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

5.2.1 Safety integrity targets

Table 1– 72-SIF-213 Safety integrity targets

(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 (MSSDL)**	70%

For "Initiators" and Trip setting, refer to Table 9.

5.2.2 SIL verification Constraints and default values

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

Table 2 - 72-SIF-213 SIL verification Constraints and default values

No.	Description	Abbreviation	Default value	Constraint value	Remark
1	Proof Test Period	TI	12 months	≥ 4 months	Initiators
				≥ 6 months	SOVs
				≥ 6 months	Safety valves
2			10 years	[redacted]	Logic Solver
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			24 hours	≥ 24 hours	Logic Solver
7	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.

      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 "Dangerous" failure rate (λ_{DD}/LdDD, (λ_{DU}/LdDU) value(s) equal to ZERO(0.0) and other devices **DO NOT**, then the "Geometric Average" shall be applied ONLY to the failure rate values other than ZERO(0.0).

   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 72-SIF-213 to fail on demand.

2) By default, "SIL verification" shall consider "Fault Detection Capabilities" (Diagnostics) for "Logic Solver" and Input/Output cards.

3) If target SIL rating is no satisfied, propose possible actions/solutions to improve the design of 72-SIF-213.

4) The indicate methodology in above section 5.2.2 point "1.b" shall be used to calculate Beta values for the following 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) Calculate the SIF's "STRavg" (and "MTTRspurious") for above point No.6.

8) For the Emergency shutdown valve 72-ESDV-213, a "Proof Test Effectiveness" (Et) of 70% applies.

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) 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]. Refer to section 5.8, point No.4 for further information.

3) 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.

4) 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.

5) ONLY a "Dangerous UnDetected" failure is enough in "Logic Solver" to make 72-SIF-213 to fail on demand.

6) 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.

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

8) 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.

9) 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 Reliability data validation (RDV)

Refer to below section 5.9 for the 72-SIF-213 Devices' data for "SIL verification" (after Reliability Data Validation)

This section is organized in the following sub-sections:

1) Turbine speed sensors 72-SI-213/214 Data Validation statement.
2) "Input cards" and "Logic Solver".
3) "Logic Solver" and "Output Cards".
4) Turbine TRIP valve 72-ESDV-213 Data Validation statement.

5.4.1 Turbine speed sensors 72-SI-213/214 Data Validation statement

Table 10 in section 5.9 indicates that speed sensors 72-SI-213/214 have fault detection capabilities (Diagnostics).

The connection between the steam turbine K-1122 speed sensors and the "Logic Solver" is via a "Pulse" signal (passing by input card). This connection **DOES NOT** use special instrument protocols, like NAMUR NE 43 or "NAMUR sensor" (EN-60947-5-6:2000 and IEC-60947-5-6:1999), to handle the speed sensors diagnostics.

Nevertheless, turbine VENDOR shall provide "Diagnostics" logics and calculations to be implemented in the "Logic Solver", as indicated in the 72-SIF-213 "Conceptual SRS" (see reference [8], section 5.16.1).

"Detected Failures" in just "Speed Sensor" **WILL NOT** initiate a demand, BUT in both "Speed Sensors" SIF demand will be initiated. See below section 5.4.2.

Data Validation statement:

"SIL verification" confirms the it is acceptable the design decision on 72-SIF-213 design/installation takes advantage of the speed sensors 72-SI-213/214 fault detection capabilities (Diagnostics) that shall be provided by Turbine VENDOR, in order to avoid "Spurious Trips" from "Speed Sensors".

Those "Diagnostics" shall be implemented in the "Logic Solver". This fact gives credit to the fault detection capabilities (Diagnostics) reported for the speed sensors 72-SI-213/214 in below section 5.9, Table 10, rows No.1 & 2, columns "B" & "H".

This design decision DOES NOT change "Speed Sensors" contribution to 72-SIF-213 "PFDavg" (SIL rating), and to "STRavg" (equivalent to "MTTFspuriusly")

5.4.2 "Input cards" and "Logic Solver"

As indicated in the 72-SIF-213 "Conceptual SRS" (see reference [8], section 5.16.2) when the "Input Card" detects a "Detected Failure" in ONLY one of the input channels:

a) "Logic Solver" **SHALL NOT** trip turbine trip valve 72-ESDV-213,
b) Speed sensors' "Decision Logic" 1oo2 shall be degraded to 1oo1. In this case, only the speed sensor connected to the other input card can initiate a SIF demand.

> **NOTE:** if the input card in failure **IS NOT** restored (or repaired) in a time less than this input card MTTR, then the "Logic Solver" shall initiate a SIF demand (automatic MOS applies).

Nevertheless, if "Logic Solver" detects that "Detected Failure" occurs in both "Input Channels", then "Logic Solver" shall initiate a demand. Refer to "Table 5" in document (reference [8]) 0418D30SD05 Conceptual SRS - Steam Turbine for all combined failures that 72-SIF-213 design considered.

Data Validation statement:

"SIL verification" considers acceptable design decisions:

1) To avoid 72-ESDV-213 "Spurious Trips" when a "Detected Failure" occurs in ONLY one(1) SIF "Input Chanel", and
2) To initiate a SIF demand when a "Detected Failure" occurs in both SIF "Input Chanels".

Design decision No.1:

a) Increases “PFDavg”, equivalent to increase SIL rating, but
b) Decreases 72-SIF-213 “STRavg”, equivalent to increase the “MTTFspuriusly”.

Design decision No.2:

c) No effect on “PFDavg” (SIL rating), and
d) Decreases 72-SIF-213 “STRavg”, equivalent to increase the “MTTFspuriusly”

5.4.3 “Logic Solver” and “Output Cards”

From above section 5.3, points 4 to 6, both “Logic Solver” and “Output cards” will work in 1oo1D architecture, and:

1) When a “Detected Failure” occurs in “Logic Solver” a SIF demand will be initiated., but
2) When a “Detected Failure” occurs in an “Output Card”, ONLY the associated SOV vslve shall be trip (opened, SAFE state).

A “Detected Failure” in “Logic Solver” will for sure make 72-SIF-213 to fail on demand, because “Logic Solver” will have **NO COMMAND** on safety actions.

A “Detected Failure” in an “Output Card” will make 72-SIF-213 to lose command on the related SOV valve. To set in “SAFE state” ONLY one(1) SOV on each SOV pair **WILL NOT** create a “Spurious Trip”, BUT “Detected Failures” in both SOVs in a pair will initiate a “Spurious Trip”.

