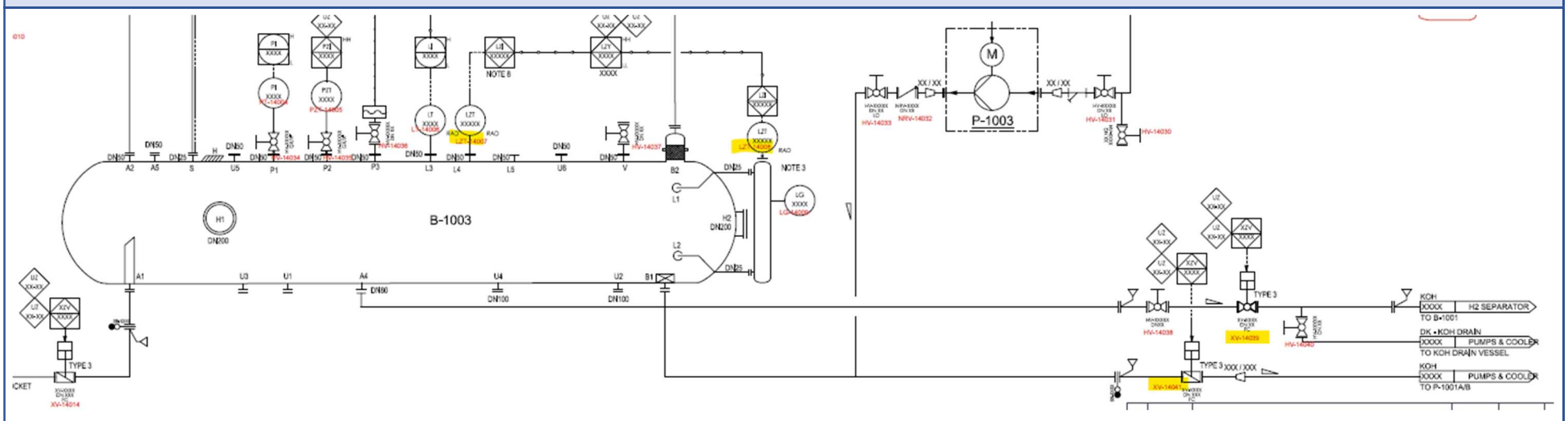
7. More pressure	1. Control valve PCV-10020 fails closed (control loop failure) while PCV-10017 is closed	4.7.1.1. PCV-10017 will open to evacuate the total production without safety consequences.	1.0E-01	5	3	5	3	3	3	LIC-10032	Low level to stop the rectifier	Control (DCS)	10	3	2	3	LZI-10007/8	Low Low level to isolate the hydrogen separator (to close XZV-10044 and XZV-10045)	SIS - SIL 2
	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 unbalance between both separators. O2 H2 mixture inside oxygen separator, due to the balancing line, leading to explosion inside the separator.															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

SRS sheet	Title : **High High level for isolating valves XZV-14039/14041** **Niveau très très haut pour fermeture des vannes XZV-14039 et XZV-14041**	PID number : MO472-01-PRO-PID-014	Name : LZI-14007/14008 Rev0

SAFETY FUNCTION PRESENTATION

Detailed description	In case of High High level of LZI-14007/08 on the O2 seperator. - XZV-14039 valve is closed - XZV-14041 valve is closed, isolating the separator 	**Required SIL** 2
Fail safe status of the process	Valves XZV-14039 and XZV-14041 are closed and separator is isolated. This prevents H2/O2 mixture formation due to the balancing line.	**Response Time** 5s **Calculated SIL** 2

Location on P&ID



	Tag	Description	Type	Failure treatment (FS / NFS)	Redundancy Monitoring	Undetected failure rate λdu (h-1)	Override
SENSOR	LZI–14007/08	Level Transmitter	Endress & Hauser – FMP51	FS	1oo2	2E-07	NA

Note : MOS for maintenance override ; OOS for operation overrides.

