The purpose of this SAMPLE document is to show in the public domain a typical SIL verification assessment & report (Detailed Report)

For a "Letdown Station", developed by:

LIUTAIO

"FUNCTIONAL SAFETY SERVICES"

For preparing this SAMPLE report, examples of industrial processes and typical process data was used in combination with

LIUTAIO experience.

However, when this report is prepared for a CUSTOMER, only the authorized or provided information by CUSTOMER will be used, and the report **WILL NOT BE** part of the public domain.

SIL Verification assessment SUMMARY

(Low Demand System)

SIF's Tag number	60-SIF-500	**SIL Verification Report No.**	0418E30SD08
SIF's Description	Gas Processing Plant inlet facilities protection against an overpressure operation scenario		
Process Safety Time (PST)	30 sec	**SIF Response Time (SRT, MART)**	15 sec
Target SIL rating	**SIL 3**	**Maximum SIL Safety Design Limit (MSSDL)**	70%
Verified SIL rating	**SIL 1**	**SIF's Service Life period (SLf)**	10 years

The purpose of this SIL verification report was to execute a preliminary assessment of the 60-SIF-500 design, considering Simple/Enhanced design/installation, Maintenance times (MTR, TD, MRT), and the SIF Devices fault detection capabilities (Diagnostics) that were used in the design.

The "SIL verification" assessment RESULTS were:

1) 60-SIF-500 design in document (reference [5]) "0418E30SD09 Conceptual SRS – Letdown Station" **is capable to satisfy "SIL 1" rating, instead of target "SIL 3" rating**. "Proof Test" 6 months. See Table 1.

2) The main reason to **DO NOT** reach the target SIL rating is the "SIL a" qualification of ALL safety valves (QSV and ESV) by "Safe Failure Fraction" (SFF). This fact allows 60-SIF-500 to claim ONLY up to "SIL 1" rating. Refer to Table 1.

"SIL verification" RESULTs (Low Demand System)					
Total PFDavg	**Total RRF**	**Total % WC**	**Effective SIL rating by**		
			IEC-61508	**MSSDL**	**Route 1H**
6.59E-04	1517	100.0%	SIL 3 **(4)**	SIL 3 **(5)**	SIL 1 **(3)**

Verified SIF's SIL rating : SIL 1 **Note 2**

3) The following action is required to make 60-SIF-500 to satisfy target "SIL 3" rating:

a) Change ALL safety valves (QSV and ESV) for valves capable to claim for up to "SIL 2" rating, according to SFF.

After verifying above indicated action:

4) 60-SIF-500 satisfies the target "SIL 3" rating (see Table 2), and

5) "Proof Test" shall be executed every 7 months for ALL 60-SIF-500 devices.

"SIL verification" RESULTs (Low Demand System)					
Total PFDavg	**Total RRF**	**Total % WC**	**Effective SIL rating by**		
			IEC-61508	**MSSDL**	**Route 1H**
6.93E-04	1444	100.0%	SIL 3 **(4)**	SIL 3 **(5)**	SIL 3 **(3)**

Verified SIF's SIL rating : SIL 3 **Note 2**

Notes	
2	Minimum Verified SIF's SIL rating among calculated values from IEC-61508, MSSDL and Route 1H.
3	Minimum SIL rating among the above listed maximum SIL ratings to CLAIM by "Route 1H".
4	Verified SIF's SIL rating according to IEC-61508.
5	"PFDavg" design limit for SIL target @ 70% MSSDL is : 7.30E-04 [1 / y]

Table of Contents

1. Document purpose

The purpose of this sample document is to show in the public domain a typical "SIL verification assessment and report", developed by **LIUTAIO** "Functional Safety Services"

For preparing this SAMPLE report:

a) Examples of industrial processes and typical process data was used in combination with **LIUTAIO** experience.

b) "Safety Requirements Specification" (SRS) was developed according to reference [4], 0418D20SD04 Safeguarding requirements - Sample Document, Rev.01.

However, **LIUTAIO** is a professional and serious company and when this report is prepared for a CUSTOMER, only the authorized or provided information by CUSTOMER will be used, and the report **WILL NOT BE** part of the public domain.

2. Abbreviations

Refer to sample document: 0418D10SD01 Abbreviations

This document additional abbreviations are:

GPP	Gas Processing Plant
LDS	Letdown Station
FCR	Field Control Room
LCR	Local Control Room

3. Glossary

Refer to sample document: 0418D10SD02 Glossary

4. References

[1] **LIUTAIO** – Functional Safety Services
0418D10SD01 Abbreviations - Sample Document
Rev.01

[2] **LIUTAIO** – Functional Safety Services
0418D10SD02 Glossary - Sample Document
Rev.01

[3] **LIUTAIO** – Functional Safety Services
0418D18SD03 SIF General Design Background - Sample Document
Rev.01

[4] **LIUTAIO** – Functional Safety Services
0418D20SD04 Safeguarding requirements - Sample Document
Rev.01

[5] **LIUTAIO** – Functional Safety Services
0418E30SD09 Conceptual SRS – Letdown Station - Sample Document
Rev.02

[6] Stein Hauge, Solfrid Håbrekke and Mary Ann Lundteigen
Reliability Prediction Method for Safety Instrumented Systems – PDS Example collection, 2010 Edition
SINTEF Technology and Society, Safety Research, 2010-12-14

5. SIL verification assessment

5.1 SIF Description

Refer to sections 5.1, 5.2 & 5.3, document (reference [5]) 0418E30SD09 Conceptual SRS – Letdown Station

5.2 Safety integrity targets, constraints and other requirements

5.2.1 Safety integrity targets

Table 1– 60-SIF-500 Safety integrity targets

(Low Demand System)

SIF's Tag number	60-SIF-500	**SIL Verification Report No.**	0418E30SD10
SIF's Description	Gas Processing Plant inlet facilities protection against an overpressure operation scenario		
Process Safety Time (PST)	30 sec	**SIF Response Time (SRT, MART)**	15 sec
Target SIL rating	**SIL 3**	**Maximum SIL Safety Design Limit (MSSDL)**	70%

For "Initiators" and Trip settings, refer to Table 11.

5.2.2 SIL verification Constraints, default values and other requirements

Table 2 shows typical constraints and default values for "SIL verification".

Table 2 - 60-SIF-500 SIL verification Constraints and default values

No.	Description	Abbreviation	Default value	Constraint value	Remark
1	Proof Test Period	TI	12 months	≥ 4 months	
2			12 months	≥ 6 months	For All QSV and ESV valves
3	Service Life	SLf	10 years		
4	Mean Time To Restoration	MTTR	72 hours	≥ 72 hours	
5	Proof Test Duration	TD	4 hours	≥ 4 hours	
6	Mean Repair Time	MRT	24 hours	≥ 24 hours	

Other constraints shall include:

1) Regarding to calculation of Beta values for "Common Cause Failure" (CCF) effect:
   a) For any "**Decision Logic**" or "**Safety Channel Architecture**" (SCA) equal to "XooN(D)" (N>X and N>1), the CCF effect **MUST BE** calculated. ZERO(0.0) values **ARE NOT** accepted for CCF effect and respective Beta (β) values.

      CCF effect is ZERO(0.0) ONLY for "NooN" logic.

   b) Default methodology to calculate Beta values for "Common Cause Failure" (CCF) effect shall be IEC-61508-6, Annex D.

   c) To estimate the CCF effect the "Geometric Average" is the default method to estimate the combined failure rates from devices.

      In a group of devices to consider for CCF effect calculation, when one (or some) of them has (have) failure rate (λDD, or LdDD) value(s) equal to ZERO(0.0) and other devices **DO NOT**, then the "Maximum" values of the Failure rates will be used instead, in order to properly consider those devices effect on the verified SIL rating.

   d) When devices with different "Proof Test Periods" (TI) are involved in the same "Proof Test", the CCF effect calculation **MUST BE** done to force the CCF's TI to meet each device's TI value.

5.2.3 Other requirements

Other requirements for this SIL verification assessment are described in the following list:

1) "SIL verification" calculations **MUST** consider individual failures of all devices, as well as all possible combined failures, that will make 60-SIF-500 to fail on demand.
2) By default, "SIL verification" shall consider "Fault Detection Capabilities" (Diagnostics) for "Common Logic Solver" (CommonLS) and Input/Output cards.
3) If target SIL rating is no satisfied, propose possible actions/solutions to improve the design of 60-SIF-500.
4) Using IEC-61508-6, Annex D, it is possible to calculate the following "Beta" value cases:
   - SIF **simple** Design/Installation quality is representative of high Beta values (or Worst values).
   - SIF **enhanced** Design/Installation quality is representative of low Beta values (or best values).

   And, "SIL verification" shall be developed by calculating and reporting "Beta" values (β, β_D) corresponding to BOTH the **Simple** (Greater CCF effect) and the **Enhanced** (Lower CCF effect) SIF's Design/Installation cases.
5) Verify SIL rating in the cases of SIF's **simple** and **enhanced** implementation quality, but with NO Maintenance effect (MTTR, TD, MRT all equal to 0.0 hours).
6) Verify SIL rating in the same condition as described in above point No.5), but including Maintenance effect (MTTR, TD, MRT).
7) For above point No.6), calculate the SIF's "STRavg" (and "MTTRspurious") in the following cases:
   a) When during normal operation, a "Spurious Trip" occurs in one(1) pipe run.
   b) When during normal operation, a "Spurious Trip" occurs in two(2) pipe runs (**NOT** necessarily at the same time).
8) Recalculate "PFDavg", "STRavg" and "MTTFspurious" for one of the proposed point No.2 actions/solutions.
9) Since the "Letdown Station" (LDS) can operate with one pipe run "Out of Service" (OOS, for MAINTENANCE purposes), verify that still 60-SIF-500 satisfy the target SIL rating with three(3) pipe runs in operation in 2oo3 configuration.

   NOTE: in this case, use the same beta values that were used for 3oo4 configuration.
10) Repeat calculation above in point No.7) for point No.9), to determine SIF's "STRavg" (and "MTTRspurious") for 3 pipe runs in operation in 2oo3 configuration.

    NOTE: in this case, use the same beta values that were used for 3oo4 configuration.

5.3 Premises and Assumptions

1) Refer to below section 5.9 for SIF Devices' List and data for "SIL verification" (after Reliability Data Validation).

2) Input cards **SHALL NOT** work in 1oo1D architecture. When a "Detected Failure" occurs in the input card, DCS (Console Operator) shall be notified and automatic MOS applies. BUT, any way related ESV shall trip after MTTR time if failure **IS NOT** repaired/fixed.

3) The "Common Logic Solver" (CommonLS) shall work in 1oo1D architecture, so when a "Detected Failure" (Safe or Dangerous) occurs in the "CommomLS", the SIF implementation shall initiate "Spurious Trips" of all QSV and ESV valves to **DO NOT** compromise safety. Refer to reference [5, SRS], section 5.16.3.

4) Since the "Common Logic Solver" (CommonLS) is connected to trip all ESVs, ONLY a "Dangerous UnDetected" failure is enough in "CommonLS" to make both 60-SIF-500 and 60-SIF-510 to fail on demand.