NOTE: in any case, automatic MOS shall apply and if the SOV in failure **IS NOT** Restored/Fixed before that SOV MTTR time expires, then a turbine trip shall be initiated.

In both above describes situations, design decision was to set the respective “Output Channel” in “SAFE state”. In this way, safety **WILL NOT** be compromised.

Data Validation statement:

“SIL verification” confirm that above described design decision is recommended:

a) On “Logic Solver” to **DO NOT** lose SIF command on SOVs, and
b) On SOVs to **DO NOT** lose command on the SOV in failure. “NAMUR sensor” **DOES NOT** apply in the SIF’s “Output Channel”.

The above described design decisions for “Logic Solver” and “Output cards”:

a) Decreases “PFDavg”, equivalent to decrease SIL rating, but
b) Increases 72-SIF-213 “STRavg”, equivalent to decrease the “MTTFspuriusly”.

5.4.4 Turbine TRIP valve 72-ESDV-213 Data Validation statement

Table 10 in section 5.9 indicates that the emergency shutdown valve 72-ESDV-213 has fault detection capabilities (Diagnostics).

Nevertheless, from 72-SIF-213 "Conceptual SRS" (see reference [8], section 5.3):

a) The only link between the 72-ESDV-213 and the arrangement of solenoids and cartridge valves 72-SOV-213A/B, 72-CRV-213A/B, 72-SOV-214A/B AND 72-CRV-214A/B is the hydraulic power supply.

b) The safety valve 72-ESDV-213 "Partial Valve Stroke Test" (PVST) facility is totally independent of the 72-SIF-213 design/installation, it CANNOT promote a SIF failure on demand, and it is normally physically blocked.

The above points indicate that there is **NO** description or evidence that 72-ESDV-213 "Diagnostics" can improve the 72-SIF-213 design/installation.

Data Validation statement:

Since 72-SIF-213 design/installation **DOES NOT** take advantage of the Turbine TRIP valve 72-ESDV-213 fault detection capabilities (Diagnostics), this valve "Detected Failure" rates **ARE NOT** considered in this "SIL verification" assessment.

Refer to below section 5.9, Table 10, rows No.14, column "B".

Design decision No.1:

a) Increases "PFDavg", equivalent to increase SIL rating, but

b) Decreases 72-SIF-213 "STRavg", equivalent to increase the "MTTFspuriusly".

5.5 Reliability Block Diagram (RBD)

The Reliability Block Diagram (RBD) shows the 72-SIF-213 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

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

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 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**. See Table 3 and Figure 3.

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.

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 "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 4.

   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.

To verify the above indicated action "3.a", reliability data in Table 11 was used, and the results were:

4) "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).

5) **72-SIF-213 will be capable to claim up to "SIL 2" rating**, and to perform with "PFDabg" 7.12E-03 1/y, and "STRavg" 6.60E-02 1/y (MTTFspuriously 15.1 years) when a "Spurious Trip" occurs.

   Refer to Table 4 and Figure 4 for further details.

6) Figure 4 shows the PFDavg/PFD(t) graph 9 months "Proof Test Period" for ALL SIF's devices.

7) The 72-SIF-213 "Proof Test Period" (TI) was verified in the range 08-12 months.

   From this "SIL verification", it was found that BOTH Maintenance effect (MTTR, TD, MRT) and CCF have an impact on 60-SIF-500 SIL rating.
   Refer to:

   - Table 6 for numeric results about "PFDavg" & "STRavg", and
   - Figure 1 and Figure 2 for graphic results.

8) Calculated "Beta" (β & β_D) values for the cases of **Simple** (Greater CCF effect) and **Enhanced** (Lower CCF effect) SIF's design/Installation are as reported in Table 5Table 4. 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 72 SIF-213 installation quality, which effect will be to decrease the "Common Cause Failure" (CCF) effect. For example:

   - 16% quality improvement will allow to increase "Proof Test" to every 10 months (CCF beta value reduction for 1oo2 from 10.00% to 8.52%).
   - 42% quality improvement will allow to increase "Proof Test" to every 11 months (CCF beta value reduction for 1oo2 from 10.00% to 6.25%).
   - 88% quality improvement will allow to increase "Proof Test" to every 10 months (CCF beta value reduction for 1oo2 from 10.00% to 2.08%).

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]	RRF	%WC	SIL by IEC-61508	SIL by MSSDL	SIL by Route 1H
1	Initiators + Input Channels	1.62E-05	61875	0.1%	SIL 4	Above SIL 1 PFDavg Design Limit 7.30E-03 Below SIL 2	SIL 3
2	Logic Solver	3.11E-04	3219	2.0%	SIL 3		SIL 3
3	Output Channels	2.78E-04	3602	1.8%	SIL 3		SIL 2
4	Final Safety Element (FSE)	1.51E-02	66	96.1%	SIL 1		SIL a

Total PFDavg	Total RRF	Total % WC	Effective SIL rating by		
			IEC-61508	MSSDL	Route 1H
1.57E-02	64	100.0%	SIL 1 **(4)**	SIL 1 **(5)**	SIL a **(3)**

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

STR Rating Results (SIF Simple implementation only)

#	Independent contributions to STRavg (Note 1)	STRavg [1 / y]	%WC	MTTFSpuriously [y]
1	Initiators + Input Channels	9.96E-10	0.0%	**- Never -**
2	Logic Solver	6.58E-03	10.0%	152.1
3	Output Channels	5.94E-02	90.0%	16.8
4	Final Safety Element	0.0	0.0%	**- Never -**

Total STRavg	Total % WC	Total MTTRspuriously
6.60E-02	100.0%	15.1

Notes	
1	Refer to Reliability Block Diagram (RBD) in Section "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-03 [1 / y]

Table 4 – "SIL Verification" detailed results for 9 months "Proof Test" and SIL-2 valve, after application of actions on above point No.3.a

SIL Rating Results original data, 9 months "Proof Test" (SIF Simple implementation)