	Tag	Description	Type		Failure treatment (FS/NFS)	Undetected failure rate λdu (h-1)			
SOLVER	F-CPU	Safety PLC	SIEMENS 6ES71366AA000CA1		FS	1,00E-09			

Note : FS for Fail Safe ; NFS for Non Fail Safe.

	Tag	Description	Type	Failure treatment (FS/NFS)	Undetected failure rate λdu (h-1)	Action	Redundancy Monitoring	Specific requirements (Tight shut off / Energy needs)
ACTUATORS	XZV-14039	Solenoid valve	COAX -Type MK 20 560141	FS	8.26E-9	Close	1oo1	/
	XZV-14041	Solenoid valve	COAX -Type MK 20 560141	FS	8.26E-9	Close	1oo1	

Note : FS for Fail Safe ; NFS for Non Fail Safe.

EFFICIENCY

EFFICIENCY	**Equipment sizing Threshold value**	A time delay (0s by default) is available to delay warning/trip triggering if required (prevent false alarms by ignoring spurious sound peaks not generated by a leak).
	Environmental conditions Specific constraints	Temperature from -20°C to +40 °C. Specific constraints coming from the manipulation of H2 have been taken into account when implementing sensors and actuators
	Resist to accidental conditions (e.g. fire…)	The instrumentation is adapted to the ambiant conditions.
	Failure tolerance	If sensors fails, the function trip.
	Equipment availability for a safety purpose	No element can prevent the running of the safety function.

OPERATION

OPERATION	**SPL trip signalisation**	Trip message is displayed on station HMI and dispenser HMI.
	Safety function manual shutdown	Not applicable
	Reseting after trip	SIF must be reset in the control room with the ESD reset push button (located on the main cabinet). Remote ESD reset on station HMI is possible (After visual inspection only)
	Automatic override	Not applicable
	Compensating actions (in case of a failure or a MOS)	No compensating actions
	Specific operating cases (e.g. blowing, flushing…)	Not applicable

MAINTENANCE

MAINTENANCE	**Test periods**	SIF must be tested from the sensor to the actuator every year
	Equipment maintenance	See "Installation operation and maintenance" manual

CHANGE HISTORY

Name	Change description	Date	Révision

COMMENTS

SRS sheet	Title : High High level for isolating valves XZV-14039/14041 Niveau très très haut pour fermeture des vannes XZV-14039 et XZV-14041	PID number : MO472-01-PRO-PID-014	Name : LZI-14007/14008 Rev0

JUSTIFICATION OF SIL LEVEL

1/ RESULT

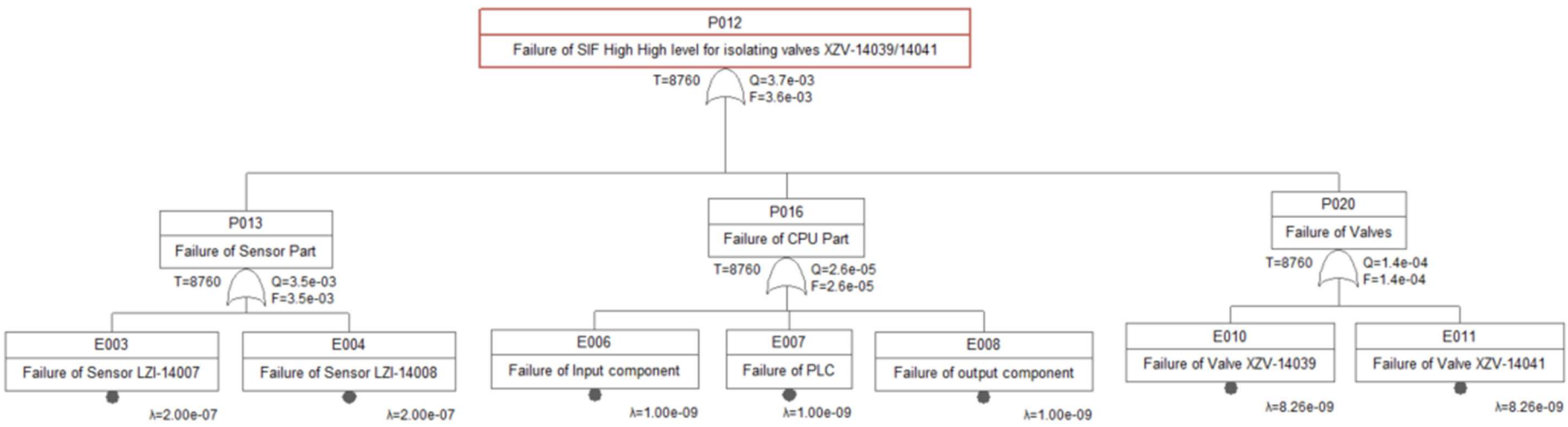
Description SIF	PFD Average	SIL achieved with architectural constraints	SIL Achieved with PFD	Targeted SIL	SIL Met
High High level for isolating valves XV-14039/10041 Niveau très très haut pour fermeture des vannes XZV-14039 et XZV-14041	3.6E-03	SIL 2	SIL 2	SIL 2	SIL 2 (NC2)