5) Output cards shall work in 1oo1D architecture, so when a "Detected Failure" (Safe or Dangerous) occurs in the Output Card, the SIF implementation shall initiate "Spurious Trip" of the related ESV valve to **DO NOT** compromise safety in the related pipe run. Refer to reference [5, SRS], section 5.16.3.

6) The "PFDavg" calculation methodology considers failures in any independent device in the safety channel that will trip a QSV or ESV valve.

   The "CommonLS" is also present in the four(4) safety channels that will trip QSV valves. Refer to High Priority Trip 60-SIF-510 in section 5.3 & 5.9, document (reference [5]) 0418E30SD09 Conceptual SRS – Letdown Station.

   BUT, a "CommonLS" "Dangerous UnDetected" failure **WILL NOT** make STAs to fail on demand to trip QSV valves. For all other failure types, "CommonLS" will initiate a "Spurious Trip".

   It **DOES NOT** have sense to include the "CommonLS" as an independent device on each of the indicated four(4) channels to Trip EDV valves, because "CommonLS" is just one device, **NOT** four(4).

   To take into account that a "Dangerous Undetected" failure in the "CommonLS" shall affect four(4) safety channels to trip ESV valves, this logic solver is included in the RBD for SIF's "PFDavg" calculation as a 4oo4 architecture to consider its high contribution to "PFDavg".

7) Regarding the following input channel devices:
   - Pressure transmitters 60-PT-510/520/530/540 and 60-PT-511/521/531/541,
   - Input isolators 60-XIB-510/520/530/540 and 60-XIB-511/521/531/541,

   The following requirement and fact apply:
   a) Each device shall be configured to set its output in SAFE state when a "Detected Failure" happens (NAMUR NE 43), and
   b) Any of those devices IS NOT physically capable to perform a 1oo1D architecture.

   However, the "Safety Trip Alarm" 60-STA-511/521/531/541 is capable to avoid spurious trips from input channel device in "Detected Failure" condition (via NAMIUR NE 43).

8) About calculation of SIF's "PFDavg":
   a) 4oo4 architecture will be used from above point No.6 to calculate "CommonLS" contribution to "PDFavg".
   b) 2oo2 architecture will be used to calculate all pairs QSV-ESV valves contribution to "PDFavg" to consider that both valves shall close for successful gas flow cut-off through a pipe run.
   c) Each "Output Card" that handles the High Priority Trip 60-SIF-510 of the related QSV valve, **DOES NOT** contribute to the SIF's "PFDavg", because a "Dangerous Failure" in this card **DOES NOT** make 60-SIF-500 to fail on demand to trip QSV valves.

9) About calculation of SIF's "STRavg":
   a) The 4oo4 architecture from above point No.6 has a very low "STRavg", typical for an architecture where four(4) devices shall have a "Spurious Tip" to trip all ESVs. This **IS NOT** the case for "CommonLS" since it is only one(1) device.
   b) Even though both safety valves per pipe run shall close (2oo2) to considered that high-pressure gas flow through the pipe run was cut-off successfully, a "Spurious Trip" occurs if only one(1) safety valve closes (1oo2).
   c) The High Priority Trip 60-SIF-510 can trip ALL safety valves in the LDS through "CommonLS". So, a CommonLS "Safe Failure" can initiate a "Spurious Trip" of ALL LDS safety valves.
   d) "Output Card" to handle the High Priority Trip 60-SIF-510 of the related QSV valve, contributes to the SIF's "STRavg", but **NO** effect for "PFDavg".

   From the above "a" to "c" statements, the following apply for SIF's "STRavg" calculation:
   - The "CommonLS" shall be considered as a 1oo8 architecture, to take into account the fact that only one device "Safe Failurre" will initiate a "Spurious Tip" on eight(8) safety valves (QSVs and ESVs).
   - The two(2) series of devices that trip the QSV and ESV valves, respectively, shall be considered as a 1oo2 architecture (instead of 2oo2 as for "PFDavg"), because a "Spurious Trip" happens if only one(1) valve closes.

   Refer to "APPENDIX B" for adjusted RBD for "STRavg" calculation.

5.4 Reliability data validation (RDV)

Refer to:

a) Below section 5.9 for the 60-SIF-500 Devices' data for "SIL verification" (after Reliability Data Validation).
b) 60-SIF-500 GPP high-pressure protection, SIF detailed diagram in "APPENDIX B" in document (reference [5]) 0418E30SD09 Conceptual SRS – Letdown Station.
c) 60-SIF-500 Reliability Block Diagram in "APPENDIX A".

This section is organized in the following sub-sections:

1) Use of fault detection capabilities in the 60-SIF-500 design
2) "Initiators", "Input isolators", "Safety Trip Alarm" (STA) and Output isolators to trip QSVs.
3) "Initiators", Input isolators, "Input cards" and "CommonLS" to trip ESVs.
4) Output isolators to trip ESVs.
5) High priority trip 60-SIF-510.

5.4.1 Use of fault detection capabilities in the 60-SIF-500 design

After reviewing the 60-SIF-500 SRS (reference [5]), it is confirmed that this SIF design uses fault detection capabilities of ALL SIF devices, except for the safety valves (QSV and ESV) and solenoid valves.

This fact is indicated in in below section 5.9, Table 12, column "B".

5.4.2 "Initiators", "Input isolators", "Safety Trip Alarm" (STA) and Output isolators to trip QSVs

From SRS (reference [5]), it is indicated in Table 12 that the devices:

- Pressure transmitters (PTs) 60-PT-511/521/531/541,
- Input isolators 60-XIB-511/521/531/541,

have fault detection capabilities (Diagnostics), and use NAMUR NE43 to indicate to all other downstream SIF devices when "Detected Failures" occurs in the referred device.

As indicated in 60-SIF-500 design, section 5.6 & 5.11 in document (reference [5]) 0418E30SD09 Conceptual SRS – Letdown Station, these devices **WILL NOT** initiate a SIF demand when a "Detected Failure" occurs.

In addition, the "Safety Trip Alarms" (STA) 60-STA-511/521/531/541 modules also include input failure detection (NAMUR NE 43) and "Dangerous Detected" failures detection. So, when a "Detected Failure" occurs in an "Initiator" or input isolator, the STA module can differentiate a trip from failure condition in order to avoid QSV valves spurious trips.

Data Validation statement:

"SIL verification" confirms it is acceptable the design decisions to avoid QSV valve "Spurious Trip" when the related "Initiator", "Input Isolator" and STA module is detected in failure. Refer to section 5.16.1 in document (reference [5]) 0418E30SD09 Conceptual SRS – Letdown Station.

This design decision:

a) Is indicated in in below section 5.9, Table 12, column "T".
b) Will allow 60-SIF-500 to identify a "Dangerous Detected" in any of the above listed devices, and to keep GPP protected in this case.
c) On PTs, input isolators and STA modules, "Detected Failures" **HAS NO** effect on "PFDavg (SIL rating) and "STRavg" (Spurious trips). So, design decision:
    - Avoids "Spurious Trips" from SD and DD failures (from Initiators, Input isolators and STAs).
    - Increases "PFDavg", equivalent to decrease SIL rating, and
    - Decreases 60-SIF-500 "STRavg", equivalent to increase the "MTTFspuriously".

5.4.3 "Initiators", Input isolators, "Input cards" and "CommonLS" to trip ESVs

From SRS (reference [5]), it is indicated in Table 12 that the devices:

- Pressure transmitters (PTs) 60-PT-510/520/530/540, and
- Input isolators 60-XIB-510/520/530/540,

have fault detection capabilities (Diagnostics), and use NAMUR NE 43 to indicate to all other downstream SIF devices when "Detected Failures" occurs in the referred device.

As indicated in 60-SIF-500 design, section 5.6 & 5.11 in document (reference [5]) 0418E30SD09 Conceptual SRS – Letdown Station, these devices **WILL NOT** initiate a SIF demand when a "Detected Failure" occurs.

NAMUR NE 43 will allow "Input card" detect "Detected Failure" in input channel, and logic in "CommonLS" **WILL NOT** trip the related safety valves

Data Validation statement:

"SIL verification" confirms it is acceptable the design decisions to avoid ESV valve "Spurious Trip" when the related "Initiator", "Input Isolator" and "Input Card" module is detected in failure. Refer to section 5.16.2 in document (reference [5]) 0418E30SD09 Conceptual SRS – Letdown Station.

This design decision:

a) Is indicated in in below section 5.9, Table 12, column "T".
b) Will allow 60-SIF-500 to identify a "Dangerous Detected" in any of the above listed devices, and to keep GPP protected in this case.
d) On PTs and input isolators, "Detected Failures" **HAS NO** effect on "PFDavg (SIL rating) and "STRavg" (Spurious trips). So, design decision:
    - Avoids "Spurious Trips" from SD and DD failures (from Initiators, Input isolators and input cards).
    - Increases "PFDavg", equivalent to decrease SIL rating, and
    - Decreases 60-SIF-500 "STRavg", equivalent to increase the "MTTFspuriusly".

5.4.4 Output isolators to trip ESVs

From SRS (reference [5]), it is indicated in below section 5.9, Table 12, column "B" that the "Output Isolators" 60-XOB-511/521/531/541 have fault detection capabilities (Diagnostics),

And, the "Output Isolator" is capable to use diagnostics to De-Energize output to trip the related QSV valve when a "Detected Failure" occurs in this device (see below section 5.9, Table 12, column "T").

Data Validation statement:

"SIL verification" confirms it is acceptable the design decisions for "Output Isolators", because there is no way to avoid "Spurious Trips" from a failure in this device, and this design decision **DOES NOT** compromise safety.

This design decision:

a) **DOES NOT** compromise safety, because in case of "Detected Failures" there **WILL NOT** be possibility to lose trip command to the ESV valves and GPP. So, GPP is always protected.

b) On "Output Isolators", "Detected Failures" (Safe & Dangerous) will always initiate a "Spurious Trip". So, design decision:

- Decreases "PFDavg", equivalent to increase SIL rating,
- BUT, increases 60-SIF-500 "STRavg", equivalent to decrease the "MTTFspuriously".

5.4.5 High priority trip 60-SIF-510

From section 5.9 in document (reference [5]) 0418E30SD09 Conceptual SRS – Letdown Station, it is a design decision to allow the higher priority 60-SIF-510 to initiate a demand in the 60-SIF-500 to close (SAFE state) ALL safety valves in the LDS (both ESVs and QSVs).

Data Validation statement:

"SIL verification" confirms it is acceptable the above described design decision to support the plant safety trip hierarchy:

a) By transferring TRIP command from 60-SIF-510 to all ESV valves, via "CommomLS", and
b) By including four(4) additional output cards in "CommonLS" to transfer TRIP command from 60-SIF-510 to all QSV valves.

This design decision:

a) **HAS NO** effect to in the "PFDavg", and SIL rating **IS NOT** affected.
b) BUT, it is in favor to increase the 60-SIF-500 "STRavg", equivalent to decrease the "MTTFspuriously".

5.5 Reliability Block Diagram (RBD)

The Reliability Block Diagram (RBD) shows the 60-SIF-500 Devices' interactions and contributions to make this SIF to fail on demand.

Refer to:

- "APPENDIX A" for RBD to calculate "PFDavg".
- "APPENDIX B" for RBD to calculate "STRavg".