#	Independent contributions to PFDavg (Note 1)	PFDavg [1 / y]	RRF	%WC	SIL by IEC-61508	SIL by MSSDL	SIL by Route 1H
5	Initiators + Input Channels	2.16E-05	46398	0.3%	SIL 4	Above SIL 1	SIL 3
6	Logic Solver	3.11E-04	3219	4.4%	SIL 3	PFDavg Design Limit 7.30E-03	SIL 3
7	Output Channels	4.34E-04	2304	6.1%	SIL 3		SIL 2
8	Final Safety Element (FSE)	6.36E-03	157	89.2%	SIL 2	Below SIL 2	SIL 2

Total PFDavg	Total RRF	Total % WC	Effective SIL rating by IEC-61508	Effective SIL rating by MSSDL	Effective SIL rating by Route 1H
7.12E-03	140	100.0%	SIL 2 **(4)**	SIL 2 **(5)**	SIL 2 **(3)**

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

STR Rating Results (SIF Simple implementation only)

#	Independent contributions to STRavg (Note 1)	STRavg [1 / y]	%WC	MTTFSpuriously [y]
5	Initiators + Input Channels	9.96E-10	0.0%	- Never -
6	Logic Solver	6.58E-03	10.0%	152.1
7	Output Channels	5.94E-02	90.0%	16.8
8	Final Safety Element	0.0	0.0%	- Never -

Total STRavg	Total % WC	Total MTTRspuriously
6.60E-02	100.0%	15.1

Notes	
1	Refer to Reliability Block Diagram (RBD) in Section "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-03 [1 / y]

Table 5 – Calculated "Beta" values for the cases of Simple (Greater CCF effect) and Enhanced (Lower CCF effect) SIF design/installation

Additional SIL Verification results

#	Independent contributions to PFDavg (Note 1)	SCA type	Proof Test (TI, months)	CCF calculate Beta values – Enhanced Design – Beta(β)	CCF calculate Beta values – Enhanced Design – BetaD(βD)	CCF calculate Beta values – Simple Design – Beta(β)	CCF calculate Beta values – Simple Design – BetaD(βD)
1	Initiators + Input Channels	1oo2	9	1.0%	1.0%	10.0%	10.0%
2	Logic Solver	1oo1	120	CCF does not apply			
3	Output Channels	1oo2	9	1.0%	1.0%	10.0%	10.0%
4	Final Safety Element (FSE)	1oo1	9	CCF does not apply			

Table 6 – Calculated PFDavg/STRavg values when 72-ESDV-213 includes "Diagnostics", with and without Maintenance effect

	Tested TI values [month]	Calculated PFDavg and STRavg values [1 / y]							
		NO Maintenance Effect				WITH Maintenance Effect (MTTR, **TD**, MRT)			
		CCF Simple Quality $\beta = \beta_D = 10.0\%$		CCF Enhanced Quality $\beta = \beta_D = 1.0\%$		CCF Simple Quality $\beta = \beta_D = 10.0\%$		CCF Enhanced Quality $\beta = \beta_D = 1.0\%$	
		PFDavg	STRavg (MTTFsp)	PFDavg	STRavg (MTTFsp)	PFDavg	STRavg (MTTFsp)	PFDavg	STRavg (MTTFsp)
1	8	6.81E-03	[redacted]	6.50E-03	[redacted]	7.02E-03	6.60E-02 (15.1 y)	6.71E-03	6.35E-02 (15.8 y)
2	9	6.95E-03		6.61E-03		7.12E-03		6.78E-03	
3	10	7.13E-03		6.76E-03		7.34E-03		6.97E-03	
4	11	7.28E-03		6.88E-03		7.45E-03		7.04E-03	
5	12	7.46E-03		7.02E-03		7.67E-03		7.23E-03	

Figure 1 - Graphic results for tested "Proof Test Period" (TI) values

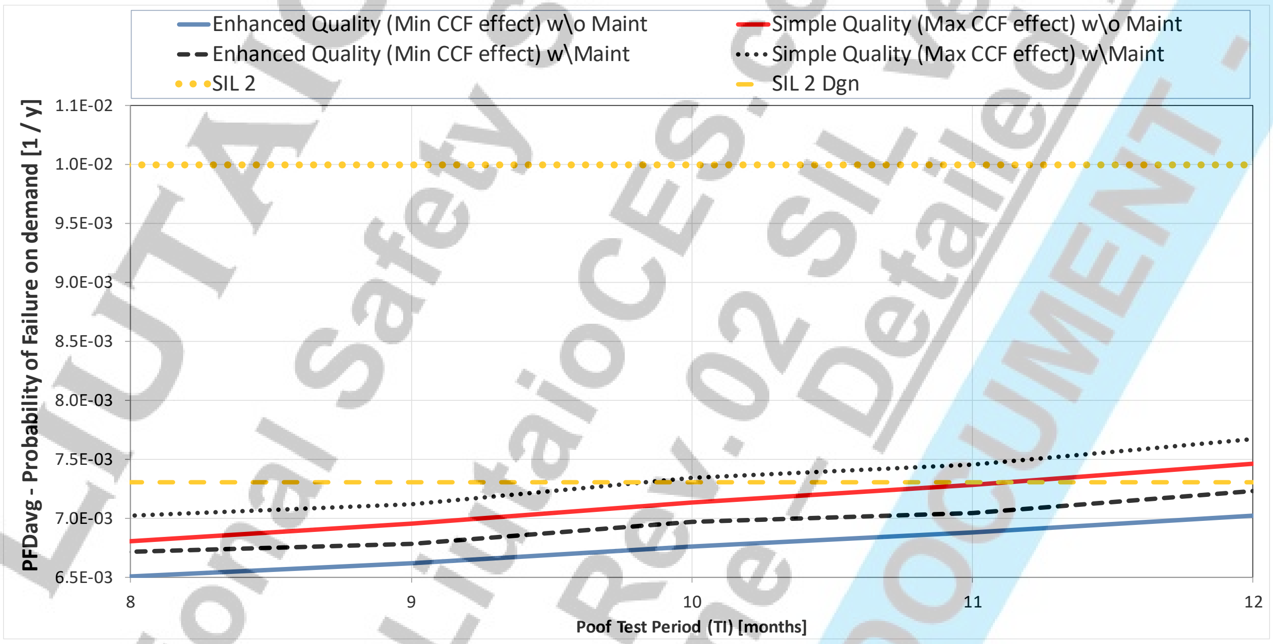


Figure 2 – ZOOM from Figure 1 to show detail of Graphic results for tested "Proof Test Period" (TI) values

