The purpose of this SAMPLE document is to show in the public domain a typical Conceptual SRS 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.

Table of Contents

1. Document purpose

The purpose of this sample document is to show in the public domain a typical "Conceptual SRS" for a "Steam Turbine", 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. (SRS) Safety Requirements Specification

5.1 SIF Tag number and short description

SIF Tag: 72-SIF-213

Short description: Steam Turbine K-1122 high speed operation protection.

5.2 Hazardous even description that the SIF is protecting from

High pressure steam is coming from boilers' output header to feed the steam turbine K-1122, to produce electrical power.

The steam turbine K-1122 load is controlled by manipulating the steam flow to the turbine, via the steam turbine control valve 72-FCV-213.

In case of malfunction of the steam turbine control valve 72-FCV-213, or overpressure from the boilers' output header, the turbine will increase speed above the maximum operation speed and the turbine will be damaged.

To avoid the steam turbine K-1122 damage for operation at high speed, when any of the high-speed trip initiators 72-SI-213/214 measurement reach the value of 110%, then the 72-SIL-213 shall close the turbine trip valve 72-ESDV-213.

5.3 SIF related process description, operation and actions to achieve the required functional safety

The simplified sketch for load control and high-speed protection of a Steam Turbine K-1122 is shown in the Figure 1.

The steam turbine control manipulates the steam turbine control valve 72-FCV-213 to control the turbine load.

SIF initiators are two(2) speed sensors 72-SI-213/214. The "Safety Instrumented Function" (SIF) 72-SIF-213 protects the Steam Turbine K-1122 against operation at 110% of maximum design speed, by closing the emergency shutdown valve 72-ESDV-213 to cut the steam flow to the turbine. De-Energize to Trip philosophy is implemented.

In NORMAL state, the emergency shutdown valve 72-ESDV-213 is in the fully opened position under hydraulic pressure, and the SOVs are energized in the in the fully closed position. The speed sensors pulse signals are sent to the Logic Solver (Input Card), and the equivalent measurement is below 110%.

In SAFE state :

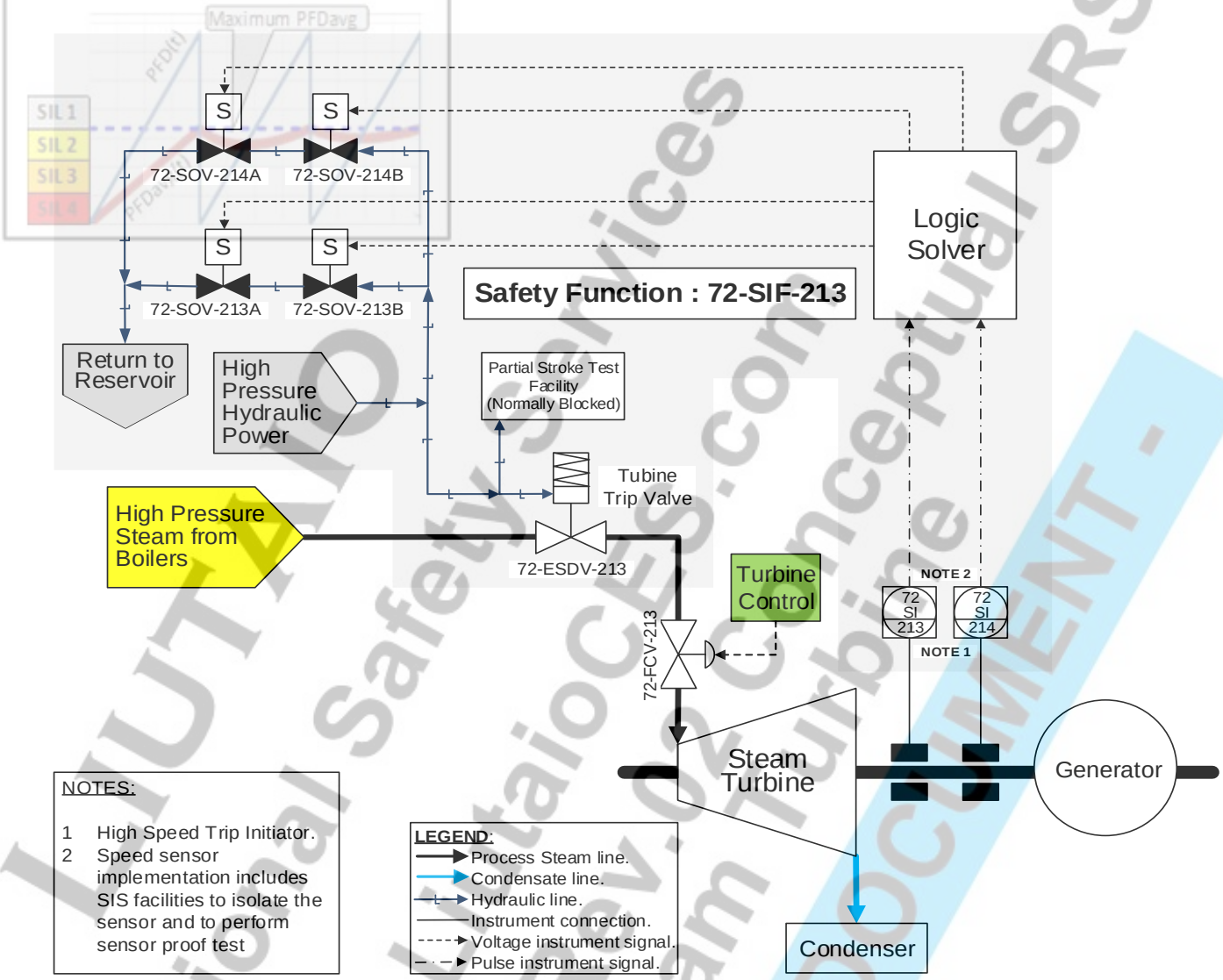
a) The speed sensors work in 1oo2 architecture, when one of the sensors' measurement signal is above 110% (SAFE state), then Logic Solver trips the SOVs 72-SOV-213A/B and 72-SOV-214A/B to quick decrease the hydraulic pressure to the shutdown valve 72-ESDV-213. Therefore, this safety valve opens (SAFE state).