5.6 Assessment results

(Low Demand System)			
SIF's Tag number	60-SIF-500	**SIL Verification Report No.**	0418E30SD10
SIF's Description	Gas Processing Plant inlet facilities protection against an overpressure operation scenario		
Process Safety Time (PST)	30 sec	**SIF Response Time (SRT, MART)**	15 sec
Target SIL rating	**SIL 3**	**Maximum SIL Safety Design Limit (MSSDL)**	70%
Verified SIL rating	**SIL 1**	**SIF's Service Life period (SLf)**	10 years

NOTE: refer to below section 5.9 for "SIF Devices' List and data for "SIL verification" (after Reliability Data Validation).

The purpose of this "SIL verification" report was to execute a preliminary assessment of the 60-SIF-500 design, considering Simple/Enhanced design/installation, Maintenance times (MTR, TD, MRT), and the SIF Devices fault detection capabilities (Diagnostics) that were used in the design.

The "SIL verification" assessment RESULTS were:

1) 60-SIF-500 design, as described in document (reference [5]) "0418E30SD09 Conceptual SRS – Letdown Station", **is capable to satisfy "SIL 1" rating, instead of target "SIL 3" rating**. "Proof Test" 6 months. See Table 3.

2) The main reason to **DO NOT** reach the target SIL rating is the "SIL a" qualification by "Safe Failure Fraction" (SFF) of ALL safety valves (QSV and ESV). This fact allows 60-SIF-500 to claim ONLY up to "SIL 1" rating. Refer to Table 3 and Figure 3.

3) **The following action is required to make 60-SIF-500 to satisfy target "SIL 3" rating**:

   a) Change ALL safety valves (QSV and ESV) for valves capable to claim for up to "SIL 2" rating according to SFF.

To verify the above indicated action, reliability data in Table 12 was used, and the results were:

4) "Proof Test" shall be executed every 7 months for ALL 60-SIF-500 devices.

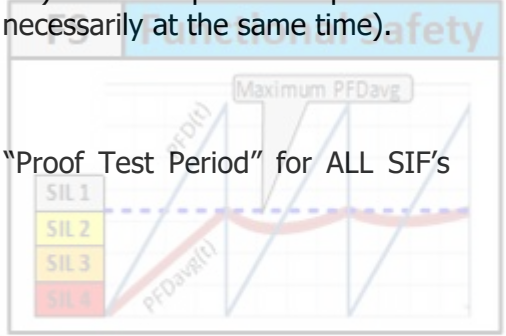
5) 60-SIF-500 will be capable to claim up to "SIL 3" rating, and to perform with "PFDavg" 6.87E-04 1/y, and:

   a) "STRavg" 1.64E-03 1/y (MTTFspuriously 6.1 years) when a "Spurious Trip" occurs in one(1) pipe run only.

   b) "STRavg" 2.50E-03 1/y (MTTFspuriously 400.3 years) when a "Spurious Trip" occurs in two(2) pipe runs, one after the other one (not necessarily at the same time).

Refer to Table 4 for further details.

6) Figure 4 shows the PFDavg/PFD(t) graph 7 months "Proof Test Period" for ALL SIF's devices, 4 pipe runs in operation (3oo4).



7) The 60-SIF-500 "Proof Test Period" (TI) was verified in the range 6-10 months.

From this verification, it was found that Maintenance effect (MTTR, TD, MRT) impact on 60-SIF-500 is negligible when SIL rating (PFDavg, STRavg) was verified. CCF has a bigger impact in 60-SIF-500 SIL rating.

Refer to:

- Table 5 for numeric results about "PFDavg" & "STRavg", and
- Figure 2 for graphic results.

8) Calculated "Beta" (β & βD) values for the cases of **Simple** (Greater CCF effect) and **Enhanced** (Lower CCF effect) SIF's design/Installation are as reported in Table 6. Refer to "Reliability Block Diagram" (RBD) in "APPENDIX A" and "APPENDIX B".

9) If it is required to increase the SIF "Proof Test" period, the project team can improve the 60-SIF-500 installation quality, which effect will be to decrease the "Common Cause Failure" (CCF) effect. For example:

- 19% quality improvement will allow to increase "Proof Test" to every 8 months (CCF beta value reduction for 3oo4 from 17.5% to 14.43%).
- 46% quality improvement will allow to increase "Proof Test" to every 9 months (CCF beta value reduction for 3oo4 from 17.5% to 10.24%).
- 71% quality improvement will allow to increase "Proof Test" to every 10 months (CCF beta value reduction for 3oo4 from 17.5% to 6.36%).
- 94% quality improvement will allow to increase "Proof Test" to every 9 months (CCF beta value reduction for 3oo4 from 17.5% to 2.64%).

Refer to Figure 2 for further details.

Design team shall review IEC-61508-6, Annex D, to identify measures to improve 60-SIF-500 design/installation quality.

10) For only three(3) pipe runs in operation, 60-SIF-500 will be capable to claim up to "SIL 3" rating, and to perform with "PFDavg" 5.98E-04 1/y, and:

a) "STRavg" 1.29E-01 1/y (MTTFspuriously 7.7 years) when a "Spurious Trip" occurs in one(1) pipe run only.

b) "STRavg" 7.15E-03 1/y (MTTFspuriously 139.8 years) when a "Spurious Trip" occurs in two(2) pipe runs, one after the other one (not necessarily at the same time).

Refer to Figure 1 for graphic details.

Table 3 – "SIL Verification" detailed results for 6 months "Proof Test"

SIL Rating Results original data, 6 months "Proof Test" (SIF Simple implementation)							
#	Independent contributions to PFDavg (Note 1)	PFDavg [1/y] (6.b)	RRF	%WC	SIL by IEC-61508	SIL by MSSDL	SIL by Route 1H
1	Initiators	5.65E-05	17562	8.64%	SIL 4	Above SIL 2	Note 6.a
2	Input Channles	3.33E-05	29832	5.09%	SIL 4		
3	Safety Trip Alarm (STA) modules	1.99E-05	49867	3.04%	SIL 4		
4	Common Logic Solver (CommonLS)	8.35E-07	1188003	0.13%	SIL 4	PFDavg Design Limit 7.30E-04	
5	Output Channels	6.14E-05	16166	9.38%	SIL 4		
6	Safety valves	4.82E-04	2058	73.72%	SIL 3	Below SIL 3	

Total PFDavg	Total RRF	Total % WC	Effective SIL rating by		
			IEC-61508	MSSDL	Route 1H
6.59E-04	1517	100.00%	SIL 3 **(4)**	SIL 3 **(5)**	SIL 1 **(3)**

Verified SIF's SIL rating : **SIL 1** **Note 2**

STR Rating Results original data (SIF Simple implementation)							
#	Independent contributions to STRavg (Note 1)	One(1) pipe run "Spurious Trip"			Two(2) pipe runs "Spurious Trip"		
		STRavg [1 / y](6.b)	%WC	MTTFSpuriously [years]	STRavg [1 / y](6.b)	%WC	MTTFSpuriously [years]
1	Initiators	3.29E-03	2.16%	304	1.39E-04	2.16%	7199
2	Input Channels	6.00E-03	3.93%	167	2.53E-04	3.93%	3951
3	Safety Trip Alarm (STA) modules	1.05E-02	6.89%	95	4.43E-04	6.89%	2256
4	Common Logic Solver (CommonLS)	4.80E-02	31.51%	21	2.03E-03	31.51%	493
5	Output Channels	3.66E-02	24.01%	27	1.54E-03	24.01%	647
6	Safety valves	0.0	0.00%	- Never -	0.0	0.00%	- Never -
7	60-SIF-510 Output Card to QSV	4.80E-02	31.51%	21	2.03E-03	31.51%	493

Total STRavg	Total % WC	Total MTTFSpuriously	Total STRavg	Total % WC	Total MTTFSpuriously
1.52E-01	100.00%	6.6	6.44E-03	100.00%	155.4

Notes	
1	Refer to Reliability Block Diagram (RBD) in "APPENDIX A".
2	Minimum Verified SIF's SIL rating among calculated values from IEC-61508, MSSDL and Route 1H.
3	Minimum SIL rating among the above listed maximum SIL ratings to CLAIM by "Route 1H".
4	Verified SIF's SIL rating according to IEC-60508.
5	"PFDavg" design limit for SIL target @ 70% MSSDL is : 7.30E-04 [1 / y]
6	From RBD (APPENDIX A) there are no individual contributions to "PFDavg", only one. So: a) It is not possible indicate SIL rating by "Route 1H". b) Estimated values to show a reasonable contribution to "PFDavg" of SIF's devices.

Table 4 - "SIL Verification" detailed results for 8 months "Proof Test" and SIL-2 valves, after application of actions on above point No.3

SIL Rating Results 7 months "Proof Test" w/SIL-2 valves (SIF Simple implementation)							
#	Independent contributions to PFDavg (Note 1)	PFDavg [1/y] (6.b)	RRF	%WC	SIL by IEC-61508	SIL by MSSDL	SIL by Route 1H
1	Initiators	3.89E-05	25739	5.61%	SIL 4	Above SIL 2	
2	Input Channles	2.29E-05	43722	3.30%	SIL 4		
3	Safety Trip Alarm (STA) modules	1.37E-05	73087	1.98%	SIL 4		
4	Common Logic Solver (CommonLS)	5.74E-07	1741182	0.08%	SIL 4	**PFDavg Design Limit 7.30E-04**	**Note 6.a**
5	Output Channels	4.22E-05	23693	6.09%	SIL 4		
6	Safety valves	5.74E-04	1741	82.93%	SIL 3	Below SIL 3	

Total PFDavg	Total RRF	Total % WC	Effective SIL rating by		
			IEC-61508	MSSDL	Route 1H
6.93E-04	1444	100.00%	SIL 3 **(4)**	SIL 3 **(5)**	SIL 3 **(3)**

Verified SIF's SIL rating : SIL 3 **Note 2**

STR Rating Results 7 months "Proof Test" w/SIL-2 valves (SIF Simple implementation)								
#	Independent contributions to STRavg (Note 1)	One(1) pipe run "Spurious Trip"			Two(2) pipe runs "Spurious Trip"		
		STRavg [1 / y](6.b)	%WC	MTTFSpuriously [years]	STRavg [1 / y](6.b)	%WC	MTTFSpuriously [years]
1	Initiators	3.36E-03	1.98%	298	1.42E-04	1.98%	7049
2	Input Channels	6.12E-03	3.60%	163	2.59E-04	3.60%	3868
3	Safety Trip Alarm (STA) modules	1.07E-02	6.31%	93	4.53E-04	6.31%	2209
4	Common Logic Solver (CommonLS)	4.90E-02	28.84%	20	2.07E-03	28.84%	483
5	Output Channels	3.76E-02	22.12%	27	1.59E-03	22.12%	630
6	Safety valves	1.33E-02	7.83%	75	5.62E-04	7.83%	1779
7	60-SIF-510 Output Card to QSV	4.98E-02	29.33%	20	2.11E-03	29.33%	475
		Total STRavg	**Total % WC**	**Total MTTFSpuriously**	**Total STRavg**	**Total % WC**	**Total MTTFSpuriously**
		1.70E-01	100.00%	5.9	7.18E-03	100.00%	139.3

Notes	
1	Refer to Reliability Block Diagram (RBD) in "APPENDIX A".
2	Minimum Verified SIF's SIL rating among calculated values from IEC-61508, MSSDL and Route 1H.
3	Minimum SIL rating among the above listed maximum SIL ratings to CLAIM by "Route 1H".
4	Verified SIF's SIL rating according to IEC-60508.
5	"PFDavg" design limit for SIL target @ 70% MSSDL is : 7.30E-04 [1 / y]
6	From RBD (APPENDIX A) there are no individual contributions to "PFDavg", only one. So: a) It is not possible indicate SIL rating by "Route 1H". b) Estimated values to show a reasonable contribution to "PFDavg" of SIF's devices.