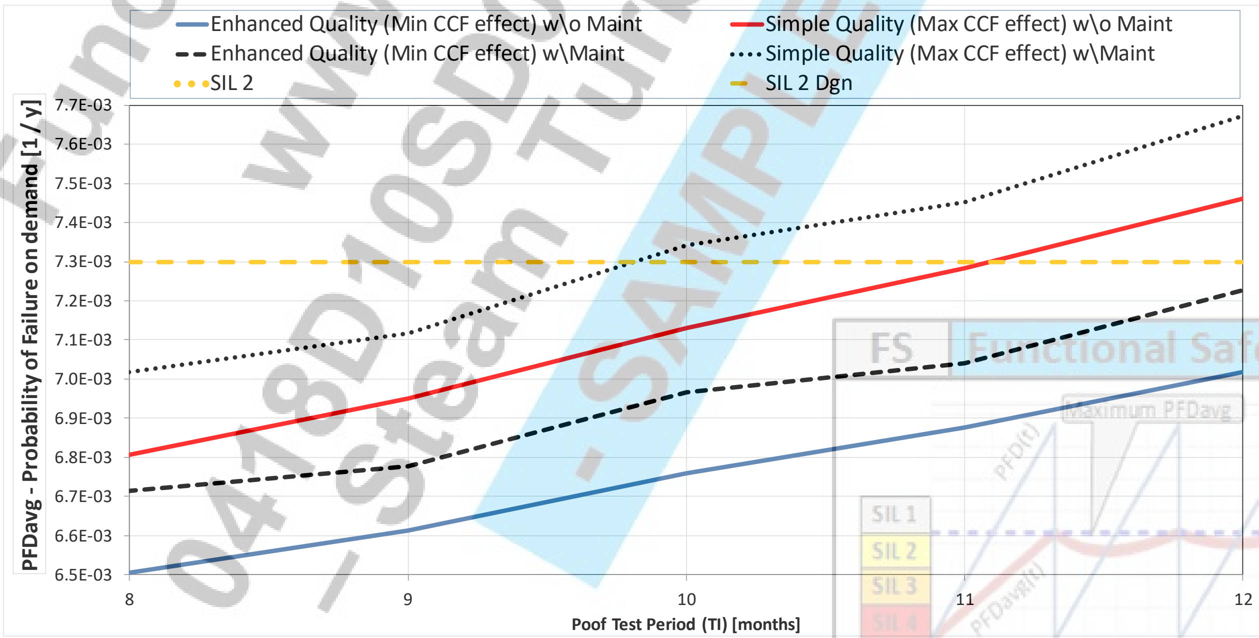


Figure 3 – 72-SIF-213 PFDavg/PFD(t) graph with 6 months "Proof Test Period" for SIF's devices, but every 10 years for the "Logic Solver", with original data

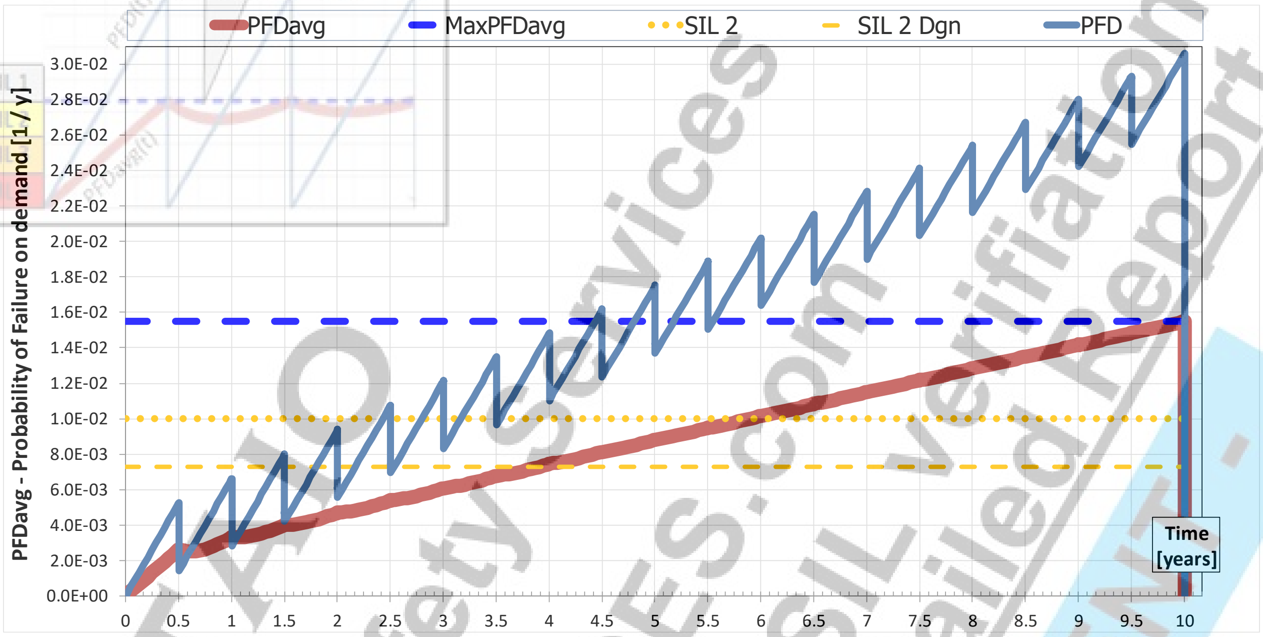
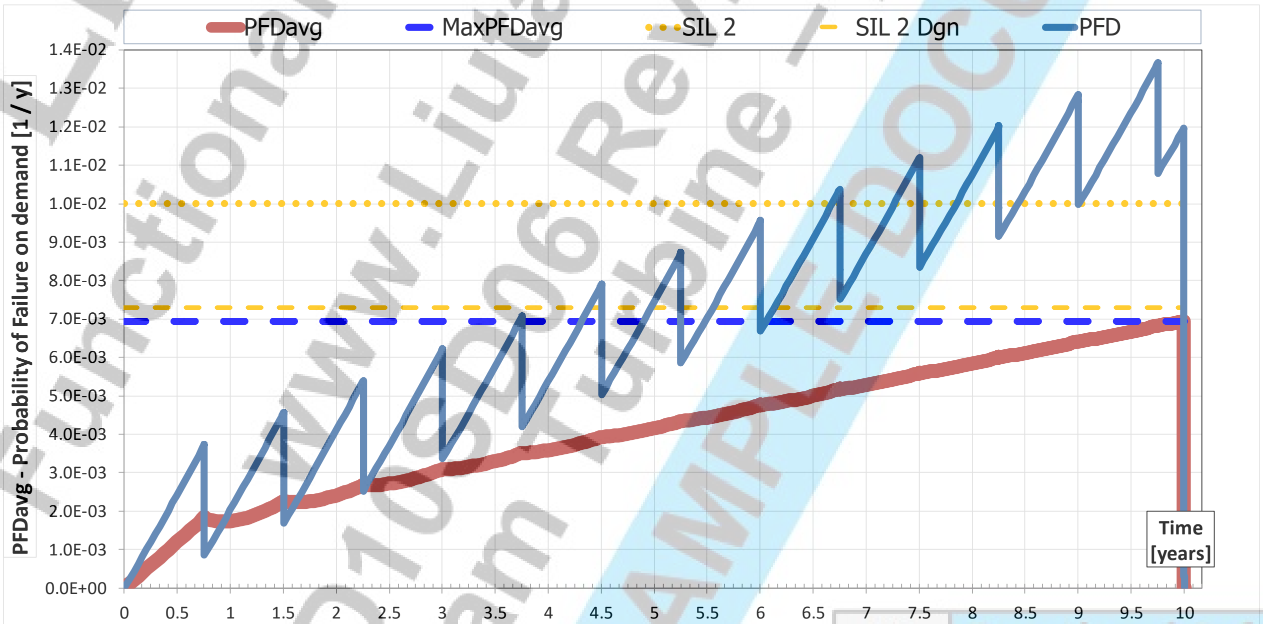


