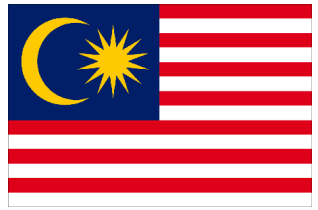
Arjen de Koning

YOKOGAWA

FS Expert
(TÜV Rheinland
#144/09, SIS/FSM)

Work in Functional Safety (Yokogawa) since 1992.
Various positions in Project management & Project Engineering.



With Yokogawa Malaysia from 2004 - 2022

Certified in 2009:	TÜV Rheinland FS Expert (SIS/FSM)
2011	TÜV Rheinland FS Eng Trainer
2017	TÜV Rheinland FS Technician Trainer

- HAZOP / SIL Classification Facilitator
- FSM Manager
- FS Auditor
- Project Safety assessments and (Site) validation Assessor
- Functional Safety trainings
- Member of MT61508-1/2, MT61508-3 & MT61511
- **Proof Test Consultancy**

YOKOGAWA

Co-innovating tomorrow™

5TH EUROPEAN CONFERENCE 2025

ON PLANT & PROCESS SAFETY

16 & 17 DECEMBER 2025

Proof Testing SIL Loops - Practical Experiences

EPSC

Arjen de Koning

FS Expert (TÜV Rheinland #144/09, SIS)

Yokogawa Europe B.V., The Netherlands

December, 2025

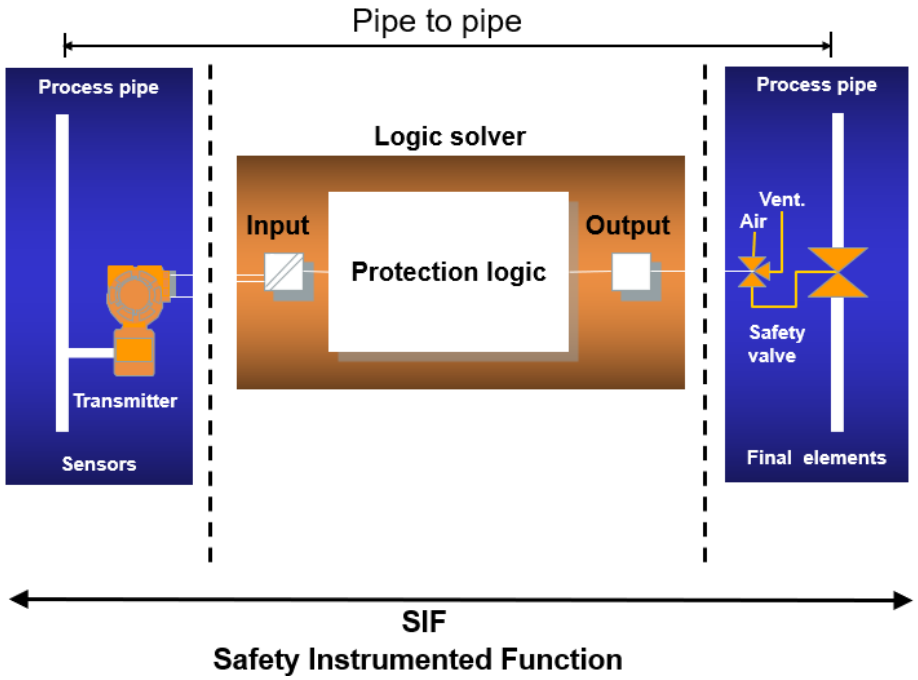
Agenda

1. Proof test in IEC61511
2. Proof Test Project
   I. Preparation - Collection
   II. Creation of Proof Test Dossiers
   III. Execution of Proof Test
   IV. Analysis of Proof Test Results
3. Results of some other Proof Test execution
4. Take away

IEC 61511-1:2016; Clause 16 SIS operation and maintenance

16.3.1 Proof testing

16.3.1.1 Periodic proof tests shall be conducted using a written procedure to **reveal undetected faults** that prevent the SIS from operating in accordance with the SRS



16.3.1.2 The entire SIS shall be tested including the sensor(s), the logic solver and the final element(s) (e.g., shutdown valves and motors).

NOTE Testing of the SIS can be performed either end-to-end or in segments (see 11.8.1).