b) Each pair of SOVs work in a 2oo2 architecture.

c) Only one(1) SOV pair shall open to trip the shutdown valve 72-ESDV-213, in order to achieve the required functional safety. So, both SOV pairs work in a 1oo2 architecture.

d) Shutdown valve 72-ESDV-213 opens when the hydraulic pressure is released through the opened SOVs.

Figure 1 – Steam Turbine simplified sketch



The installation detail of the Solenoid Valves (SOV) arrangement is shown in the Figure 2.

Figure 3 shows the SOV and Cartridge valves (CRV) arrangements in NORMAL state (Energized) during normal operation. In this condition, SOVs are energized from Logic Solver output card.

Figure 4 shows the SOV arrangement in SAFE state (De-Energized) when a SIF demand occurs.

Figure 2 – Solenoid Valve arrangement detail

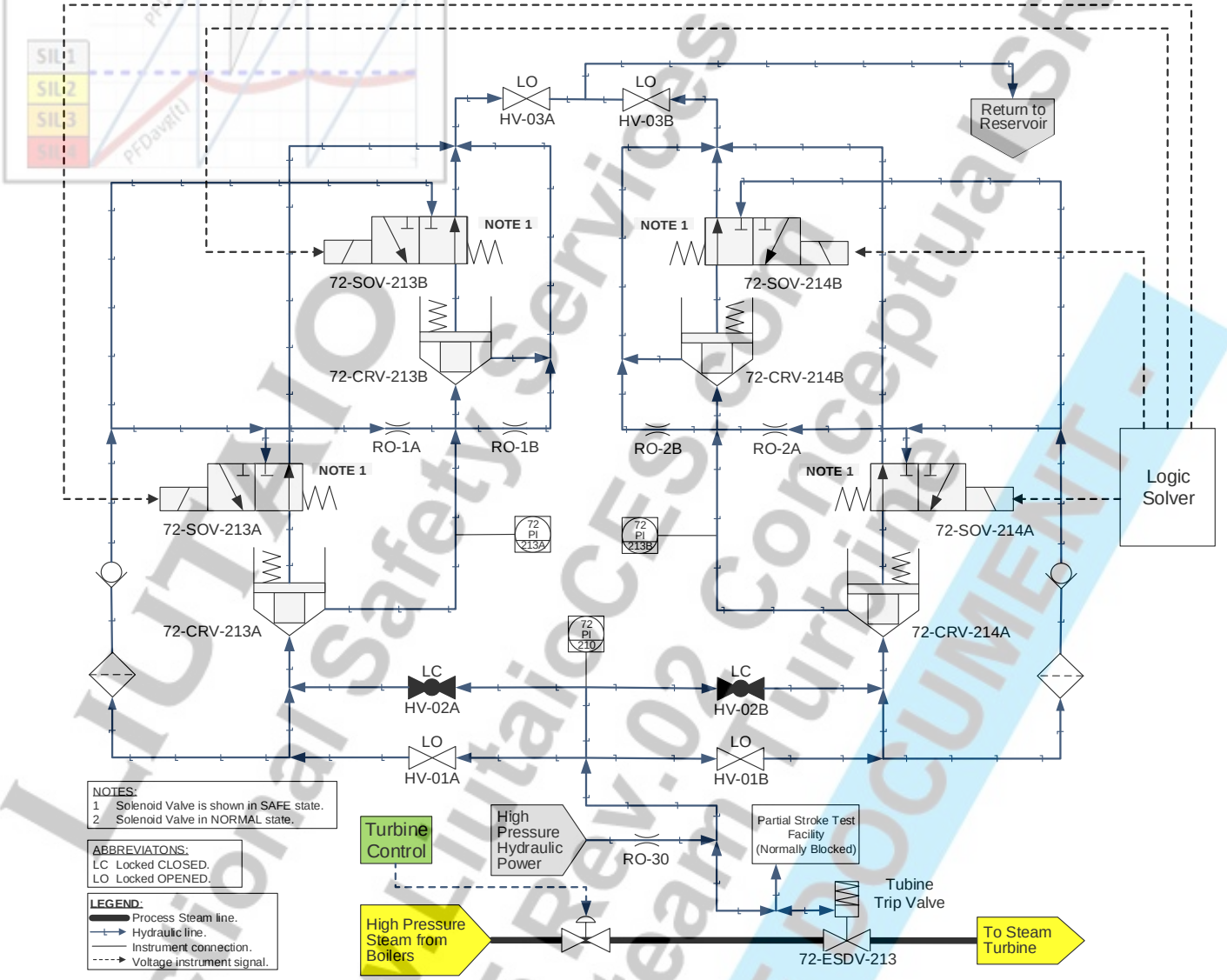


Figure 3 – Hydraulic fluid action on SOV in NORMAL state

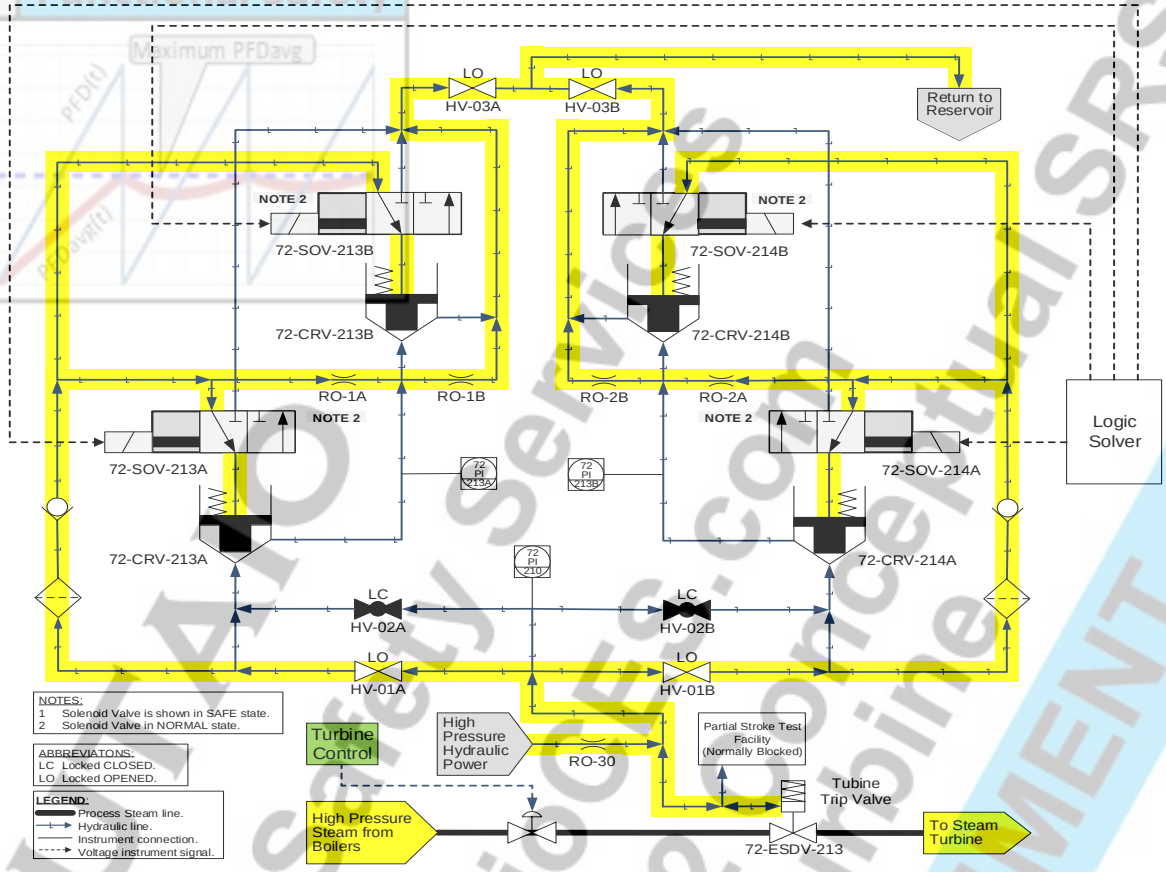
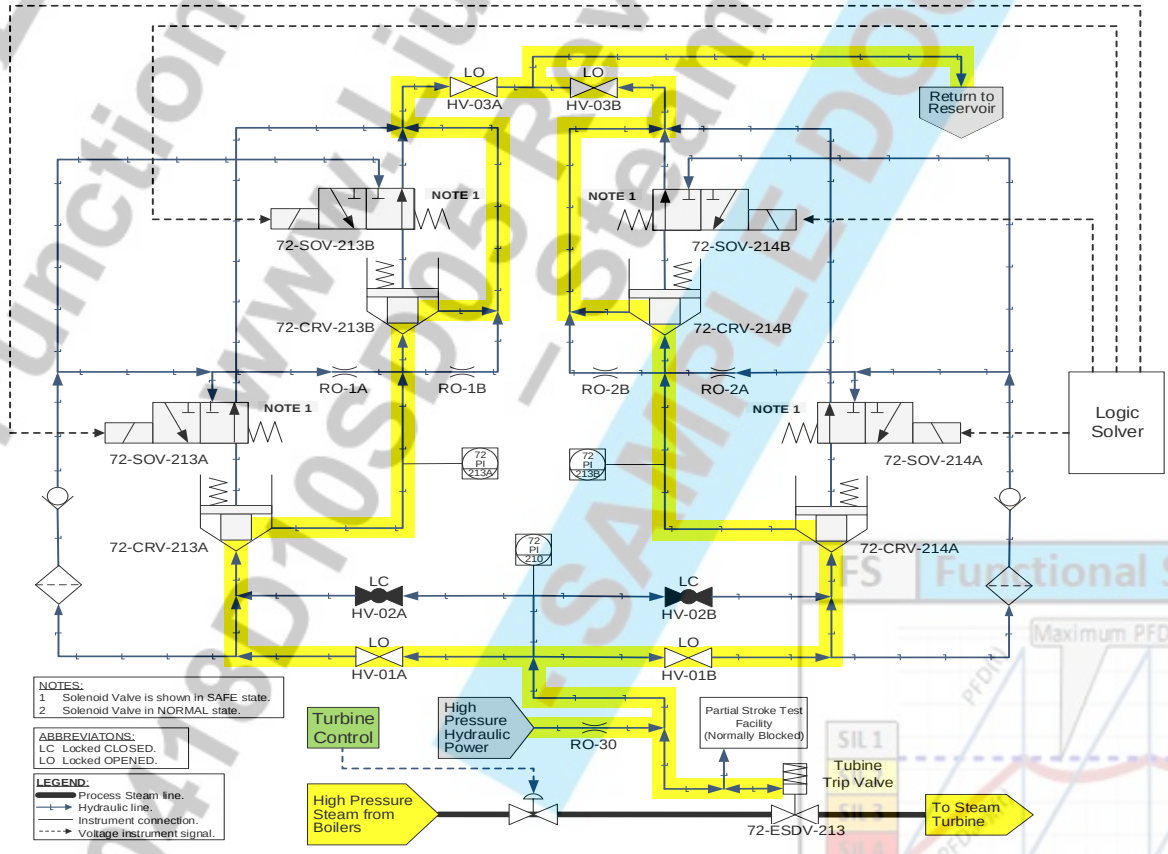


Figure 4 – Hydraulic fluid routing in SAFE state to release hydraulic pressure and to open the emergency shutdown valve 72-ESDV-213



5.4 SIF Devices' List

Table 1 – 72-SIF-213 Devices' List

#	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 **(2)**	Output	24 VDC	Hydraulic	Energized	De-Energized	SIL & STR	Combined Dev: 72-PI-213B, 72-SOV-214A, 72-CRV-214A **(2)**
13	PI-SOV-CRV-214B **(2)**	Output	24 VDC	Hydraulic	Energized	De-Energized	SIL & STR	Combined Dev: 72-PI-213B, 72-SOV-214B, 72-CRV-214B **(2)**
14	72-ESV-213	FSE	Hydraulic		Pressurized, Opened	De-Pressurized, Closed	SIL & STR	Turbine Trip Valve

Note 1: Combined SIF Device. Refer to section 5.15.2 for further information.
Note 2: Combined SIF Device. Refer to section 5.15.3 for further information.

Column "Device 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.