Calculation assumptions:

The calculations are performed on a 1-year lifecycle or 8760 hours.
The proof test frequency is 1 year or 8760 hours.
All the safety functions operate in "low demand mode".
All components follow Route 1H of IEC 61508.
The PFD average is defined from λd, as per IEC 61508.
All equipment is considered repairable, and each piece of equipment has its own specific MTTR.

2/ FAULT TREE

The SIF architecture used in the calculations are shown below:



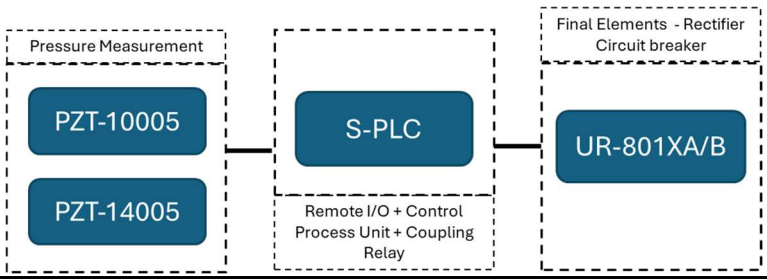
Hazard & risk assessment

Source document : XL Pilot Hazop report
Version : v1
Date : 10/03/2025
Node Number : 4

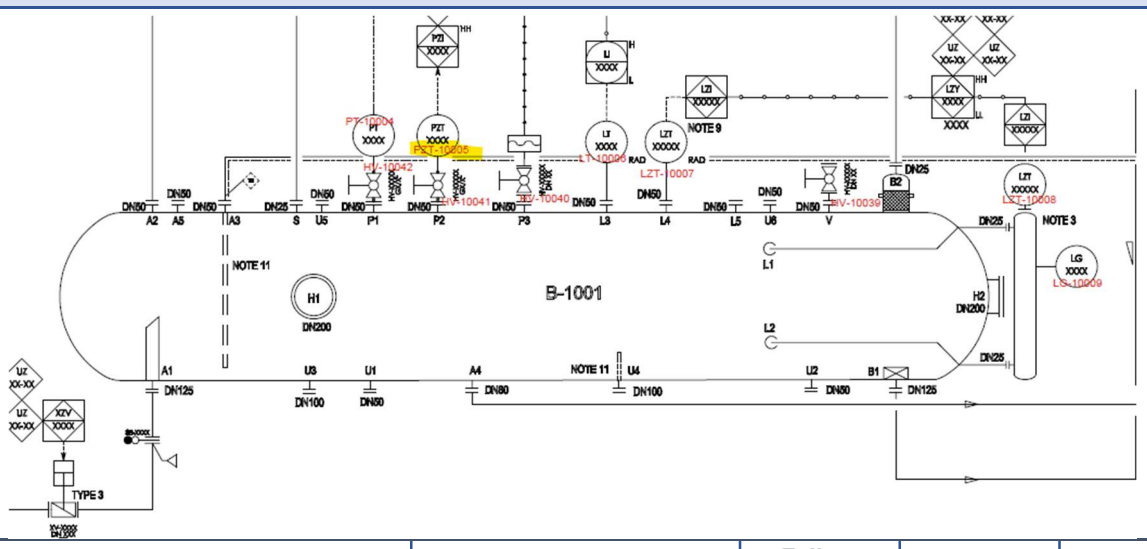
7. More pressure	1. Control valve PCV-10020 fails closed (control loop failure) while PCV-10017 is closed	4.7.1.1. PCV-10017 will open to evacuate the total production without safety consequences.																		
	2. Control valve PCV-10017 fails closed (control loop failure) while PCV-10020 is closed	4.7.2.1. Pressure build up inside the H2 separator leading to level unbalance between both separators. O2 H2 mixture inside oxygen separator, due to the balancing 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