16.3.1.3 The schedule for the proof tests shall be according to the SRS. The frequency of proof tests for a SIF shall be determined through PFDavg or PFH calculation in accordance with 11.9 for the SIS as installed in the operating environment.

NOTE **Different parts of the SIS can require different test intervals,** for example, the logic solver can require a different test interval than the sensors or final elements

IEC 61511-1:2016; Clause 16 SIS operation and maintenance

16.3.1 Proof testing

16.3.1.4 Any deficiencies found during the proof testing shall be repaired in a safe and timely manner. A proof test **shall be repeated** after the repair is completed.

16.3.1.5 At some periodic interval (determined by the user), **the frequency of testing shall be re-evaluated** based on various factors including historical test data, plant experience and hardware degradation.

16.3.1.6 Any change to the application program requires full validation and a proof test of any SIF impacted by the change. Exceptions to this are allowed if appropriate review and partial testing of changes are carried out to ensure the changes were designed per the updated safety requirements and correctly implemented.

16.3.1.7 Suitable management procedures shall be applied to review deferrals and prevent significant delay to proof testing.

What is Proof Test

A proof test means a complete test of the SIF.

The purpose of the proof test is to reveal all undetected failures that are present in the SIF

After the proof test the elements in the SIF should be in their initial state

SIF must be tested completely

Also allowed to split it in sensor, LS and final elements and test separately

Also allowed to use (false) trip as a proof test, if recorded that actions were successful.

Proof test does not mean only a functionality check confirming the (expected) function of the complete SIF or SIF input only!

BUT……

What about:

16.3.2 Inspection

Each SIS shall be periodically visually inspected to ensure there are no unauthorized modifications and no observable deterioration (e.g., missing bolts or instrument covers, rusted brackets, open wires, broken conduits, broken heat tracing, and missing insulation).

NOTE These problems could indicate an increase in the frequency of faults.

And ….. Documentation (Part of Proof Test Dossier)

16.3.3 Documentation of proof tests and inspection

The user shall maintain records that certify that proof tests and inspections were completed as required. These records shall include the following information as a minimum:

a) description of the tests and inspections performed including identification of the test procedure used;

b) dates of the tests and inspections;

c) name of the person(s) who performed the tests and inspections;

d) serial number or other unique identifier of the system tested (e.g., loop number, tag number, equipment number, and SIF number);

e) results of the tests and inspection including the “as-found” condition, all faults found (including the failure mode) and the "as-left" condition.

Let’s do Proof test!

Easier said then done

Client:

- Original HAZOP report is not available.
- SIL classification was done for this existing site based on the crosses (X) on the C&E.

After SIL Classification;

Proof testing is a KPI for the Facility Functional Safety compliance

But nothing available.