Figure 4 – 72-SIF-213 PFDavg/PFD(t) graph with 9 months "Proof Test Period" for SIF's devices, but every 10 years for the "Logic Solver", with proposed solution "3.a" to allow 72-SIF-213 design to satisfy target SIL2 rating



5.7 (FMEA) Failure Modes and Effects Analysis

Failure modes and effects are listed in Table 7.

Table 7 - 72-SIF-213 list of failure modes and effects

	Device / Short Desc	Normal Operation	Failure mode	Failure Effect on SIF	Failure Type	Diagnostic
	SIF Initiators					
01	72-SI-213 Speed sensor	Speed below 110% value	• Constant or ZERO(0.0) speed value. • Loose, burned, Short circuit, or otherwise damaged wiring and/or connectors.	TRIP after MTTR if speed sensor failure remains.	Dangerous Detected, BUT could be "Safe Detected". See sec.5.4.1	Turbine VENDOR includes Spike rejection and other diagnostics in "Logic Solver" to degrade from 1oo2 to 1oo1. Refer to section 5.16.1 in "Conceptual SRS", reference [8].
02	72-SI-214 Speed sensor			TRIP after MTTR if speed sensor failure remains.		
03	Both 72-SI-213 72-SI-214 simultaneous			Turbine Spurious TRIP.	Safe Detected	
	SIF Input channels					
10	IC-72-SI-213 IC-72-SI-214	Input Pulse signal and output soft signal match measured Turbine speed lesser than 110%	• Electronic component.	Fail on demand to trip Turbine	Dangerous UnDetected	None. Only revealed by Proof test.
11	Input cards		• Electronic component. • Defective input. • Short circuit.	**No effect.** DCS (Console Operator) is notified and automatic MOS applies. **BUT**, Turbine could trip after MTTR.	Dangerous Detected	Internal electronic diagnostics.
12			• Electronic component.		Safe Detected , BUT implemented as "Dangerous Detected". See section 5.4.2	
13			• Electronic component. • UPS Power failure.	Turbine TRIP.	Safe UnDetected	
	Logic Solver					
20	Logic Solver	Working	• Electronic component.	Fail on demand to trip turbine trip valve 72-ESDV-213	Dangerous UnDetected	None. Only revealed by Proof test.
21			• Electronic component.	Turbine TRIP. DCS (Console Operator) is notified.	Dangerous Detected, **BUT** implemented (1oo1D) as "Safe Detected". See section 5.3	Logic Solver diagnostic
22			• Electronic component.		Safe Detected	

	Device / Short Desc	Normal Operation	Failure mode	Failure Effect on SIF	Failure Type	Diagnostic
23			• SIF logic **DOES NOT** perform on power up.			
			• Main Power failure	**No Effect.** UPS power supply continue powering Logic Solver	No Effect	
24			• Electronic component. • UPS Power failure.	Turbine TRIP.	Safe UnDetected	
SIF Output Channels						
30	OC-72-SOV-213A OC-72-SOV-213B OC-72-SOV-214A OC-72-SOV-214B	Input soft signal (NORMAL state) and 24 VDC output signal (Energized) match.	• Electronic component.	Fail on demand to trip Turbine	Dangerous UnDetected	None. Only revealed by Proof test.
31	Output cards		• Electronic component. • Defective input. • Short circuit.	Turbine TRIP. DCS (Console Operator) is notified.	Dangerous Detected, **BUT** implemented (1oo1D) as "Safe Detected". See section 5.3	Internal electronic diagnostics.
32			• Electronic component.		Safe Detected	
33			• Electronic component. • UPS Power failure.	Turbine TRIP.	Safe UnDetected	
40	72-SOV-213A 72-SOV-213B 72-SOV-214A 72-SOV-214B	SOV is Energized, making hydraulic fluid to keep CRV valve pressurized in the fully closed position.	• SOV leaking	**No Effect.** BUT after some time Turbine TRIPs if leakage increases.	Dangerous UnDetected	None. Only revealed by maintenance or site inspection. PI may indicate pressure variation.
41	Solenoid valves		• SOV fails to open on demand	Fail on demand to trip Turbine.		None. Only revealed by maintenance or site inspection.
42			• SOV-A failed and is opened	**No effect.** Possible Turbine TRIP if SOV-B or CRV-B fails in same mode.	Safe Detected	PI shows pressure increases.
43			• SOV-B failed and is opened	**No effect.** Possible Turbine TRIP if SOV-A or CRV-A fails in same mode.		PI shows pressure decreases.
44			• Both SOV-A/B failed and are opened.	Turbine TRIP.		PI shows pressure increases substantially.
45			• SOV opens due to failure or coil burnout.		Safe UnDetected	