5.5 Safety integrity targets, constraints and other requirements

5.5.1 Safety integrity targets

Table 2 – 72-SIF-213 Safety integrity targets

(Low Demand System)

SIF's Tag number	72-SIF-213	**SIL Verification Report No.**	To be defined
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 settings, refer to Table 1.

5.5.2 SIL verification Constraints and default values

Table 3 shows typical constraints and default values for "SIL verification".

Table 3 – 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		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.

5.5.3 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) Using IEC-61508-6, Annex D, it is possible to calculate the following "Beta" values:
   - 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.

5.6 Additional Initiators and Input Channels description

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".

5.7 Manual shutdown requirements

N/A

5.8 Startup Bypass requirements

N/A

5.9 SIF Decision Logic and Calculations

The speed sensors work in 1oo2 architecture, so, when one of the sensors' measurement signal is above 110%, then Logic Solver trips the SOVs 72-SOV-213A/B and 72-SOV-214A/B to open the turbine trip valve 72-ESDV-213.

5.10 Interlock management requirements

N/A

5.11 Additional "Final Safety Elements" (FSEs) and Output Channels description

Turbine trip valve 72-ESDV-213shall include magnetic limit switches, to detect the closed, opened and travelling valve position.

These magnetic limit switches shall be connected to DCS.

5.12 Reset function requirements, actions after shutdowns and/or before startup

Refer to references [3] and [4] for "Reset function" description.

Only "Reset Logic", with "Manual Reset" shall be implemented in SIS.

Soft-button 72-HS-213 shall be implemented in DCS console, to allow Console Operator to apply Reset to 72-SIF-213.

"Reset Logic" output shall be in SAFE state after SIS power up.

5.13 Operation and DCS HMI, alarms and even messages

Refer to section 4.2.13 in document: (reference [3])

0418D20SD04 Safeguarding requirements - Sample Document

5.14 Integration with Control and operation startup

Before commissioning, turbine trip valve 72-ESDV-213 shall be isolated from steam line. 72-SIF-213 shall "Out Of service" (OOS state) to facilitate the installation and local testing of this safety valve and other control and SIF instruments.

During "Steam Turbine" commissioning, Console Operator shall dismiss OOS state in 72-SIF-213. This action shall:

a) Close turbine trip valve 72-ESDV-213 (SAFE state), and
b) Force in closed position control valve 72-FCV-213.

Once all PERMISSIVE are satisfied to start up the "Steam Turbine", the Console Operator shall apply Reset to 72-SIF-213, via the soft-button 72-HS-213 in DCS console. This action shall:

1) Open turbine trip valve 72-ESDV-213 (NORMAL state), and

2) Allow "Turbine Control" to command the control valve 72-FCV-213 to modulate the steam feed flow to the turbine.

When a demand occurs, 72-SIF-213 will close (SAFE state) the turbine trip valve 72-SIF-213, and the control valve 72-FCV-213 shall be forced in the closed position as well.

5.15 "Proof Test" requirements and use of MOS

Refer to section 4.2.14, in document (reference [3]) 0418D20SD04 Safeguarding requirements for further MOS information and requirements.

Independent "Proof Test" facilities shall be provided for:

1) "Initiators" and "Input Channels".
2) Solenoid valves 72-SOV-213A/B.
3) Solenoid valves 72-SOV-214A/B.
4) Turbine Trip valve 72-ESDV-213.

In total, Seven(7) "Proof Tests" can be performed. See Table 4.

ALL SAFETY and PERMISSION procedures **MUST BE** completed and approved before executing any "Proof Test". Only one(1) "Proof Test" can be executed at the time.

If another MOS is active in the same "MOS Group" where 72-SIF-213 is located, then **NO** "Proof Test" can be executed in 72-SIF-213.

Only the Turbine Trip valve 72-ESDV-213 "Proof Test" shall affect normal turbine operation. All other "Proof Tests" **WILL NOT** affect turbine operation.

Table 4 – Required MOS logics per SIF device, or "Input/Output Channel"