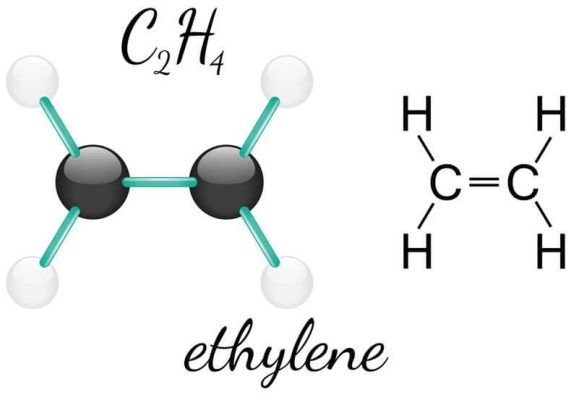
Start from Scratch

2. Proof Test Preparation: Project Scope

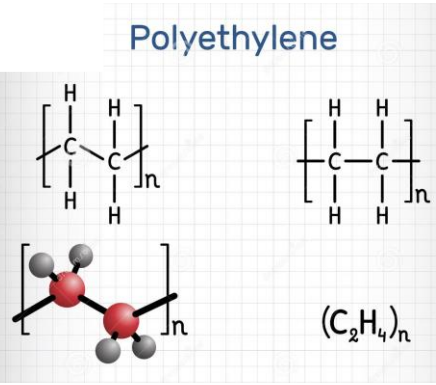
Site: Ethylene / Polyethylene Plant

Built in mid 90's

Ethylene C_2H_4 Plant –
157 SIF's **96 +16 Selected during Site** SIL 0 - 3



Polyethylene $(C_2H_4)_n$ Plant –
52 SIF's **48 selected** SIL 1 - 3



Note: > 40% of the SIF's are SIL 3 rated

2. Proof Test Preparation: Project Team

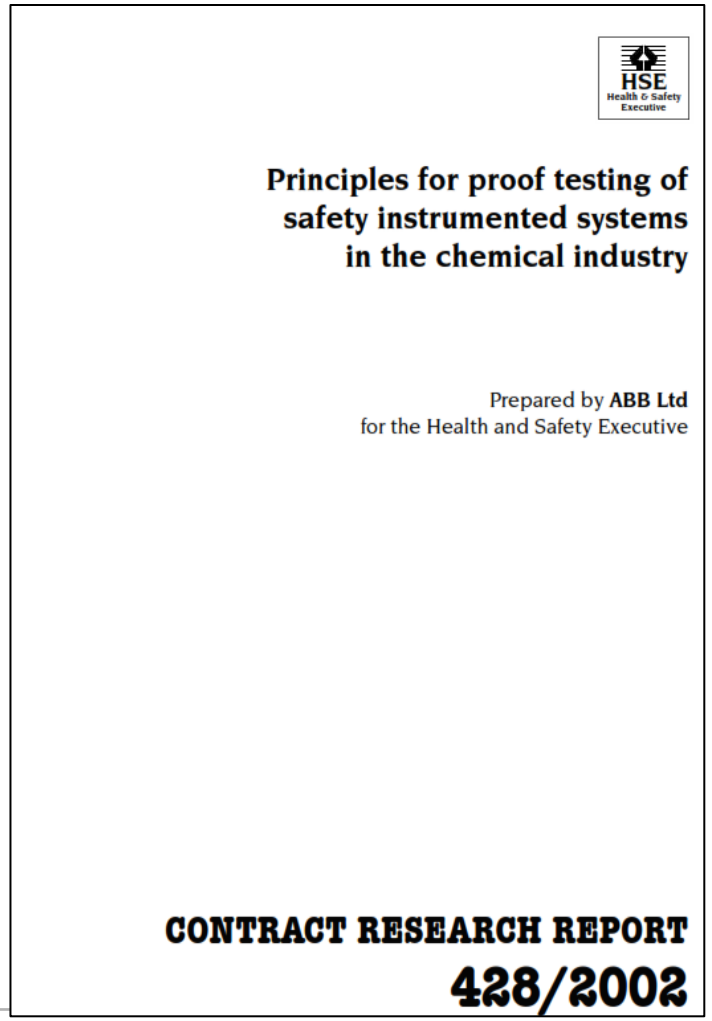
Project team: 1 Lead with 5 safety engineers

- 4 months preparing the 144 SIF proof test dossier.
- 4 weeks at site – Actual Proof Test Execution

- What is needed to Create this Proof test procedure & Dossier?

2. Proof test Preparation: Proof Test Procedure & Dossier

- **IEC-61511 Standard**
- **HSE UK crr428/2002 (OG54)**
- Safety Manuals of each device in the SIF
  - Proof test procedure/methodology devices
  - Proof Test coverage of each device
- Application logic and settings/Parameters
- P&ID
- Datasheets



2. Proof test Preparation: Proof Test Procedure

What is needed to Creation of Proof test procedure

- IEC-61508/61511 Standards
- HSE UK crr02428

- **Safety Manuals of all devices in the SIF**
  - **Proof test procedure/methodology of the devices**
  - **Proof Test coverage of these devices**
- Application logic and settings/Parameters
- P&ID
- Datasheets

Technical Information

Functional Safety Manual

DPharp EJX™
DPharp EJA™

TI 01C25A05-01EN

Contents

2. Proof test Preparation: Proof Test Methodology & Coverage

Transmitters

Testing method	Tools required	Expected outcome	Remarks
Functional test: 1. Follow all Management of Change procedures to bypass logic solvers if necessary. 2. Execute HART/BRAIN command to send value to high alarm (21.6 mA) and verify that current has reached this level. 3. Execute HART/BRAIN command to send value to low alarm (3.6 mA) and verify that current has reached this level. 4. Restore logic solvers operation and verify.	• Handheld terminal	Proof Test Coverage =52%	The output needs to be monitored to assure that the transmitter communicates the correct signal.
Perform three point calibration along with the functional test listed above.	• Handheld terminal • Calibrated pressure source	Proof Test Coverage =99%	

