The purpose of this SAMPLE document is to show in the public domain a typical SIL verification report (Short 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.**

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.**

"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, 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 report" (Short 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

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

5.3 Premises and Assumptions

1) 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.

2) 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.

3) 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.

4) 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.

5) The "PFDavg" calculation methodology considesr 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".

6) 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).

7) 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 cuttinh-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-600 to fail on demand to trip QSV valves.

8) 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.

5.4 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

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**. See
2) Table 1. "Proof Test" 6 months.

*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*

3) Table 1.
4) **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:

5) "Proof Test" shall be executed every 7 months for ALL 60-SIF-500 devices.
6) 60-SIF-500 will be capable to claim up to "SIL 3" rating, and to perform with "PFDavg" 6.87E-04 1/y. Refer to Table 2.

7) 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.

Table 1 – "SIL Verification" detailed results for 6 months "Proof Test"

"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**

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

"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-60508.
5	"PFDavg" design limit for SIL target @ 70% MSSDL is : 7.30E-04 [1 / y]