#	Device's Tag	Type	MOS Tag (2)	"Proof Test" Fail/Success Criterion	Device Description
1	72-SI-213	Initiator	72-MOS-213-I	SIS fetches signal changes in less than 1.0 sec **(1)**	Turbine Speed Sensor
	IC-72-SI-213	Input			Input Card 72-SI-213
2	72-SI-214	Initiator	72-MOS-214-I	SIS fetches signal changes in less than 1.0 sec **(1)**	Turbine Speed Sensor
	IC-72-SI-214	Input			Input Card 72-SI-214
3	OC-72-SOV-213A	Output	72-MOS-213A-O	72-PI-213A pressure increases when 72-SOV-213A opens. Pressure change in < 2 sec.	Output Card to 72-SOV-213A
	PI-SOV-CRV-213A	Output			Combined Dev: 72-PI-213A, 72-SOV-213A, 72-CRV-213A
4	OC-72-SOV-213B	Output	72-MOS-213B-O	72-PI-213A pressure decreases when 72-SOV-213B opens. Pressure change in < 2 sec.	Output Card to 72-SOV-213B
	PI-SOV-CRV-213B	Output			Combined Dev: 72-PI-213A, 72-SOV-213B, 72-CRV-213B
5	OC-72-SOV-214A	Output	72-MOS-214A-O	72-PI-214A pressure increases when 72-SOV-214A opens. Pressure change in < 2 sec.	Output Card to 72-SOV-214A
	PI-SOV-CRV-214A	Output			Combined Dev: 72-PI-213B, 72-SOV-214A, 72-CRV-214A
6	OC-72-SOV-214B	Output	72-MOS-214B-O	72-PI-214A pressure decreases when 72-SOV-214B opens. Pressure change in < 2 sec.	Output Card to 72-SOV-214B
	PI-SOV-CRV-214B	Output			Combined Dev: 72-PI-213B, 72-SOV-214B, 72-CRV-214B
7	72-ESV-213	Output	72-MOS-213	72-ESDV-213 closes from 100% to 50% opening in less than 8.0 sec., and next closes fully.	Turbine K-1122 Trip Valve

Note 1: Signal change **MUST BE** tested above and below trip setting value.
Note 2: Only one(1) MOS can be "Activated" at the time, or none if other MOS are already activated in the same "MOS Group".

5.15.1 "Proof Test" for "Initiators" and "Input Channels"

Refer to section 4.2.14, in document (reference [3]) 0418D20SD04 Safeguarding requirements for further MOS information and requirements.

When 72-MOS-213-I (or 72-MOS-214-I) is activated:

a) The speed sensors' related SIF 1oo2 "Decision Logic" shall be degraded to "1oo1" (see above section 5.9), or set the 72-SI-213 (72-SI-214) input signal to "Logic Solver" in the SAFE state, and
b) ONLY 72-SI-214 (72-SI-213) can trip 72-ESDV-213.

"Proof Test" of "Initiators" and "Input Channels" shall be monitored in DCS, but not initiated from control room.

MAINTENANCE personnel shall simulate speed sensor 72-SI-213 (72-SI-214) signal to verify reading from SIS.

Sensor maintenance can be executed only on turbine maintenance overhaul.

The Fail/Success completion criterion for this "Proof Test" is:

- **SUCCESFUL** From DCS it was possible to verify that "Logic Solver" can detect when speed signal is above and below trip setting.
- **UNSUCCESSFUL** From DCS it **WAS NOT** possible to verify that "Logic Solver" can detect when speed signal is above or below trip setting.
- **FAIL SAFE** "Proof Test" was aborted by any other mean.

5.15.2 "Proof Test" for Solenoid valves 72-SOV-213A/B

Refer to section 4.2.14, in document (reference [3]) 0418D20SD04 Safeguarding requirements for further MOS information and requirements.

72-SOV-213A (72-SOV-213B) "Proof Test" includes testing of the associated "Cartridge Valve" (CRV) 72-CRV-213A (72-CRV-213B).

"Proof Test" shall be monitored in DCS and executed from control room @ DCS console.

Since the pressure transmitter 72-PI-213A can detect when any of the SOVs open, then the use of this instrument can be considered as part of the SOVs fault detection capabilities (Diagnostic). BUT, a failure in any of the pressure transmitter 72-PI-213A WILL NOT make 72-SIF-213 to fail on demand (NO effect).

This means that pressure transmitter and associated SOVs shall be considered a combined SIF device.

Once ALL SAFETY and PERMISSION procedures are completed and approved, MAINTENANCE personnel can:

a) "Activated" 72-MOS-213A-O (or 72-MOS-213B-O).
b) Wait until 72-PI-213A measured pressure is stable.
c) Initiate "Proof Test" via push button 72-HS-213A-O (or 72-HS-213B-O).

d) 72-PI-213A pressure shall increase (decrease) up to a stable value in less than 2.0 sec. to consider "Proof Test" completed successfully.

The Fail/Success completion criterion for this "Proof Test" is:

- **SUCCESFUL** From DCS it was possible to verify that 72-PI-213A can detect when 72-SOV-213A (72-SOV-213B) opens, and this SOV closed after 10 sec after trip command was sent.
- **UNSUCCESSFUL** From DCS it **WAS NOT** possible to verify that 72-PI-213A can detect when 72-SOV-213A (72-SOV-213B) opens, or this SOV DID NOT close after 10 sec after trip command was sent.
- **FAIL SAFE** "Proof Test" was aborted by any other mean.