Table 5 – Calculated PFDavg/STRavg values w/SIL-2 valves, Simple/Enhance implementation, with and without Maintenance effect

	Tested TI values [months]	Calculated PFDavg and STRavg values [1 / y]							
		NO Maintenance Effect				WITH Maintenance Effect (MTTR, TD, MRT)			
		CCF Simple Quality		CCF Enhanced Quality		CCF Simple Quality		CCF Enhanced Quality	
		PFDavg	STRavg (MTTFsp)	PFDavg	STRavg (MTTFsp)	PFDavg	STRavg (MTTFsp)	PFDavg	STRavg (MTTFsp)
1	6	5.60E-04		2.29E-04		5.69E-04	**(1)** 1.70E-01 (5.9 y)	2.30E-04	**(1)** 1.64E-01 (6.1 y)
2	7	6.77E-04		3.02E-04		6.87E-04		3.03E-04	
3	8	8.02E-04		3.86E-04		8.12E-04		3.87E-04	
4	9	9.35E-04		4.80E-04		9.44E-04	**(2)** 7.18E-03 (139.3 y)	4.81E-04	**(2)** 7.68E-04 (1302.0 y)
5	10	1.07E-03		5.80E-04		1.07E-03		5.80E-04	

Note 1: One(1) pipe run "Spurious Trip". **Note 2:** Two(2) pipe runs "Spurious Trip".

Figure 1 – Graphic results for 60-SIF-500 "PFDavg" review in the 7-11 months "Proof Test" range, 3 pipe runs in operation (2oo3)

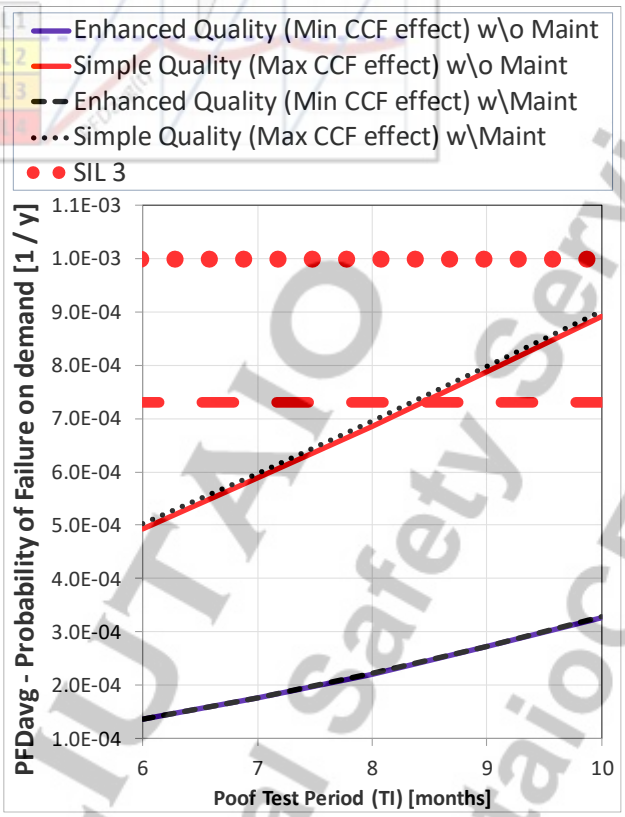


Figure 2 - Graphic results for 60-SIF-500 "PFDavg" review in the 6-10 months "Proof Test" range, 4 pipe runs in operation (3oo4)

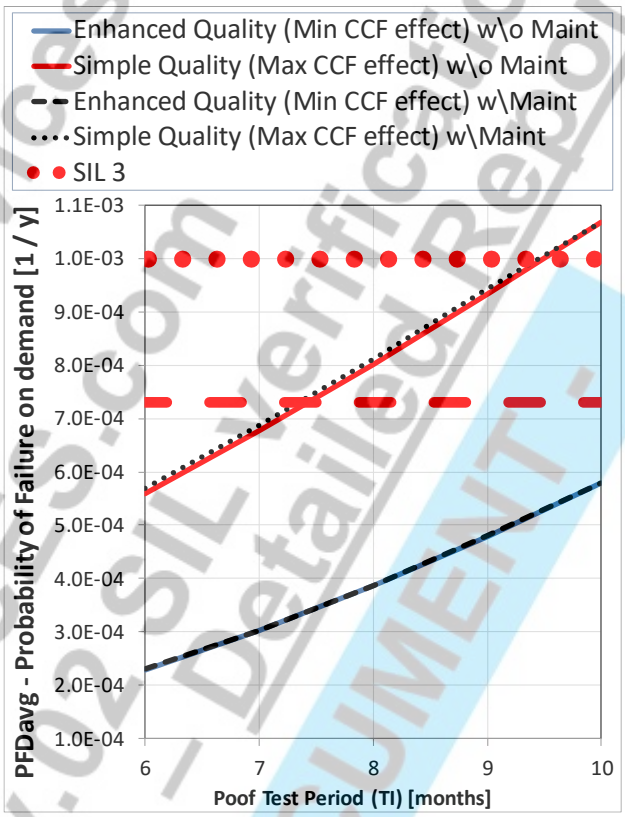


Table 6 - Calculated "Beta" values for the cases of Simple (Greater CCF effect) and Enhanced (Lower CCF effect) SIF design/installation

#	Safety Architecture	Use description	Calculation use	CCF Effect calculate Beta values			
				Enhanced Design		Simple Design	
				Beta(β)	BetaD(β_D)	Beta(β)	BetaD(β_D)
1	3oo4	Whole "Letdown Station" (LDS) "Decision Logic" to trip at least 3 of 4 pipe runs	PFD (SIL) & STR	1.75 %	1.75 %	17.50 %	17.50 %
2	1oo2	"Decision Logic" to quantify the "Spurious Trip" of one(1) valve in a pipe run.	STR only	0.10 %	0.10 %	10.00 %	10.00 %
3	1oo8	"Common Logic Solver" (CommoLS) contribution to calculate "STRavg" of the whole LDS.	STR only	0.15 %	0.15 %	1.50 %	1.50 %

Figure 3 – 60-SIF-500 PFDavg/PFD(t) graph 6 months "Proof Test Period" for ALL SIF's devices, 4 pipe runs in operation (3oo4)

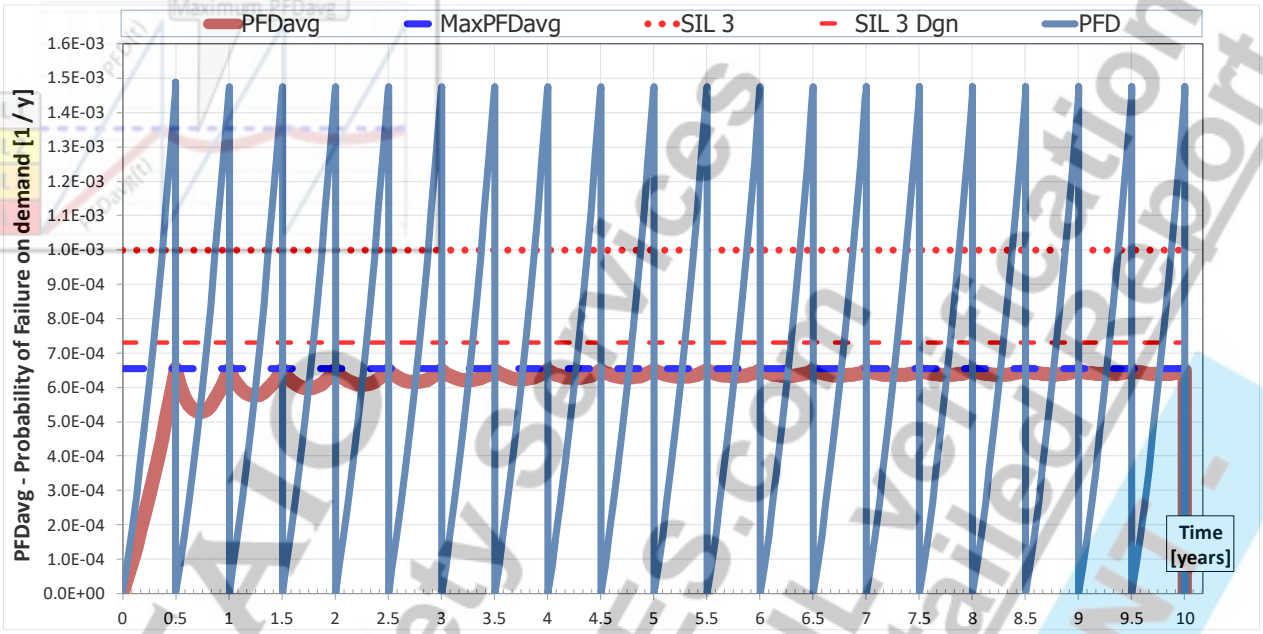
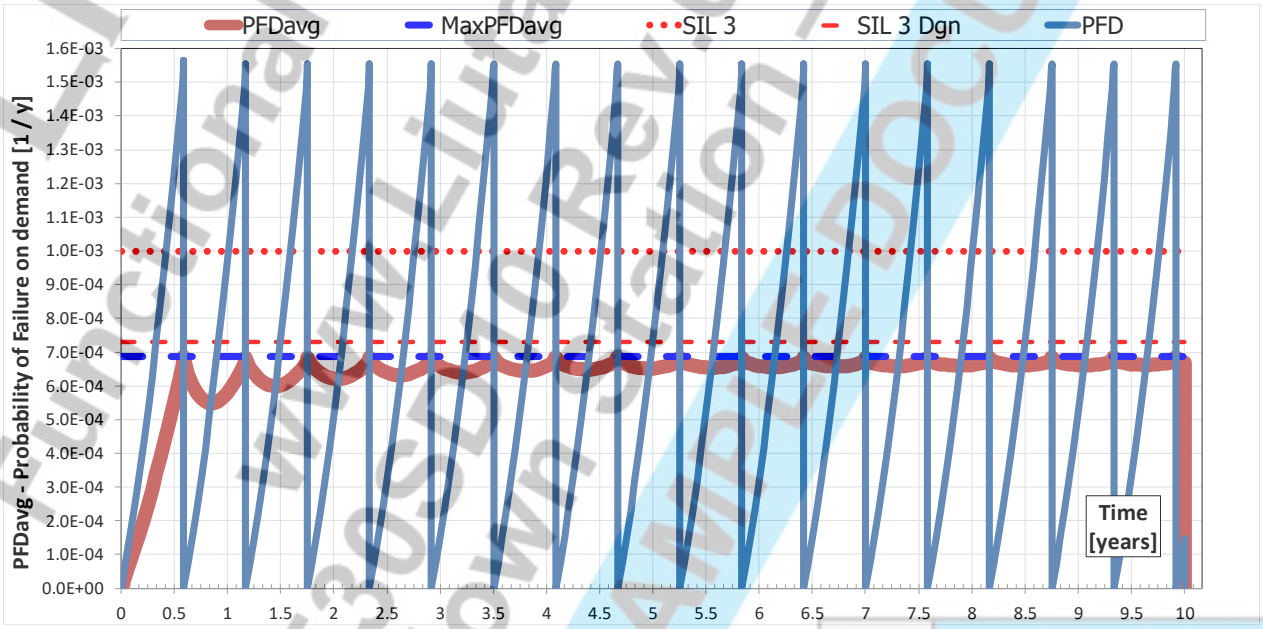


Figure 4 – 60-SIF-500 PFDavg/PFD(t) graph 7 months "Proof Test Period" for ALL SIF's devices, 4 pipe runs in operation (3oo4), after application of actions on above point No.3



5.7 (FMEA) Failure Modes and Effects Analysis

Individual device Failure modes and effects are listed in Table 7 and Table 8.