SRS sheet	Title : **High High pressure for stopping the rectifier Pression très très élevée pour arrêter du rectifier**	PID number : MO472-01-PRO-PID-010	Name : PZT-10005/14005 Rev0

SAFETY FUNCTION PRESENTATION

Detailed description	In case of High high pressure of PZT-10005 or PZT-14005 on either of the H2/O2 separator. - Rectifier is shut down by means of the circuit breaker 	**Required SIL** 2
Fail safe status of the process	Rectifier is shutdown using the circuit breaker and the production is completely stopped.	**Response Time** 5s **Calculated SIL** 2

Location on P&ID



	Tag	Description	Type	Failure treatment (FS / NFS)	Redundancy Monitoring	Undetected failure rate λdu (h-1)	Override
SENSOR	PZT – 10005/14005	Pressure Transmitter	SIEMENS -SITRANS P320/420	FS	1oo2	4.8E-08	NA

Note : MOS for maintenance override ; OOS for operation overrides.

	Tag	Description	Type		Failure treatment (FS/NFS)	Undetected failure rate λdu (h-1)			
SOLVER	F-CPU	Safety PLC	SIEMENS 6ES71366AA000CA1		FS	1,00E-09			

Note : FS for Fail Safe ; NFS for Non Fail Safe.

	Tag	Description	Type	Undetected failure rate λdu (h-1)	Action	Redundancy Monitoring	Specific requirements (Tight shut off / Energy needs)
ACTUATORS	UR-801XA/B	Circuit breaker rectifier	SEIMENS - 3SK1121-1AB40	1.6E-9	Open	1oo1	/

Note : FS for Fail Safe ; NFS for Non Fail Safe.

EFFICIENCY

EFFICIENCY	**Equipment sizing** **Threshold value**	A time delay (0s by default) is available to delay warning/trip triggering if required (prevent false alarms by ignoring spurious sound peaks not generated by a leak).
	Environmental conditions **Specific constraints**	Temperature from -20°C to +40 °C. Specific constraints coming from the manipulation of H2 have been taken into account when implementing sensors and actuators
	Resist to accidental conditions (e.g. fire…)	The instrumentation is adapted to the ambient conditions.
	Failure tolerance	If sensors fails, the function trip.
	Equipment availability for a safety purpose	No element can prevent the running of the safety function.