5.15.3 "Proof Test" for Solenoid valves 72-SOV-214A/B

Refer to section 4.2.14, in document (reference [3]) 0418D20SD04 Safeguarding requirements for further MOS information and requirements.

72-SOV-214A (72-SOV-214B) "Proof Test" includes testing of the associated "Cartridge Valve" (CRV) 72-CRV-214A (72-CRV-214B).

"Proof Test" shall be monitored in DCS and executed from control room @ DCS console.

Since the pressure transmitters 72-PI-214A can detect when any of the SOVs open, then the use of this instrument can be considered as part of the SOVs fault detection capabilities (Diagnostic). BUT, a failure in any of the pressure transmitters 72-PI-214A WILL NOT make 72-SIF-213 to fail on demand (NO effect).
This means that pressure transmitter and associated SOVs shall be considered a combined SIF device.

Once ALL SAFETY and PERMISSION procedures are completed and approved, MAINTENANCE personnel can:

a) "Activated" 72-MOS-214A-O (or 72-MOS-214B-O).
b) Wait until 72-PI-213B measured pressure is stable.
c) Initiate "Proof Test" via push button 72-HS-214A-O (or 72-HS-214B-O).
d) 72-PI-213B pressure shall increase (decrease) up to a stable value in less than 2.0 sec. to consider "Proof Test" completed successfully.

The Fail/Success completion criterion for this "Proof Test" is:

- **SUCCESFUL** From DCS it was possible to verify that 72-PI-213B can detect when 72-SOV-213A (72-SOV-213B) opens, and this SOV closed after 10 sec after trip command was sent.
- **UNSUCCESSFUL** From DCS it **WAS NOT** possible to verify that 72-PI-213B can detect when 72-SOV-213A (72-SOV-213B) opens, or this SOV DID NOT close after 10 sec after trip command was sent.
- **FAIL SAFE** "Proof Test" was aborted by any other mean.

5.15.4 "Proof Test" for Turbine Trip valve 72-ESDV-213

The Emergency shutdown valve 72-ESDV-213 "Proof Test" is executed with a separate facility, because the opening of this valve should be quick and SOV/CRV **ARE NOT** designed to execute a controlled ESDV stroke.

The turbine trip valve 72-ESDV-213 "Partial Valve Stroke Test" (PVST) facility is a separate system that is not described in this document.

The 72-ESDV-213 PVST facility is normally blocked, and it is lined-up only for testing purposes. Refer to 72-ESDV-213 VENDOR manual for further information.

5.16 Fault detection capabilities (Diagnostics) and required actions

This section is organized in the following sub-sections:

1) Turbine speed sensors 72-SI-213/214 required diagnostics.
2) "Logic Solver" and respective Input/Output cards required diagnostics.
3) "Solenoid valves" with "Cartridge valves" arrangement required diagnostics.

5.16.1 Turbine speed sensors 72-SI-213/214 required diagnostics

Since the turbine speed sensors connection to SIS is via pulse signal, Turbine VENDOR shall provide "Diagnostics" logics and calculations to be implemented in the "Logic Solver", like: Spike rejection, identify signal constant value (or ZERO[0.0]), and other diagnostics.

If a "Dangerous Detected" failure is identified in ONLY one of the speed sensors, then the 1oo2 "Decision Logic" associated to these sensors shall be degraded to 1oo1, or the sensor in failure set in SAFE state in the "Logic Solver". In this case, only one speed sensor can initiate a SIF demand.

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

If a "Dangerous Detected" failure is identified in BOTH speed sensors 72-SI-213A/B, then the "Logic Solver" shall initiate a SIF demand (**NO** MTTR delay applies). In this way, turbine safety **IS NOT** compromised.

5.16.2 "Logic Solver" and respective Input/Output cards required diagnostics

The "Logic Solver" and respective Input/Output cards shall include:

a) "Fault detection capabilities" (Diagnostics).
b) Pre-configured functionality to allow:
   - "Logic Solver" to make decisions according to "Diagnostic" results.
   - To show (or transmit) statuses in DCS (Console Operator), about operation and "Diagnostic" statuses of all SIF devices connected to "Logic Solver".

ONLY the input card:

c) **SHALL NOT** trip when a "Detected Failure" occurs in the same input card, and the 1oo2 "Decision Logic" associated to this input card 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).

d) **SHALL NOT** trip valve when a "Detected Failure" occurs in the associated speed sensor.

ONLY the "Logic Solver" shall:

e) Include additional circuitry to allow this device to perform the 1oo1D "Decision Logic".

f) Trip the turbine trip valve 72-ESDV-213 when a "Detected Failure" occurs in the "Logic Solver".

g) Trip the turbine trip valve 72-ESDV-213 when "Detected Failures" occur in both input channels. It means, to trip 72-ESDV-213 when any combination failure in Table 5 occurs.

h) Include 3rd party VENDOR "Diagnostic" logics and calculations to reveal speed sensors "Detected failures".