Table 7 - 60-SIF-500 list of failure modes and effects of each individual device related to trip a QSV valve

	Device / Short Desc	Normal Operation	Failure mode	Failure Effect on SIF	Failure Type	Diagnostic
Safety Channel to trip a QSV valve						
SIF Initiators						
01	60-PT-511 60-PT-521 60-PT-531 60-PT-541 Pressure transmitter	LDS downstream pressure lesser than 8.5 Bar(g)	• Miscalibration. • Plugged impulse pipe. • HV closed	Fail on demand to trip related QSV.	Dangerous UnDetected	None. Only revealed by Proof test.
02			• Software failure. • Electronic failure. • Broken membrane.	**No effect.** DCS (Console Operator) is notified and automatic MOS applies. **BUT**, QSV shall trip after MTTR.	Dangerous Detected , **BUT** implemented as "Safe Detected". See sec.5.4.2	Internal electronic diagnostics.
03			• XIB power failure.		Safe Detected	
04			• UPS Power failure.	TRIP related QSV valve.	Safe UnDetected	
SIF Input channels						
10	60-XIB-511 60-XIB-521 60-XIB-531 60-XIB-541 Input isolator	Input and output signals match measured pressure lesser than 8.5 Bar(g)	• Electronic component.	Fail on demand to trip related QSV.	Dangerous UnDetected	None. Only revealed by Proof test.
11			• Software failure. • Electronic failure.	**No effect.** DCS (Console Operator) is notified and automatic MOS applies. **BUT**, QSV shall trip after MTTR.	Dangerous Detected, **BUT** implemented as "Safe Detected". See sec.5.4.2	Internal electronic diagnostics.
12			• UPS Power failure.	TRIP related QSV valve.	Safe UnDetected	
Safety Trip Alarm (STA)						
20	60-STA-511 60-STA-521 60-STA-531 60-STA-541 Safety Trip Alarm	Working	• Miscalibration.	Fail on demand to trip related QSV.	Dangerous UnDetected	None. Only revealed by Proof test.
21			• Software failure. • Electronic failure.	**No effect.** DCS (Console Operator) is notified and automatic MOS applies. **BUT**, QSV shall trip after MTTR.	Dangerous Detected, **BUT** implemented as "Safe Detected". See sec.5.4.2	Internal electronic diagnostics.
22			• UPS Power failure. • Double relay output failure.	TRIP related QSV valve.	Safe UnDetected	

	Device / Short Desc	Normal Operation	Failure mode	Failure Effect on SIF	Failure Type	Diagnostic
SIF Output Channels						
30	60-XOB-511 60-XOB-521 60-XOB-531 60-XOB-541 Output isolator	Input and output signals match output state from STA module.	• Electronic component.	Fail on demand to trip related QSV.	Dangerous UnDetected	None. Only revealed by Proof test.
31			• Software failure. • Electronic failure.	TRIP related QSV valve.	Dangerous Detected, **BUT** implemented (1oo1D) as "Safe Detected". See sec.5.4.4.	Internal electronic diagnostics.
32			• UPS Power failure.		Safe UnDetected	
33	60-SOV-511 60-SOV-521 60-SOV-531 60-SOV-541 Solenoid valve	SOV is Energized, making instrument air to keep QSV valve in the fully opened position.	• SOV leaking	**No Effect.** BUT after some time QSV valve can open spuriously if leakage increases.	Dangerous UnDetected	None. Only revealed by maintenance or site inspection.
34			• SOV fails to open on demand	Fail on demand to trip related QSV.		
35			• SOV opens due to failure or coil burnout.	TRIP related QSV valve.	Safe UnDetected	
SIF Final Safety Elements (FSE)						
40	60-QSV-511 60-QSV-521 60-QSV-531 60-QSV-541 Quick shutdown valve	Fully opened	• QSV fails to close on demand	Fail on demand to trip related QSV.	Dangerous UnDetected	None. Only revealed by Proof test.
41			• QSV closes but slowly.	Possible fail on demand to trip related QSV.		
42			• QSV leaking	**No Effect.** BUT after some time QSV valve can open spuriously if leakage increases.		None. Only revealed by maintenance or site inspection.

High Priority Trip 60-SIF-510 support to close QSV						
43	OC-60SIF510-01 OC-60SIF510-02 OC-60SIF510-03	Input soft signal (NORMAL state) and 24 VDC output signal (Energized) match.	• Electronic component.	Fail on demand to trip related ESV.	Dangerous UnDetected	None. Only revealed by Proof test.
44	OC-60SIF510-04		• Electronic component. • Defective input/output.	TRIP related QSV valve. DCS (Console Operator) is notified.	Dangerous Detected, **BUT** implemented (1oo1D) as "Safe Detected". See sec.5.3, points No.8 & 9.	Internal electronic diagnostics.
45			• Electronic component.		Safe Detected	
46			• Electronic component. • UPS Power failure.	TRIP related ESV valve.	Safe UnDetected	

Table 8 – 60-SIF-500 list of failure modes and effects of each individual device related to trip an ESV valve

	Device / Short Desc	Normal Operation	Failure mode	Failure Effect	Failure Type	Diagnostic
Safety Channel to trip an ESV valve						
SIF Initiators						
01	60-PT-510 60-PT-520 60-PT-530 60-PT-540	LDS downstream pressure lesser than 8.5 Bar(g)	• Miscalibration. • Plugged impulse pipe. • HV closed	Fail on demand to trip related ESV.	Dangerous UnDetected	None. Only revealed by Proof test.
02	Pressure transmitter		• Software failure. • Electronic failure. • Broken membrane.	**No effect.** DCS (Console Operator) is notified and automatic MOS applies. **BUT**, ESV shall trip after MTTR.	Dangerous Detected, **BUT** implemented as "Safe Detected". See sec.0.	Internal electronic diagnostics.
03			• XIB power failure.		Safe Detected	
04			• UPS Power failure.	TRIP related ESV valve.	Safe UnDetected	
SIF Input Channels						
10	60-XIB-510 60-XIB-520 60-XIB-530 60-XIB-540	Input and output signals match measured pressure lesser than 8.5 Bar(g)	• Electronic component.	Fail on demand to trip related ESV.	Dangerous UnDetected	None. Only revealed by Proof test.
11	Input isolator		• Software failure. • Electronic failure.	**No effect.** DCS (Console Operator) is notified and automatic MOS applies.	Dangerous Detected, **BUT** implemented as "Safe Detected". See sec.0	Internal electronic diagnostics.

	Device / Short Desc	Normal Operation	Failure mode	Failure Effect	Failure Type	Diagnostic
				BUT, ESV shall trip after MTTR.		
12			• UPS Power failure.	TRIP related ESV valve.	Safe UnDetected	
	"CommonLS" – Common Logic Solver					
20	IC-60-PT-510 IC-60-PT-520 IC-60-PT-530 IC-60-PT-540	Input HART signal and output soft signal match measured pressure lesser than 8.5 Bar(g)	• Electronic component.	Fail on demand to trip related ESV.	Dangerous UnDetected	None. Only revealed by Proof test.
21	Input cards		• Electronic component. • Defective input/output.	**No effect.** DCS (Console Operator) is notified and automatic MOS applies. **BUT**, ESV shall trip after MTTR.	Dangerous Detected	Internal electronic diagnostics.
22			• Electronic component.		Safe Detected, **BUT** implemented (1oo1D) as "Dangerous Detected". See section 5.4.3	
23			• Electronic component. • UPS Power failure.	TRIP related ESV valve.	Safe UnDetected	
30	CommonLS "Common Logic Solver"	Working	• Electronic component.	Fail on demand to trip related ESV.	Dangerous UnDetected	None. Only revealed by Proof test.
31			• Electronic component.	TRIP ALL QSV and ESV valve. DCS (Console Operator) is notified.	Dangerous Detected, **BUT** implemented (1oo1D) as "Safe Detected". See section 5.3, point No.3.	Internal electronic diagnostics.
32			• Electronic component.		Safe Detected	
33			• SIF logic **DOES NOT** perform on power up.			
			• Main power failure.	**No Effect.** UPS power supply continue powering Logic Solver	No Effect	
34			• Electronic component. • UPS Power failure.	TRIP both ESV and ESV valves.	Safe UnDetected	

	Device / Short Desc	Normal Operation	Failure mode	Failure Effect	Failure Type	Diagnostic
40	OC-60-PT-510 OC-60-PT-520 OC-60-PT-530 OC-60-PT-540 Output cards	Input soft signal (NORMAL state) and 24 VDC output signal (Energized) match.	• Electronic component.	Fail on demand to trip related ESV.	Dangerous UnDetected	None. Only revealed by Proof test.
41			• Electronic component. • Defective input/output.	TRIP related ESV valve. DCS (Console Operator) is notified.	Dangerous Detected, **BUT** implemented (1oo1D) as "Safe Detected". sec.5.3, point No.4	Internal electronic diagnostics.
42			• Electronic component.		Safe Detected.	
43			• Electronic component. • UPS Power failure.	TRIP related ESV valve.	Safe UnDetected	
SIF Output Channels						
50	60-XOB-511 60-XOB-521 60-XOB-531 60-XOB-541 Output isolator	Input and output signals match output state from STA module.	Electronic component.	Fail on demand to trip related ESV.	Dangerous UnDetected	None. Only revealed by Proof test.
51			• Software failure. • Electronic failure.	TRIP related ESV valve.	Dangerous Detected, **BUT** implemented as "Safe Detected". See sec.5.4.4	Internal electronic diagnostics.
52			UPS Power failure.		Safe UnDetected	
53	60-SOV-510 60-SOV-520 60-SOV-530 60-SOV-540 Solenoid valve	SOV is Energized, making instrument air to keep ESV valve in the fully opened position.	• SOV leaking	**No Effect.** BUT after some time ESV valve can open spuriously if leakage increases.	Dangerous UnDetected	None. Only revealed by maintenance or site inspection.
54			• SOV fails to open on demand	Fail on demand to trip related ESV.		
55			• SOV opens due to failure or coil burnout.	TRIP related ESV valve.	Safe UnDetected	
Final Safety Element (FSE)						
60	60-ESV-510 60-ESV-520 60-ESV-530 60-ESV-540 Emergency shutdown valve	Fully opened	• ESV fails to close on demand	Fail on demand to trip related ESV.	Dangerous UnDetected	None. Only revealed by Proof test.
61			• ESV closes but slowly.	Possible fail on demand to trip related ESV.		
62			• ESV leaking	**No Effect.** BUT after some time ESV valve can open spuriously if leakage increases.		None. Only revealed by maintenance or site inspection.

