The purpose of this SAMPLE document is to show in the public domain a typical SIL verification report (Short Report) For a "Steam Turbine", 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	72-SIF-213	**SIL Verification Report No.**	0418D30SD06
SIF's Description	Steam Turbine K-1122 High Speed operation protection		
Process Safety Time (PST)	20 sec	**SIF Response Time (SRT, MART)**	10 sec
Target SIL rating	**SIL 2**	**Maximum SIL Safety Design Limit**	70%
Verified SIL rating	**SIL a**	**SIF's Service Life period (SLf)**	10 years

The purpose of this "SIL verification" report was to execute a preliminary assessment of the 72 SIF 213 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 RESULTS of this SIL verification assessment were:

1) 72-SIF-213 design in document (reference [8]) "0418D30SD05 Conceptual SRS – Steam Turbine" **is capable to satisfy "SIL a" rating, instead of target "SIL 2" rating**.

2) The reasons that **DO NOT** allow 72-SIF-213 design to reach the target "SIL 2" rating are:

   a) The Steam Turbine Trip valve 72-ESDV-213 is a "SIL 1" device by "Safe Failure Fraction" (SFF). This fact **DOES NOT** allow the 72-SIF-213 design to claim up to "SIL 1" rating only, and

   b) Even though reliability data of 72-ESDV-213 indicates that this valve includes "Diagnostics" (fault detection capabilities"), the 72-SIF-213 design **DOES NOT** use this valve "Diagnostics". This fact makes 72-ESDV-213 to decrease more its classification up to "SIL a" rating by SFF. So, the 72-SIF-213 design can claim up to "SIL a" rating only.

Total PFDavg	Total RRF	Total % WC	Effective SIL rating by			Verified SIF's SIL rating :
			IEC-61508	MSSDL	Route 1H	
1.57E-02	64	100.0%	SIL 1 **(4)**	SIL 1 **(5)**	SILa1 **(3)**	**SIL a** **Note 2**

3) Possible actions/solutions to improve 72-SIF-213 design to satisfy a target SIL 2 rating can be:

   a) Change selected emergency shutdown valve 72-ESDV-213 by another valve that "In Fact" includes "Diagnostics" to claim SIL 2 rating for 72-SIF-213 (by "Rout 1H", Type "A")

   b) Verify if "proven in use" data is available for current emergency shutdown valve 72-ESDV-213, to justify for this device to claim SIL rating up to SIL 2.

   c) Include two(2) emergency shutdown valves, instead of just one(1), in the process stream where 72-ESDV-213 is located, with at least "SIL 1" rating by "Safe Failure Fraction" (SFF).

   NOTE: in all above choices from "a" to "c", information shall be provided to indicate how the valve "Diagnostics" will be used in the 72-SIF-213 design/installation.

4) Above simplest action/solution in point No.3.a was reviewed. "SIL verification" results were:

   a) 72-SIF-21 3 satisfied **SIL 2** rating. Refer to below table for further information.

   b) "Proof Test" shall be applied for all SIF's devices every 9 months (TI), except for the "Logic Solver" with every 10 years "Proof Test Period" (TI).

Total PFDavg	Total RRF	Total % WC	Effective SIL rating by			Verified SIF's SIL rating :
			IEC-61508	MSSDL	Route 1H	
7.12E-03	140	100.0%	SIL 2 **(4)**	SIL 2 **(5)**	SIL 2 **(3)**	**SIL 2** **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-03 [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" 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] 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

[2] Geir Klingenberg Hansen
Reliability Data for Control and Safety Systems.
Trondheim, Norway: SINTEF. 1998.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY
COMPONENT RELIABILITY DATA FOR USE IN PROBABILISTIC SAFETY ASSESSMENT
IAEA-TECDOC-478. VIENNA, 1988

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

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

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

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

[8] LIUTAIO – Functional Safety Services
0418D30SD05 Conceptual SRS - Steam Turbine - Sample Document
Rev.02

5. SIL verification assessment

5.1 SIF Description

Refer to section 5.1, 5.2 & 5.3, document 0418D30SD05 Conceptual SRS - Steam Turbine

5.2 Safety integrity targets, constraints and other requirements

Refer to section 5.5, document (reference [8]) 0418D30SD05 Conceptual SRS – Letdown Station

5.3 Premises and Assumptions

1) The pressure transmitters 72-PI-213 A/B, solenoid and cartridges valves are considered as a combined device with failure data as described in reference [2].

2) Input cards **SHALL NOT** work in 1oo1D architecture. When a "Detected Failure" occurs in the input card, "Logic Solver" shall degrade input channels' "Decesion Logic" from 1oo2 to 1oo1. So, ONLY the speed sensor in the other input card can initiate a demand.
BUT, anyway 72-ESDV-213 shall trip after MTTR time if failure **IS NOT** repaired/fixed.