ONLY the "Logic Solver" Output cards shall include:

i) Additional circuitry to allow this device to perform the 1oo1D "Decision Logic".

j) To trip the turbine trip valve 72-ESDV-213 when a "Detected Failure" occurs in the output card.

Table 5 – Speed sensors and input cards combination failures that shall initiate a 72-SIF-213 demand (automatic from diagnostics)

	Input Channel 01		Input Channel 02	
Combination case number	**Speed sensor 72-SI-213**	**Input card IC-72-SI-213**	**Speed sensor 72-SI-214**	**Input card IC-72-SI-214**
1	"Detected Failure"		"Detected Failure"	
2	"Detected Failure"			"Detected Failure"
3		"Detected Failure"	"Detected Failure"	
4		"Detected Failure"		"Detected Failure"

5.16.3 "Solenoid valves" with "Cartridge valves" arrangement required diagnostics

"Solenoid valves" 72-SOV-213A/B & 72-SOV-214A/B, as well as "Cartridge valves" 72-CRV-213A/B & 72-CRV-214A/B are SIF mechanical devices with NO diagnostic capabilities.

Nevertheless, the use of the pressure transmitters 72-PI-213A/B can provide fault detection capabilities to these mechanical devices for SIF purposes.

Refer to sections 5.15.2 & 5.15.3, and Table 4 for further information.

5.17 Maintenance provisions

Refer to:

- Table 6 for 60-SIF-500 description of basic facilities for MAINTENANCE.
- Section 4.2.17, document (reference [4]) 0418D20SD04 Safeguarding requirements for further information.

72-SIF-213 installation shall be done in such a way that:

a) When an "Out Of Service" (OOS) tag is active, MAINTENANCE personnel shall be able to isolate the related 72-SIF-213 devices,
b) To manually command it, if it is required,
c) To Restore/Fix the related 72-SIF-213 devices.
d) BUT NONE of the above actions **SHALL NOT** initiate a 72-SIF-213 demand.

The ONLY exception to the above listed requirements are:

1) MAINTENANCE can be applied to the turbine trip valve 72-ESDV-213 ONLY during turbine maintenance overhaul. Only "Full Valve Stroke Test" (FVST) can be applied.
2) Speed sensors can be tested, BUT they can be deinstalled for MAINTENANCE during turbine maintenance overhaul.

Table 6 – 72-SIF-213 description of facilities for MAINTENANCE

#	Device's Tag	Type	MOS Tag (2)(3)	OOS Tag (1)	MAINTENANCE facility Description
1	72-SI-213	Initiator	72-MOS-213-I	72-OOS-213-I	Longer time MAINTENANCE than MTTR can be applied after OOS activation.
	IC-72-SI-213	Input			
2	72-SI-214	Initiator	72-MOS-214-I	72-OOS-214-I	Longer time MAINTENANCE than MTTR can be applied after OOS activation.
	IC-72-SI-214	Input			
3	OC-72-SOV-213A	Output	72-MOS-213A-O	72-OOS-213-O	Longer time MAINTENANCE than MTTR can be applied after OOS activation, and 72-HV-01A/03A shall be locked closed. 72-HV-02A is used to slowly re-pressurize SOV arrangement. **(4)**
	PI-SOV-CRV-213A	Output			
4	OC-72-SOV-213B	Output	72-MOS-213B-O		
	PI-SOV-CRV-213B	Output			
5	OC-72-SOV-214A	Output	72-MOS-214A-O	72-OOS-214-O	Longer time MAINTENANCE than MTTR can be applied after OOS activation, and 72-HV-01B/03B shall be locked closed. 72-HV-02B is used to slowly re-pressurize SOV arrangement. **(4)**
	PI-SOV-CRV-214A	Output			
6	OC-72-SOV-214B	Output	72-MOS-214B-O		
	PI-SOV-CRV-214B	Output			
7	72-ESV-213	Output	72-MOS-213		Maintenance can be applied only during Turbine K-1122 shutdown.

Note 1: OOS tag shall be "Activated" to avoid MOS shutdown after MTTR.

Note 2: Only one(1) MOS can be "Activated" at the time, or none if other MOS are already activated in the same "MOS Group".

Note 3: Above "Note 2" DOES NOT apply for MOS AUTOMATIC activation. Refer to section 4.2.14, in document (reference [3]) 0418D20SD04 Safeguarding requirements for further MOS information.

Note 4: 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.

5.18 Adjustments and Modifications according to operation modes and/or the project phases

N/A