	Device / Short Desc	Normal Operation	Failure mode	Failure Effect on SIF	Failure Type	Diagnostic
50	72-CRV-213A 72-CRV-213B 72-CRV-214A 72-CRV-214B Solenoid valves	CRV valve is pressurized in the fully closed position.	• CRV leaking	**No Effect.** BUT after some time Turbine TRIPs if leakage increases.	Dangerous UnDetected	None. Only revealed by maintenance or site inspection. PI may indicate pressure variation.
51			• CRV fails to open on demand	Fail on demand to trip Turbine.		None. Only revealed by maintenance or site inspection.
52			• CRV-A failed and is opened	**No effect.** Possible Turbine TRIP if CRV-B fails in same mode.	Safe Detected	PI shows pressure increases.
53			• CRV-B failed and is opened	**No effect.** Possible Turbine TRIP if CRV-A fails in same mode.		PI shows pressure decreases.
54			• Both CRV-A/B fail	Turbine TRIP.		PI shows pressure increases substantially.
55			• CRV opens due to failure or coil burnout.		Safe UnDetected	
60	72-PI-213A 72-PI-213B PTs for SOV diagnostics	PT measuring hydraulic pressure.	• Miscalibration. • Plugged impulse pipe.	**No Effect.** PI shows wrong information.	Annunciation UnDetected	None. Only revealed by Proof test.
61			• UPS power failure.	**No Effect.** Loss of SOVs diagnostics.		DCS diagnostics.
62			• Broken membrane. • Software failure. • Electronic failure.			PI internal electronic diagnostics.
	Final Safety Element (FSE)					
70	72-ESDV-213 Turbine TRIP valve	Fully opened	TRIP valve fails to close on demand	Possible Turbine damage. SIF failed on demand.	Dangerous UnDetected Failure	None. Only revealed by Proof test.
71			TRIP valve closes but slowly.			
72			TRIP valve leaking	**No Effect.** Possible Turbine Spurious TRIP if leakage becomes bigger.	Safe UnDetected Failure	Only revealed by maintenance or site inspection.

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

The purpose of this section is to record other identified 72-SIF-213 failures that **ARE NOT** included in the "SIL verification" assessment, because they **DO NOT** make this SIF to fail on demand.

Refer to Figure No.2, 3 & 4 in document (reference [8]) "0418D30SD05 Conceptual SRS - Steam Turbine".

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

For Steam Turbine K-1122 NORMAL operation, the hand valves HV-01A/B, HV-02A/B and HV-03A/B in the SOV/CRV arrangement **MUST BE** locked in the required position.

According to reference [1], 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 indicated hand valves are not an active element of the 72-SIF-213, 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 72-SIF-213 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) FAILURE of Restriction Orifices RO-1 A/B, RO-2 A/B and RO-30

If any of the restriction orifices RO-1 A/B, RO-2 A/B and RO-30 becomes plugged, due to a possible malfunction of the Hydraulic system filter facility:

a) The Emergency safety valve 72-ESDV-213 will remain in the fully opened position, and

b) Since flow path through the Cartridge valve is significantly low resistance,

It is foreseen that the safety function 72-SIF-213 WILL perform on demand.

Further malfunctions in the Hydraulic system may lead to decrease the system pressure, and this condition is equivalent to a "Safe Failure" for the safety function 72-SIF-213.

FAILURE of Restriction Orifices **DO NOT** have credit for "PFDavg" assessment, BUT they have for "STRavg" assessment.

3) FAILURE on hydraulic filters and check valves

Same analysis as for "Restriction Orifices" applies. See above point No.2.

4) FAILURE on Pressure transmitters 72-PI-213 A/B

A failure in any of the Pressure transmitters 72-PI-213 A/B **WILL NOT** MAKE the 72-SIF-213 to fail on demand.

However, since the Solenoid and Cartridge valve arrangements are mechanical devices with no fault detection capabilities (Diagnostics), then to consider the Pressure transmitters as part of this arrangement can introduce diagnostic capabilities to each SOV/CRV arrangement.
So, the pressure transmitters can be used to reveal some of the SOV/CRV arrangement UnDetected failures. Refer to Table 7 for further information.

At the end, to consider the Pressure transmitter, Solenoid and Cartridge valves arrangement as a combined device with Detected Failure rate, and a reduced UnDetected failure rate, will reduce the arrangement impact on "PFDavg".

5) FAILURE on "Partial Valve Stroke Test" (PVST) facility of the Emergency Shutdown Valve 72-ESDV-213

Any failure in the "Partial Valve Stroke Test" (PVST) facility of the Emergency Shutdown Valve 72-ESDV-213 can be considered as a "Safe Failure", because it will lead the SIF to SAFE state.

At the end, the 72-ESDV-213 PVST facility is considered has NO impact on both "PFDavg" and "STRavg" assessments, because:

- PVST facility is most of the time locked closed, and
- Proper working permits' management and maintenance procedures **MUST BE** followed to avoid human errors.

6) Electrical and hydraulic power supply failures

Table 8 – 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	Hydraulic power supply fault	Safe UnDetected	NO	YES

NOTE 1: An indication in DCS will reveal this failure.

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

Table 9 – 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	72-SI-213	Initiator		Pulse	< 110%	≥ 110%	SIL & STR	Turbine Speed Sensor
2	72-SI-214	Initiator		Pulse	< 110%	≥ 110%	SIL & STR	Turbine Speed Sensor
3	IC-72-SI-213	Input	Pulse	Logic Solver	< 110%	≥ 110%	SIL & STR	Input Card 72-SI-213
4	IC-72-SI-214	Input	Pulse	Logic Solver	< 110%	≥ 110%	SIL & STR	Input Card 72-SI-214
5	LogicSolver	Logic					SIL & STR	Logic Solver
6	OC-72-SOV-213A	Output	Logic Solver	24 VDC, loop powered	Energized	De-Energized	SIL & STR	Output Card to 72-SOV-213A
7	OC-72-SOV-213B	Output	Logic Solver	24 VDC, loop powered	Energized	De-Energized	SIL & STR	Output Card to 72-SOV-213B
8	OC-72-SOV-214A	Output	Logic Solver	24 VDC, loop powered	Energized	De-Energized	SIL & STR	Output Card to 72-SOV-214A
9	OC-72-SOV-214B	Output	Logic Solver	24 VDC, loop powered	Energized	De-Energized	SIL & STR	Output Card to 72-SOV-214B
10	PI-SOV-CRV-213A **(1)**	Output	24 VDC	Hydraulic	Energized	De-Energized	SIL & STR	Combined Dev: 72-PI-213A, 72-SOV-213A, 72-CRV-213A **(1)**
11	PI-SOV-CRV-213B **(1)**	Output	24 VDC	Hydraulic	Energized	De-Energized	SIL & STR	Combined Dev: 72-PI-213A, 72-SOV-213B, 72-CRV-213B **(1)**
12	PI-SOV-CRV-214A **(1)**	Output	24 VDC	Hydraulic	Energized	De-Energized	SIL & STR	Combined Dev: 72-PI-213B, 72-SOV-214A, 72-CRV-214A **(1)**
13	PI-SOV-CRV-214B **(1)**	Output	24 VDC	Hydraulic	Energized	De-Energized	SIL & STR	Combined Dev: 72-PI-213B, 72-SOV-214B, 72-CRV-214B **(1)**
14	72-ESV-213	FSE	Hydraulic		Pressurized, Opened	De-Pressurized, Closed	SIL & STR	Turbine Trip Valve