5.7.1 List of considered combined individual devices in failure for "SIL verification" assessment

Refer to "Reliability Block Diagram" (RBD) in "APPENDIX A".

The 60-SIF-500 structure contains four(4) pipe runs, and each pipe run contains two(2) safety channels with SIF devices in series. The safety channels per pipe run are indicated in the RBD as "Channel xQ" and "Channel xE", where:

- "x" is the pipe run number,
- "Q" is the channel that trips a QSV valve, and
- "E" is the channel that trips an ESV valve.

In addition, the "CommonLS" is commanding four(4) channels that trips each ESV valve (see above section 5.3).

The following facts rule the "failure on demand" condition for each "Letdown Station" (LDS) safety valve, and for the whole 60-SIF-500:

a) Failure of one(1) or more devices in the same series makes the whole series to fail on demand. In other words, a QSV or an ESV will fail to close on demand.

b) One(1) series that fails on demand in the same pipe run will make the pipe run safety to fail on demand (both QSV and ESV shall close, see section 5.3, document (reference [5]) 0418E30SD09 Conceptual SRS – Letdown Station).

c) ALL pipe runs work in 3oo4 architecture, so two(2) or more pipe runs that fail on demand will make 60-SIF-500 to fail on demand as well.

Based on the above statements, Table 9 shows the Minimum Combined Channels in Failure cases that WILL make 60-SIF-500 to fail on demand.

This means, any other operation condition with several channels in failure that include any of the listed cases in Table 9 WILL make 60-SIF-500 to fail on demand.

All combination of channels in failure as described in above paragraph were considered in the "SIL verification" assessment for 60-SIF-500.

Table 9 – Minimum Combined Channels in Failure cases that WILL make 60-SIF-500 to fail on demand

		A	B	C	D	E	F	G	H	I
		Safety Channels description								
	Case No.	Pipe Run 1		Pipe Run 2		Pipe Run 3		Pipe Run 4		
		Channel 1Q to trip 60-QSV-511	Channel 1E to trip 60-ESV-510	Channel 2Q to trip 60-QSV-521	Channel 2E to trip 60-ESV-520	Channel 3Q to trip 60-QSV-531	Channel 3E to trip 60-ESV-530	Channel 4Q to trip 60-QSV-541	Channel 4E to trip 60-ESV-540	CommonLS
Combined Channel Failure cases that are considered in the "SIL verification" assessment	01	Failure		Failure						It DOES NOT matter if "CommonLS" is in failure or NOT in these cases, 60-SIF-500 fails on demand.
	02	Failure			Failure					
	03	Failure				Failure				
	04	Failure					Failure			
	05	Failure						Failure		
	06	Failure							Failure	
	07		Failure	Failure						
	08		Failure		Failure					
	09		Failure			Failure				
	10		Failure				Failure			

11		Failure					Failure		
12		Failure						Failure	
13			Failure		Failure				
14			Failure			Failure			
15			Failure				Failure		
16			Failure					Failure	
17				Failure	Failure				
18				Failure		Failure			
19				Failure			Failure		
20				Failure				Failure	
21					Failure		Failure		
22					Failure			Failure	
23						Failure	Failure		
24						Failure		Failure	
25									Failure

5.8 Failure modes that DO NOT promote a "Failure on Demand"

The purpose of this section is to record other identified 60-SIF-500 failures that **ARE NOT** included in the "SIL verification" assessment, because they **DO NOT** make this SIF to fail on demand.

1) FAILURE: Hand valves are not in the required position for normal operation.

Hand valves **MUST BE** locked in the required position.

According to reference [6], Section 2.3, pg 17:

> *The contribution from human errors should be included in the quantification of PFD (or PFH) if a person/operator is an active element in the execution of the SIF. For example, an operator may be expected to initiate a valve closure (shutdown) or valve opening (blow down) upon an alarm from the SIS.*

Since the "Letdown Station" (LDS) hand valves are not an active element of the 60-SIF-500, these hand valves are not included in the "SIL verification" assessment.

Proper working permits' management and implementation of Lock-out of hand valves **MUST APPLY** to keep these hand valves in the required position during normal operation to allow 60-SIF-500 to execute action on demand.

Proper design of hand valve Lock-out **MUST** allow to Lock hand valves **ONLY** when these ones are in the required normal operation position.

2) Instrument Air FAILURE

Malfunctions in the Instrument Air system may lead to decrease the system pressure, and this condition is equivalent to a "Safe Failure" for the safety function 60-SIF-500: the QSV and/or ESV shall close.

Instrument Air system reliability depends on the system configuration, but this information **IS NOT** available.

3) Electrical and Instrument Air power supply failures

Table 10 – Electrical and hydraulic power supply failures

#	Failure description	Failure type	Failure impact on assessment of	
			"PFDavg"	"STRavg"
1	Main Electrical power fault	Safe Detected **(1)**	NO	YES
2	UPS power supply fault	Safe Detected	NO	YES
3	Instrument Air supply fault	Safe UnDetected	NO	YES

NOTE 1: An indication in DCS shall notify Console Operator about above listed failures.

5.9 SIF Devices' List and data for "SIL verification" (after Reliability Data Validation)

Table 11 – List of SIF Devices that are considered in the SIL Verification report for "PFDavg" and "STRavg" calculations

#	Device's Tag	Device Type	Input Type	Output Type	Input states		Device data purpose	Device Description
					NORMAL	SAFE		
1	60-PT-511 60-PT-521 60-PT-531 60-PT-541	Initiator		4-20 ma IS, HART, NAMUR NE 43	< 8.5 Bar(g)	≥ 8.5 Bar(g)	SIL & STR	Pipe Run 1, 2, 3 & 4 Quick Shutdown pressure transmitter
2	60-XIB-511 60-XIB-521 60-XIB-531 60-XIB-541	Input	4-20 ma IS, HART pass through, loop powered, NAMUR NE 43	4-20 ma HART pass through, NAMUR NE 43	< 8.5 Bar(g)	≥ 8.5 Bar(g)	SIL & STR	Pipe Run 1, 2, 3 & 4 Quick Shutdown pressure input Barrier/Isolator
3	60-STA-511 60-STA-521 60-STA-531 60-STA-541	Logic	4-20 ma HART, loop powered, NAMUR NE 43	24 VDC	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 Quick Shutdown Logic Solver
4	60-XOB-511 60-XOB-521 60-XOB-531 60-XOB-541	Output	24 VDC	24 VDC, IS, loop powered	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 Quick Shutdown pressure output Barrier/Isolator
5	60-SOV-511 60-SOV-521 60-SOV-531 60-SOV-541	Output	24 VDC, IS	Pneumatic	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 SOV to Quick Shutdown Valve
6	60-QSV-511 60-QSV-521 60-QSV-531 60-QSV-541	FSE	Pneumatic		Pressurized, Opened	De-Pressurized, Closed	SIL & STR	Pipe Run 1, 2, 3 & 4 Quick Shutdown Valve
7	60-PT-510 60-PT-520 60-PT-530 60-PT-540	Initiator		4-20 ma IS, HART, NAMUR NE 43	< 8.5 Bar(g)	≥ 8.5 Bar(g)	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown pressure transmitter

#	Device's Tag	Device Type	Input Type	Output Type	Input states		Device data purpose	Device Description
					NORMAL	SAFE		
8	60-XIB-510 60-XIB-520 60-XIB-530 60-XIB-540	Input	4-20 ma IS, HART pass through, loop powered, NAMUR NE 43	4-20 ma HART pass through, NAMUR NE 43	< 8.5 Bar(g)	≥ 8.5 Bar(g)	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown pressure input Barrier/Isolator
9	IC-60-PT-510 IC-60-PT-520 IC-60-PT-530 IC-60-PT-540	Input	4-20 ma HART pass through, loop powered, NAMUR NE 43	Logic Solver	< 8.5 Bar(g)	≥ 8.5 Bar(g)	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown pressure input card
10	CommonLS	Logic					SIL & STR	Common Logic Solver
11	OC-60-PT-510 OC-60-PT-520 OC-60-PT-530 OC-60-PT-540	Output	Logic Solver	24 VDC	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown pressure output card
12	60-XOB-510 60-XOB-520 60-XOB-530 60-XOB-540	Output	24 VDC	24 VDC, IS, loop powered	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown pressure output Barrier/Isolator
13	60-SOV-510 60-SOV-520 60-SOV-530 60-SOV-540	Output	24 VDC, IS	Pneumatic	Energized	De-Energized	SIL & STR	Pipe Run 1, 2, 3 & 4 SOV to Shutdown Valve
14	60-ESV-510 60-ESV-520 60-ESV-530 60-ESV-540	FSE	Pneumatic		Pressurized, Opened	De-Pressurized, Closed	SIL & STR	Pipe Run 1, 2, 3 & 4 Shutdown Valve
15	OC-60SIF510-01 OC-60SIF510-02 OC-60SIF510-03 OC-60SIF510-04	Support	Logic Solver	24 VDC	Energized	De-Energized	ONLY STR	Pipe Run 1, 2, 3 & 4 High Priority Trip 60-SIF-510 output card

Column "Type" description:

Initiator	Device that is directly measuring the process variable that can initiate the SIF action to set the FSE in the SAFE state.
Input	Device included in the safety input channel to transfer the "Initiator" condition up to the "Logic Solver".
Logic	SIF's "Logic Solver", or Device that is performing the "Logic Solver" function.
Output	Device included in the safety output channel to transfer the "Logic Solver" output condition up to the "Final Safety Element" (FSE).
FSE	Final Safety Element.