3) The "Logic Solver" shall work in 1oo1D architecture and perform as described in above point No.3. BUT, when "Detected Failures" occur in both input channels 72-SIF-213 implementation shall initiate "Spurious Trips" to **DO NOT** compromise safety. Refer to reference [5, SRS], section 5.16.2, point g.

4) ONLY a "Dangerous UnDetected" failure is enough in "Logic Solver" to make 72-SIF-213 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" to **DO NOT** compromise safety. Refer to reference [5, SRS], section 5.16.2, point j.

6) The "PFDavg" calculation methodology considers failures in any independent device, and combined failures, in the 72-SIF-213 that will initiate a demand.

7) About calculation of SIF's "PFDavg", 1oo2 architecture shall be used to calculate the PFD contribution of the "Speed Sensor"/"Input Card" channels, because any of them can initiate a demand. Refer to section 5.15.1 (point b) 5.16.1 & 5.16.2 (point c) in document (reference [8]) 0418D30SD05 Conceptual SRS - Steam Turbine.

8) About calculation of SIF's "STRavg", 2oo2 architecture shall be used instead of 1oo2 to calculate the STR contribution of the "Speed Sensor"/"Input Card" channels, because when one channel is in failure, a "Spurious Trip" will occur ONLY when the other channel is also in failure. Refer to section 5.16.1 & 5.16.2 (point g) in document (reference [8]) 0418D30SD05 Conceptual SRS - Steam Turbine.

5.4 Assessment results

SIF's Tag number	72-SIF-213	**SIL Verification Report No.**	0418D30SD06-1
SIF's Description	Steam Turbine K-1122 High Speed operation protection		
Process Safety Time (PST)	20 sec	**SIF Response Time (SRT, MART)**	10 sec
Target SIL rating	**SIL 2**	**Maximum SIL Safety Design Limit**	70%
Verified SIL rating	**SIL a**	**SIF's Service Life period (SLf)**	10 years

The purpose of this "SIL verification" report was to execute a preliminary assessment of the 72-SIF-213 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) 72-SIF-213 design in document (reference [8]) "0418D30SD05 Conceptual SRS – Steam Turbine" **is capable to satisfy "SIL a" rating, instead of target "SIL 2" rating**.

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

Total PFDavg	Total RRF	Total % WC	Effective SIL rating by IEC-61508	Effective SIL rating by MSSDL	Effective SIL rating by Route 1H	Verified SIF's SIL rating :
1.57E-02	64	100.0%	SIL 1 **(4)**	SIL 1 **(5)**	SILa1 **(3)**	**SIL a** **Note 2**

2) The reasons that **DO NOT** allow 72-SIF-213 design to reach the target "SIL 2" rating are:

a) The Steam Turbine Trip valve 72-ESDV-213 is a "SIL 1" device by "Safe Failure Fraction" (SFF). This fact **DOES NOT** allow the 72-SIF-213 design to claim up to "SIL 1" rating only, instead of up to "SIL 2", and

b) Reliability data of 72-ESDV-213 indicates that this valve includes "Diagnostics" (fault detection capabilities"), BUT the 72-SIF-213 design **DOES NOT** use this valve "Diagnostics". This fact makes 72-ESDV-213 to decrease more its SIL classification from "SIL 1" to "SIL a" by SFF. So, the 72-SIF-213 design can claim up to "SIL a" rating only.

1) **Possible actions/solutions to improve 72-SIF-213 design to satisfy a target SIL 2 rating can be:**

a) Change selected emergency shutdown valve 72-ESDV-213 by another valve that "In Fact" includes "Diagnostics" to claim "SIL 2" rating for 72-SIF-213 (by "Route 1H", device "Type A")

b) Verify if "proven in use" data is available for current emergency shutdown valve 72-ESDV-213, to justify for this device to claim SIL rating up to SIL 2. Refer to below Table 2.

c) Include two(2) emergency shutdown valves, instead of just one(1), in the process stream where 72-ESDV-213 is located, with at least "SIL 1" rating by "Safe Failure Fraction" (SFF).

NOTE: in all above choices from "a" to "c", information shall be provided to "SIL verification", in order to indicate how the valve "Diagnostics" will be used in the 72-SIF-213 design/installation.

3) Above possible action/solution “3.a” was reviewed, and the results were:

a) “Proof Test” shall be applied for all SIF’s devices every 9 months (TI), except for the “Logic Solver” with every 10 years “Proof Test Period” (TI).

b) 72-SIF-213 satisfied **SIL 2** rating, and to perform with “PFDabg” 7.12E-03 1/y. Refer to Table 2.

Table 2 – “SIL Verification” detailed results for 9 months “Proof Test” and SIL-2 valve, after application of actions on above point No.3.a

Total PFDavg	Total RRF	Total % WC	Effective SIL rating by			Verified SIF’s SIL rating :	
			IEC-61508	MSSDL	Route 1H		
7.12E-03	140	100.0%	SIL 2 **(4)**	SIL 2 **(5)**	SIL 2 **(3)**	**SIL 2**	**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-03 [1 / y]