Note 1: Combined SIF Device. Refer to section 5.8 for further information.

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) .

NOTE: The Final safety element is also an "Output" device.

FSE — Final Safety Element.

Support — Device that IS NOT part of the SIF from "Initiator" to FSE, but it is required to allow proper operation of the SIF.

Example: Instrument Air, UPS power supply, Hydraulic power supply, etc.

If a "Support" device fails, the SIF changes to SAFE state, or it is NOT able to perform its duty.

Table 10 – 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 [m]	SLF [m]	Failure Data [FIT]				[%]	Maintenance [h]			DC_S	DC or DC_D	SFF				STR	
	Tag	(A)	Type			λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	Et	TD	MRT	MTTR			Value	Type	Claim	Note	SDD	
1	72-SI-213	✓	Initiator	13	120			720.0	46.0	100%	4	24	72	0.0%	94.0%	94.0%	B	SIL 2	Note 3	✓	1
2	72-SI-214	✓	Initiator	13	120			720.0	46.0	100%	4	24	72	100.0%	0.0%	94.0%	B	SIL 2	Note 3	✓	2
3	IC-72-SI-213	✓	Input	13	120	39.0	49.0	13.0	3.4	100%	4	24	72	44.3%	79.3%	96.7%	B	SIL 2	Note 2	○	3
4	IC-72-SI-214	✓	Input	13	120	39.0	49.0	13.0	3.4	100%	4	24	72	44.3%	79.3%	96.7%	B	SIL 2	Note 2	○	4
5	LogicSolver	✓	Logic	120	120	1343.0	761.0	932.0	3.4	100%	24	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 2. 1oo1D	○	5
6	OC-72-SOV-213A	✓	Output	13	120	1369.0	776.0	942.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 2. 1oo1D	○	6
7	OC-72-SOV-213B	✓	Output	13	120	1369.0	776.0	942.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 2. 1oo1D	○	7
8	OC-72-SOV-214A	✓	Output	13	120	1369.0	776.0	942.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 2. 1oo1D	○	8
9	OC-72-SOV-214B	✓	Output	13	120	1369.0	776.0	942.0	3.4	100%	4	24	72	63.8%	99.6%	99.9%	B	SIL 3	Note 2. 1oo1D	○	9
10	PI-SOV-CRV-213A	✓	Output	13	120	1750.0	750.0		1140.0	100%	4	24	72	70.0%	0.0%	68.7%	B	SIL 1	Note 1	○	10
11	PI-SOV-CRV-213B	✓	Output	13	120	1750.0	750.0		1140.0	100%	4	24	72	70.0%	0.0%	68.7%	B	SIL 1	Note 1	○	11
12	PI-SOV-CRV-214A	✓	Output	13	120	1750.0	750.0		1140.0	100%	4	24	72	70.0%	0.0%	68.7%	B	SIL 1	Note 1	○	12
13	PI-SOV-CRV-214B	✓	Output	13	120	1750.0	750.0		1140.0	100%	4	24	72	70.0%	0.0%	68.7%	B	SIL 1	Note 1	○	13
14	72-ESDV-213	○	FSE	13	120			647.2	422.8	70%	4	24	72	0.0%	0.0%	0.0%	B		Note 4	○	14

NOTES:

1) Combined Pressure transmitter, Solenoid and Cartridge valve. Refer to reference [8] ("Conceptual SRS"), section 5.14.2 and Table 4.

2) Delta V SIS system, NFPA72, EN54-2 Logic Solver. Data from Exida Certificate FRS 091023 C001.

3) Reliability data of Turbine speed sensors is available from VENDORS upon request ONLY. To prepare this report, Speed sensors reliability data was estimated based on available public information from Woodward, SIL-3 Speed Sensors, Product Specification 03429.
Assumption Sensor PFDavg is SIL-3 with "Proof Test" (TI) 1 year, and 10 years "Service Life" (SLf).

4) Reliability data of Emergency Shutdown Valve is available from VENDORS upon request ONLY. In order to prepare this report, a typical Emergency shutdown valve reliability data for SIL 1 application is used.

DESCRIPTION OF COLUMNS IN Table 10:

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.