Table 12 – SIF Devices Reliability data

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
				TI	SLF	Failure Data [FIT]				[%]	Maintenance [h]			DC_S	DC or DC_D	SFF				STR	
	Tag	(A)	Type	[m]	[m]	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	Et	TD	MRT	MTTR			Value	Type	Claim	Note	SDD	
PIPE RUN 1																					PIPE RUN 1
1	60-PT-511	✓	Initiator	6	120	33.0	104.0	312.0	115.0	100%	4	24	72	24.1%	73.1%	79.6%	A	SIL 2	Note 1.	✓	1
2	60-XIB-511	✓	Input	6	120		165.0	160.0	40.0	100%	4	24	72	49.2%	0.0%	89.0%	A	SIL 2	Note 2.	✓	2
3	60-STA-511	✓	Logic	6	120		663.7	168.7	81.0	100%	4	24	72	20.3%	0.0%	91.1%	B	SIL 2	Note 3	✓	3
4	60-XOB-511	✓	Output	6	120		109.7	94.5	35.2	100%	4	24	72	46.3%	0.0%	85.3%	A	SIL 2	Note 4	✓	4
5	60-SOV-511		Output	6	120		184.0		88.0	100%	4	24	72	0.0%	0.0%	67.6%	A	SIL 2	Note 5		5
6	60-QSV-511		FSE	6	120				1272.0	100%	4	24	72	0.0%	0.0%	0.0%	B		Note 7. Tight-Shutoff		6
7	60-PT-510	✓	Initiator	6	120	33.0	104.0	312.0	115.0	100%	4	24	72	76.8%	0.0%	79.6%	A	SIL 2	Note 1	✓	7
8	60-XIB-510	✓	Input	6	120		165.0	160.0	40.0	100%	4	24	72	49.2%	0.0%	89.0%	A	SIL 2	Note 2.	✓	8
9	IC-60-PT-510	✓	Input	6	120	39.0	49.0	13.0	3.4	100%	4	24	72	44.3%	79.3%	96.7%	B	SIL 2	Note 6.	○	9
10	CommonLS	✓	Logic	6	120	1343.0	761.0	932.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 6. 1oo1D	○	10
11	OC-60-PT-510	✓	Output	6	120	1369.0	776.0	942.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 6. 1oo1D	○	11
12	60-XOB-510	✓	Output	6	120		109.7	94.5	35.2	100%	4	24	72	46.3%	0.0%	85.3%	A	SIL 2	Note 4	✓	12
13	60-SOV-510		Output	6	120		184.0		88.0	100%	4	24	72	0.0%	0.0%	67.6%	A	SIL 2	Note 5		13
14	60-ESV-510		FSE	6	120				691.0	100%	4	24	72	0.0%	0.0%	0.0%	B		Note 7		14
15	OC-60SIF510-01	✓	Support	6	120	1369.0	776.0	942.0	3.4	100%	4	24	72	74.9%	0.0%	99.9%	B	SIL 3	Note 8. 1oo1D	○	15

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
				TI	SLF	Failure Data [FIT]				[%]	Maintenance [h]			DC_S	DC or DC_D	SFF				STR	
	Tag	(A)	Type	[m]	[m]	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	Et	TD	MRT	MTTR			Value	Type	Claim	Note	SDD	
PIPE RUN 2																					PIPE RUN 2
16	60-PT-521	✓	Initiator	6	120	33.0	104.0	312.0	115.0	100%	4	24	72	24.1%	73.1%	79.6%	A	SIL 2	Note 1.	✓	16
17	60-XIB-521	✓	Input	6	120		165.0	160.0	40.0	100%	4	24	72	49.2%	0.0%	89.0%	A	SIL 2	Note 2.	✓	17
18	60-STA-521	✓	Logic	6	120		663.7	168.7	81.0	100%	4	24	72	20.3%	0.0%	91.1%	B	SIL 2	Note 3	✓	18
19	60-XOB-521	✓	Output	6	120		109.7	94.5	35.2	100%	4	24	72	46.3%	0.0%	85.3%	A	SIL 2	Note 4	✓	19
20	60-SOV-521		Output	6	120		184.0		88.0	100%	4	24	72	0.0%	0.0%	67.6%	A	SIL 2	Note 5		20
21	60-QSV-521		FSE	6	120				1272.0	100%	4	24	72	0.0%	0.0%	0.0%	B		Note 7. Tight-Shutoff		21
22	60-PT-520	✓	Initiator	6	120	33.0	104.0	312.0	115.0	100%	4	24	72	76.8%	0.0%	79.6%	A	SIL 2	Note 1	✓	22
23	60-XIB-520	✓	Input	6	120		165.0	160.0	40.0	100%	4	24	72	49.2%	0.0%	89.0%	A	SIL 2	Note 2.	✓	23
24	IC-60-PT-520	✓	Input	6	120	39.0	49.0	13.0	3.4	100%	4	24	72	44.3%	79.3%	96.7%	B	SIL 2	Note 6.	○	24
25	CommonLS	✓	Logic	6	120	1343.0	761.0	932.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 6. 1oo1D	○	25
26	OC-60-PT-520	✓	Output	6	120	1369.0	776.0	942.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 6. 1oo1D	○	26
27	60-XOB-520	✓	Output	6	120		109.7	94.5	35.2	100%	4	24	72	46.3%	0.0%	85.3%	A	SIL 2	Note 4	✓	27
28	60-SOV-520		Output	6	120		184.0		88.0	100%	4	24	72	0.0%	0.0%	67.6%	A	SIL 2	Note 5		28
29	60-ESV-520		FSE	6	120				691.0	100%	4	24	72	0.0%	0.0%	0.0%	B		Note 7		29
30	OC-60SIF510-02	✓	Support	6	120	1369.0	776.0	942.0	3.4	100%	4	24	72	74.9%	0.0%	99.9%	B	SIL 3	Note 8. 1oo1D	○	30

PIPE RUN 3

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
						Failure Data [FIT]				[%]	Maintenance [h]					SFF				STR
	Tag	(A)	Type	TI [m]	SLF [m]	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	Et	TD	MRT	MTTR	DC_S	DC or DC_D	Value	Type	Claim	Note	SDD
31	60-PT-531	✓	Initiator	6	120	33.0	104.0	312.0	115.0	100%	4	24	72	24.1%	73.1%	79.6%	A	SIL 2	Note 1.	✓
32	60-XIB-531	✓	Input	6	120		165.0	160.0	40.0	100%	4	24	72	49.2%	0.0%	89.0%	A	SIL 2	Note 2.	✓
33	60-STA-531	✓	Logic	6	120		663.7	168.7	81.0	100%	4	24	72	20.3%	0.0%	91.1%	B	SIL 2	Note 3	✓
34	60-XOB-531	✓	Output	6	120		109.7	94.5	35.2	100%	4	24	72	46.3%	0.0%	85.3%	A	SIL 2	Note 4	✓
35	60-SOV-531		Output	6	120		184.0		88.0	100%	4	24	72	0.0%	0.0%	67.6%	A	SIL 2	Note 5	
36	60-QSV-531		FSE	6	120				1272.0	100%	4	24	72	0.0%	0.0%	0.0%	B		Note 7. Tight-Shutoff	
37	60-PT-530	✓	Initiator	6	120	33.0	104.0	312.0	115.0	100%	4	24	72	76.8%	0.0%	79.6%	A	SIL 2	Note 1	✓
38	60-XIB-530	✓	Input	6	120		165.0	160.0	40.0	100%	4	24	72	49.2%	0.0%	89.0%	A	SIL 2	Note 2.	✓
39	IC-60-PT-530	✓	Input	6	120	39.0	49.0	13.0	3.4	100%	4	24	72	44.3%	79.3%	96.7%	B	SIL 2	Note 6.	○
40	CommonLS	✓	Logic	6	120	1343.0	761.0	932.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 6. 1oo1D	○
41	OC-60-PT-530	✓	Output	6	120	1369.0	776.0	942.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 6. 1oo1D	○
42	60-XOB-530	✓	Output	6	120		109.7	94.5	35.2	100%	4	24	72	46.3%	0.0%	85.3%	A	SIL 2	Note 4	✓
43	60-SOV-530		Output	6	120		184.0		88.0	100%	4	24	72	0.0%	0.0%	67.6%	A	SIL 2	Note 5	
44	60-ESV-530		FSE	6	120				691.0	100%	4	24	72	0.0%	0.0%	0.0%	B		Note 7	
45	OC-60SIF510-03	✓	Support	6	120	1369.0	776.0	942.0	3.4	100%	4	24	72	74.9%	0.0%	99.9%	B	SIL 3	Note 8. 1oo1D	○

PIPE RUN 4

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
						Failure Data [FIT]				[%]	Maintenance [h]					SFF				STR
	Tag	(A)	Type	TI [m]	SLF [m]	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	Et	TD	MRT	MTTR	DC_S	DC or DC_D	Value	Type	Claim	Note	SDD
46	60-PT-541	✓	Initiator	6	120	33.0	104.0	312.0	115.0	100%	4	24	72	24.1%	73.1%	79.6%	A	SIL 2	Note 1.	✓
47	60-XIB-541	✓	Input	6	120		165.0	160.0	40.0	100%	4	24	72	49.2%	0.0%	89.0%	A	SIL 2	Note 2.	✓
48	60-STA-541	✓	Logic	6	120		663.7	168.7	81.0	100%	4	24	72	20.3%	0.0%	91.1%	B	SIL 2	Note 3	✓
49	60-XOB-541	✓	Output	6	120		109.7	94.5	35.2	100%	4	24	72	46.3%	0.0%	85.3%	A	SIL 2	Note 4	✓
50	60-SOV-541		Output	6	120		184.0		88.0	100%	4	24	72	0.0%	0.0%	67.6%	A	SIL 2	Note 5	
51	60-QSV-541		FSE	6	120				1272.0	100%	4	24	72	0.0%	0.0%	0.0%	B		Note 7. Tight-Shutoff	
52	60-PT-540	✓	Initiator	6	120	33.0	104.0	312.0	115.0	100%	4	24	72	76.8%	0.0%	79.6%	A	SIL 2	Note 1	✓
53	60-XIB-540	✓	Input	6	120		165.0	160.0	40.0	100%	4	24	72	49.2%	0.0%	89.0%	A	SIL 2	Note 2.	✓
54	IC-60-PT-540	✓	Input	6	120	39.0	49.0	13.0	3.4	100%	4	24	72	44.3%	79.3%	96.7%	B	SIL 2	Note 6.	○
55	CommonLS	✓	Logic	6	120	1343.0	761.0	932.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 6. 1oo1D	○
56	OC-60-PT-540	✓	Output	6	120	1369.0	776.0	942.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 6. 1oo1D	○
57	60-XOB-540	✓	Output	6	120		109.7	94.5	35.2	100%	4	24	72	46.3%	0.0%	85.3%	A	SIL 2	Note 4	✓
58	60-SOV-540		Output	6	120		184.0		88.0	100%	4	24	72	0.0%	0.0%	67.6%	A	SIL 2	Note 5	
59	60-ESV-540		FSE	6	120				691.0	100%	4	24	72	0.0%	0.0%	0.0%	B		Note 7	
60	OC-60SIF510-04	✓	Support	6	120	1369.0	776.0	942.0	3.4	100%	4	24	72	74.9%	0.0%	99.9%	B	SIL 3	Note 8. 1oo1D	○

NOTES:

1) Rosemount 1151 Smart pressure transmitter. Intrinsically safe. NAMUR NE43.
2) Siemens 9106B isolator, 1-channel input, 2-channels outputs. Input from Zone 0, intrinsically safe. HART transparent. NAMUR NE43 capable. Input with Loop powered mode.
3) Moore Industries Safety Trip Alarm (STA/LHPRG/3PRG/24DC [DIN] Relay Output, Current/Voltage). MII 1103026 C001. SIL 3 capable by "Route 2H". Since All internal diagnostic faults will cause the fault relay to de-energize and remain in a latched state, in case of "Dangerous Detected" failure, STA is set in SAFE state (SDD is (v)). Refer to section 6, page 60, "STA User Manual No.225-748-01L, Moore Industries.
4) GM International D5244S Isolator, 1-channel input, 1-channel output. Output to Zone 0. Intrinsically safe. Output with Loop powered mode.
5) ASCO Series 8320 Solenoid valve. De-Energize to trip.
6) Delta V SIS system, NFPA72, EN54-2 Logic Solver. Data from Exida Certificate FRS 091023 C001.
7) Reliability data of Safety Valve is available from VENDORS upon request ONLY. In order to prepare this report, a typical Safety valve reliability data was used (see Exida report No. VIR 08/01-53 R001).
8) Output card in "CommonLS" to allow 60-SIF-510 High Priority Trip to close QSV on SIF demand. Refer to section 5.4.5 for further information.