OPERATION

OPERATION	**SPL trip signalisation**	Trip message is displayed on station HMI and dispenser HMI.
	Safety function manual shutdown	Not applicable
	Reseting after trip	SIF must be reset in the control room with the ESD reset push button (located on the main cabinet). Remote ESD reset on station HMI is possible (After visual inspection only)
	Automatic override	Not applicable
	Compensating actions (in case of a failure or a MOS)	No compensating actions
	Specific operating cases (e.g. blowing, flushing…)	Not applicable

MAINTENANCE

MAINTENANCE	**Test periods**	SIF must be tested from the sensor to the actuator every year
	Equipment maintenance	See "Installation operation and maintenance" manual

CHANGE HISTORY

Name	Change description	Date	Révision

COMMENTS

SRS sheet	Title : High High pressure for stopping the rectifier Pression très très élevée pour arrêter du rectifier	PID number : MO472-01-PRO-PID-010	Name : PZT-10005/14005 Rev0

JUSTIFICATION OF SIL LEVEL

1/ RESULT

Description SIF	PFD Average	SIL achieved with architectural constraints	SIL Achieved with PFD	Targeted SIL	SIL Met
High High pressure for stopping the rectifier Pression très très élevée pour arrêter du rectifier	8.8E-04	SIL 2	SIL 2	SIL 2	SIL 2 (NC2)

Calculation assumptions:

The calculations are performed on a 1-year lifecycle or 8760 hours.
The proof test frequency is 1 year or 8760 hours.

All the safety functions operate in "low demand mode".

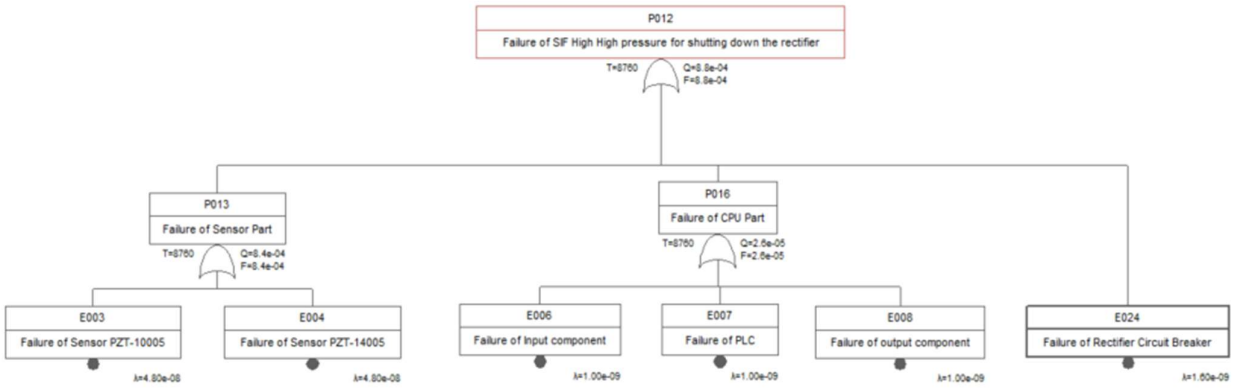
All components follow Route 1H of IEC 61508.

The PFD average is defined from λd, as per IEC 61508.

All equipment is considered repairable, and each piece of equipment has its own specific MTTR.

2/ FAULT TREE

The SIF architecture used in the calculations are shown below:



Hazard & risk assessment

Source document : XL Pilot Hazop report

Version : v1

Date : 10/03/2025

Node Number : 4

7. More pressure	1. Control valve PCV-10020 fails closed (control loop failure) while PCV-10017 is closed 2. Control valve PCV-10017 fails closed (control loop failure) while PCV-10020 is closed	4.7.1.1. PCV-10017 will open to evacuate the total production without safety consequences. 4.7.2.1. Pressure build up inside the H2 separator leading to level unbalance between both separators. O2 H2 mixture inside oxygen separator, due to the balancing line, leading to explosion inside the separator.	10E-01	5	3	5	3	3	3	LIC-10032	Low level to stop the rectifier	Control (DCS)	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 XZV-10045) High high pressure trip to stop the rectifier High high level to isolate the oxygen separator (to close XZV-14039 and XZV-14041)	SIS - SIL 2 SIS - SIL 2 SIS - SIL 2