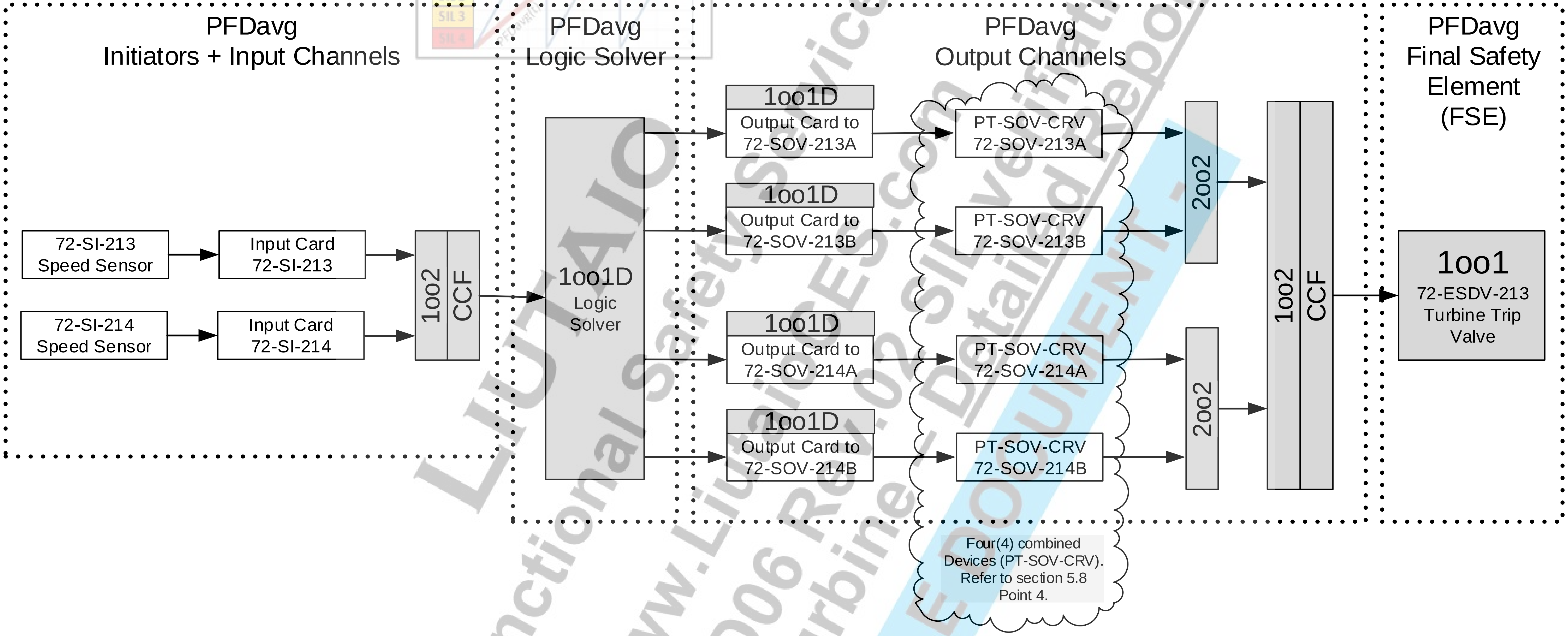
So, when a device "Dangerous Detected" failure occurs, nothing happens, the SIF may fail on demand if the faulted "Device" is in the straight path to the FSE. ONLY a periodic "Proof Test" can detect the failure.

Table 11 – Reliability data of selected new valve 72-ESDV-213 to satisfy 72-SIF-213 target "SIL 2" rating

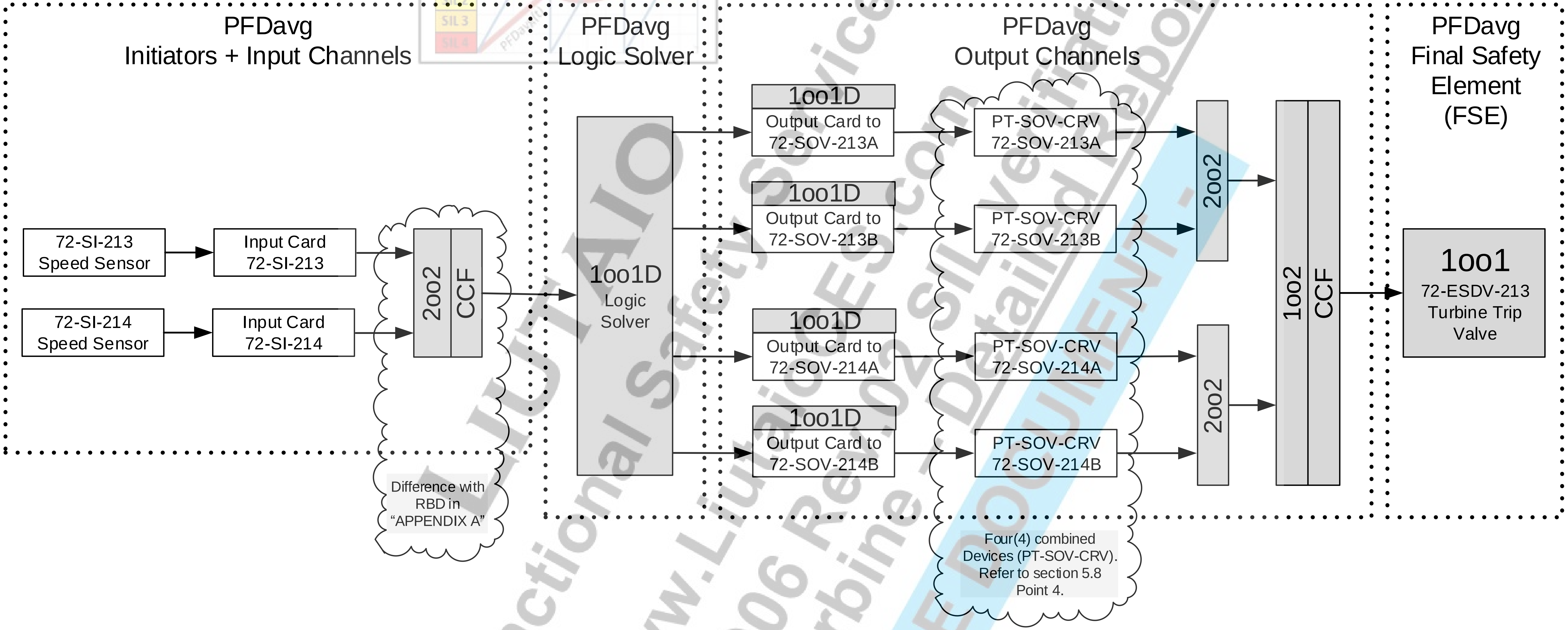
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
				TI	SLF	Failure Data [FIT]				[%]	Maintenance [h]			DC_S	DC or	SFF				STR	
	Tag	(A)	Type	[m]	[m]	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	Et	TD	MRT	MTTR		DC_D	Value	Type	Claim	Note	SDD	
14	72-ESDV-213	✓	FSE	13	120			647.2	422.8	70%	4	24	72	0.0%	60.5%	60.5%	A	SIL 2	Note 4	○	14

Refer to Table 10 for "Note 4"and further description of columns in the above tables

APPENDIX A – Reliability Block Diagram (RBD) to calculate "PFDavg"



APPENDIX B – Reliability Block Diagram (RBD) to calculate “STRavg”



Difference with RBD in “APPENDIX A”

Four(4) combined Devices (PT-SOV-CRV). Refer to section 5.8 Point 4.