DESCRIPTION OF COLUMNS IN Table 12:

Column "A" Device tag number.

Column "B" "Column (A)" flag indicates if the SIF design/installation takes advantage of the related "Device" fault detection capabilities (Diagnostics), or NOT.

- ■ "Device" **DOES NOT** have fault detection capabilities at all (NO Diagnostics). It means both λ_{SD} and λ_{DD} are equal to ZERO(0.0) FIT.
- ☑ YES, "Device" fault detection capabilities (Diagnostics) are used in SIF design/installation, and can be communicated to other devices, or systems (SIS, DCS).
- ○ NO, even though the "Device" has fault detection capabilities (Diagnostics), such capabilities **ARE NOT** used in SIF design/installation.

Column "C" Column "Type" description:

- Initiator: Device that is directly measuring the process variable that can initiate the SIF action to set the FSE in the SAFE state.
- Input: Device included in the safety input channel to transfer the "Initiator" condition up to the "Logic Solver".
- Logic: SIF's "Logic Solver", or Device that is performing the "Logic Solver" function.
- Output: Device included in the safety output channel to transfer the "Logic Solver" output condition up to the "Final Safety Element" (FSE).
- FSE: Final Safety Element.

Column "D" Proof Test Period (TI) in months.
Column "E" Service Life period (SLf), or Mission time in month.
Column "F" Safe Detected failure rate in FIT.
Column "G" Safe UnDetected failure rate in FIT.
Column "H" Dangerous Detected failure rate in FIT.
Column "I" Dangerous UnDetected failure rate n FIT.
Column "J" Proof test effectiveness (Et), or Proof Test Coverage (PTC), in percentage (%).
Column "K" Proof test duration (TD, maintenance time) in hours.
Column "L" Mean Restoration Time (MRT, maintenance time) in hours.
Column "M" Mean Time To Restoration, or Mean Time To Repair (MTTR, maintenance time) in hours.
Column "N" Safe Diagnostic Coverage (DC_S) in percentage (%). Calculated from safe failure rates.
Column "O" Diagnostic Coverage (DC), or Dangerous Diagnostic Coverage (DC_D) in percentage (%). Calculated from dangerous failure rates.
Column "P" "Device" Safe Failure Factor (SFF) value in percentage (%).
Column "Q" Device type "A" or "B", according to IEC-61508-4 (2010), section 3.6.15.
Column "R" Maximum SIL rating to claim for "Device", according to IEC-61508-4 (2010), section 3.6.15. This "Device" data is used to calculate the whole SIF maximum SIL rate to claim by using "Route 1H".
Column "S" Notes to provide more information about the referred "Device".

Column "T" Device "Spurious Dangerous Detected" (SDD) flag indicates if the SIF design/installation takes advantage of the related "Device" fault detection capabilities (Diagnostics) to initiate SIF demand to set FSE in SAFE state when a "Dangerous Detected" failure occurs.

Strictly speaking, "STRavg" calculation should be based on "$\lambda_{SD} + \lambda_{SU}$" (SD+SU) ONLY, BUT if "$\lambda_{DD}$" (DD) can initiate SIF demand to set FSE in SAFE state, then "λ_{DD}" (DD) **MUST BE** considered in the "STRavg" calculation.

So,

■ "Device" **DOES NOT** have fault detection capabilities at all (NO Diagnostics, see column "B" above), or the device "Dangerous Detected" failure rate (λ_{DD}) is equal to ZERO(0.0) FIT.

☑ YES, "Device" fault detection capabilities (Diagnostics) were considered in the SIF design/installation, and if a "Device" "Dangerous Detected" failure occurs. So, when the failure is detected, a WARN is given to Operator, and SIF initiate action to set "Device" in SAFE state. NO delay time applies.

This action may lead to a SIF AUTOMATIC TRIP if the faulted "Device" is in the straight path to the FSE. So, a device "Dangerous Detected" failure will initiate a "Spurious Trip".

○	NO, even though the "Device" has fault detection capabilities (Diagnostics), such capabilities **ARE NOT** used in SIF design/installation to set the "Device" in SAFE state. So, when a device "Dangerous Detected" failure occurs, nothing happens, the SIF may fail on demand if the faulted "Device" is in the straight path to the FSE. ONLY a periodic "Proof Test" can detect the failure.

Table 13 – Reliability data of selected new valves to satisfy 60-SIF-500 target "SIL 3" rating

Pipe Run 1

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
						Failure Data [FIT]				[%]	Maintenance [h]										
	Tag	(A)	Type	TI [m]	SLF [m]	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	Et	TD	MRT	MTTR	DC_S	DC or DC_D	SFF Value	SFF Type	SFF Claim	Note	STR SDD	
6	60-QSV-511	✓	FSE	8	120		485.0	1054.6	958.8	100%	4	24	72	0.0%	52.4%	61.6%	A	SIL 2	Note 7. Tight-Shutoff		6
14	60-ESV-510	✓	FSE	8	120		339.0	710.2	676.5	100%	4	24	72	0.0%	51.2%	60.8%	A	SIL 2	Note 7		14

Pipe Run 2

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
						Failure Data [FIT]				[%]	Maintenance [h]										
	Tag	(A)	Type	TI [m]	SLF [m]	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	Et	TD	MRT	MTTR	DC_S	DC or DC_D	SFF Value	SFF Type	SFF Claim	Note	STR SDD	
21	60-QSV-521	✓	Output	8	120		485.0	1054.6	958.8	100%	4	24	72	0.0%	52.4%	61.6%	A	SIL 2	Note 7. Tight-Shutoff		21
29	60-ESV-520	✓	FSE	8	120		339.0	710.2	676.5	100%	4	24	72	0.0%	51.2%	60.8%	A	SIL 2	Note 7		29

Pipe Run 3

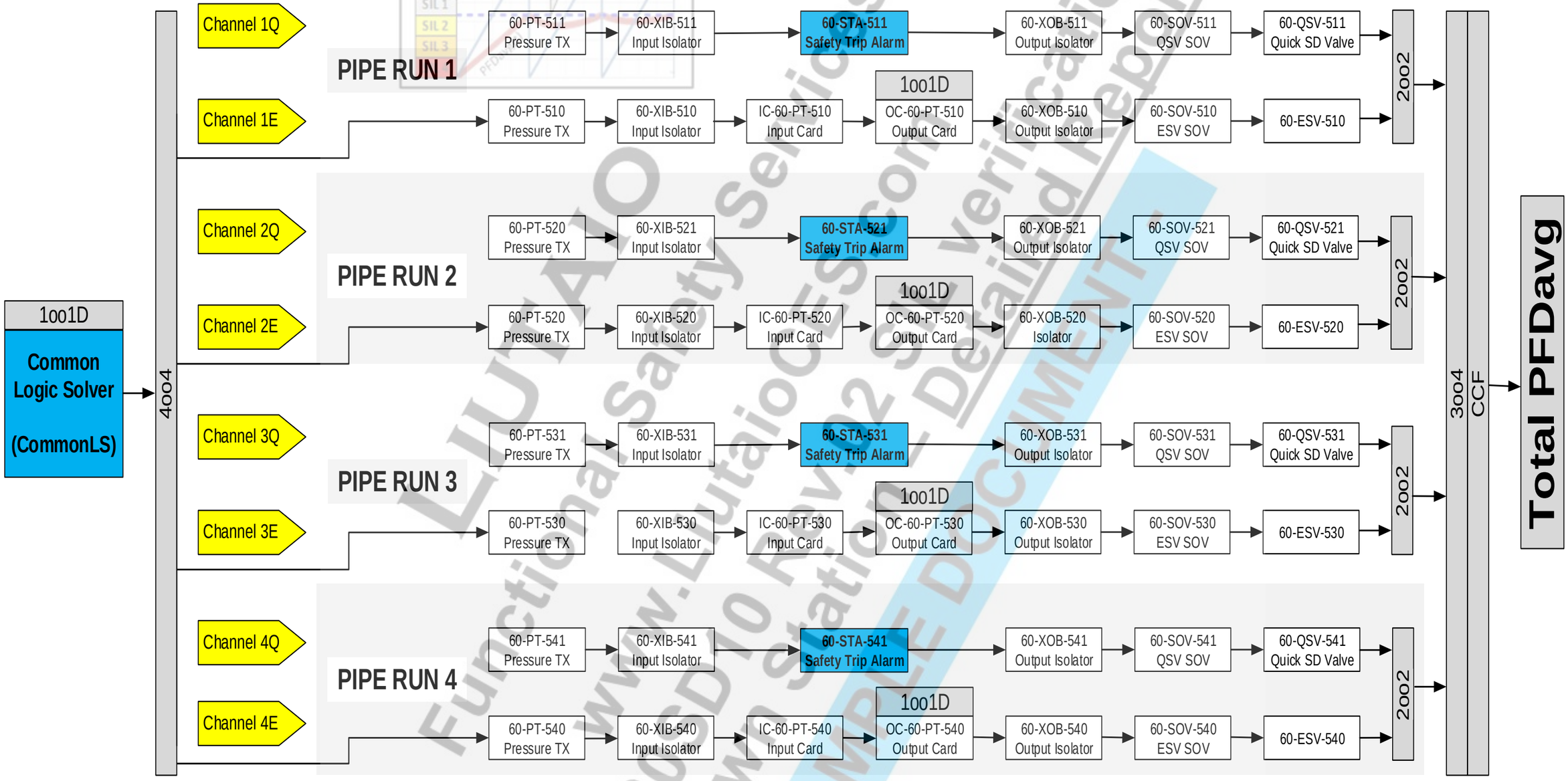
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
						Failure Data [FIT]				[%]	Maintenance [h]										
	Tag	(A)	Type	TI [m]	SLF [m]	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	Et	TD	MRT	MTTR	DC_S	DC or DC_D	SFF Value	SFF Type	SFF Claim	Note	STR SDD	
36	60-QSV-531	✓	Output	8	120		485.0	1054.6	958.8	100%	4	24	72	0.0%	52.4%	61.6%	A	SIL 2	Note 7. Tight-Shutoff		36
44	60-ESV-530	✓	FSE	8	120		339.0	710.2	676.5	100%	4	24	72	0.0%	51.2%	60.8%	A	SIL 2	Note 7		44

Pipe Run 4

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
						Failure Data [FIT]				[%]	Maintenance [h]										
	Tag	(A)	Type	TI [m]	SLF [m]	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	Et	TD	MRT	MTTR	DC_S	DC or DC_D	SFF Value	SFF Type	SFF Claim	Note	STR SDD	
51	60-QSV-541	✓	Output	8	120		485.0	1054.6	958.8	100%	4	24	72	0.0%	52.4%	61.6%	A	SIL 2	Note 7. Tight-Shutoff		51
59	60-ESV-540	✓	FSE	8	120		339.0	710.2	676.5	100%	4	24	72	0.0%	51.2%	60.8%	A	SIL 2	Note 7		59

Refer to Table 12 for "Note 7"and further description of columns in the above tables.

APPENDIX A – 60-SIF-500 Reliability Block Diagram (RBD) to calculate "PFDavg"



APPENDIX B - 60-SIF-500 Reliability Block Diagram (RBD) to calculate "STRavg"