PTC test sequence A [5]	88 %	
PTC test sequence B [6]	34 %	38 %
PTC test sequence C [7]	-	88 %

1) This value takes into account failure types relevant to the function of the electronic components according to Siemens SN29500.
2) During this time, all diagnostic functions are executed at least once.
3) Time between error detection and error response.
4) Step response time as per DIN EN 61298-2.
5) Proof test coverage when the level is approached, or when the sensor is removed and the tines are immersed in a medium of similar density and viscosity.
6) Proof test coverage when simulation is performed on the Nivotester by activating the test button.
7) Proof test coverage when checking the switch point under reference operating conditions.

Valve / Actuator Assembly

Proof Test Coverage (PTC) / Diagnostic Coverage (DC)
Considering the application of the above described Test procedure, the "Test Coverage", in case of automatic procedure, can be considered > 99% (it will be lower in case of imperfection/incompleteness of the test procedure and/or use of not calibrated/adequate equipment).
In case of manual procedure the "Test Coverage" shall take into account also the test imperfection and the reliability/competence of the operator.

6.2 Full Stroke Test

The "Full Stroke Test" ("On-line") must be performed to satisfy the PFDAVG (average probability of failure on demand) value.

The full test frequencies will be defined from the final integrator, in relation to the defined SIL level to achieve.

Procedure:

- Operate the Actuator/Valve assembly for an open/close complete cycle, with complete opening - closing of the valve.
- Verify the Correct performing of open – close manoeuvre (e.g. check locally, or automatically, via Logic solver, the correct movement of the actuator/valve).

Considering the application of the above described Full Stroke Test procedure, the "Test Coverage" can be considered 99%.

2. Proof test Preparation: Proof Test Methodology & Coverage

Valve (PTC?)

6.2 Full Stroke + Leak Test

The "Full Stroke + Leak Test" ("On line") must be performed to satisfy the PFD_{AVG} (average probability of failure on demand) value.
The test frequencies shall be defined from the final integrator in relation to the defined SIL grade to achieve.

Procedure for Full Stroke Test

- Operate the Actuator/Valve assembly for No. 2 open/close complete cycles with complete closing of the valve.
- Verify the correct performing of open – close manoeuvre (e.g. check locally, or automatically via Logic solver, the correct movement of the actuator/valve).

The achievement of the safe position (open or closed) shall be confirmed with the control of:

- The OPEN/CLOSED indications on actuator and the relative feedback to the logic solver, if existing. (see the specific actuator operating manual for details)
- The mechanical position indicator on actuator and/or valves, if existing; (see the specific actuator operating manual and/or the valve assembly drawing for details)

Procedure for Leak Test On Line
The Valve assembly shall be operated in order to reach the closed position.
(The closed position shall be verified and confirmed as described above).
Then, the pressure value shall be checked using the manometers or automatic system installed on line, upstream of the valve: the absence of the seat leakage shall be confirmed by any pressure loss.
With the available plant facilities, the seat leakage can also be measured downstream of the valve and read by the logic solver.

SOV

Mode of Operation		Low Demand
Proof Test Coverage	PTC	92 %
Partial Stroke Test Coverage	PSTC	70 %

SOV (PTC?)

3.2.1 Suggested Proof Test

The suggested proof test consists of a full stroke of the final element actuator and valve. It is assumed that the BXS valve is able to perform the safety function properly if the final element reaches the safety state within the specified safety time.

Step Action
1 Bypass the safety function and take appropriate action to avoid a false trip
2 De-energise the BXS Valve to force the actuator and valve to the fail-safe state and confirm that the safe state was achieved and within the correct time.
3 Return the BXS valve to the energised state and inspect the final element for any leaks, visible damage or contamination and confirm that the normal operating state was achieved.
4 Remove the bypass otherwise restore normal operation.

No Proof Test Coverage
What to choose?

90% ? or……

Proof Test is not a Diagnostic Test …

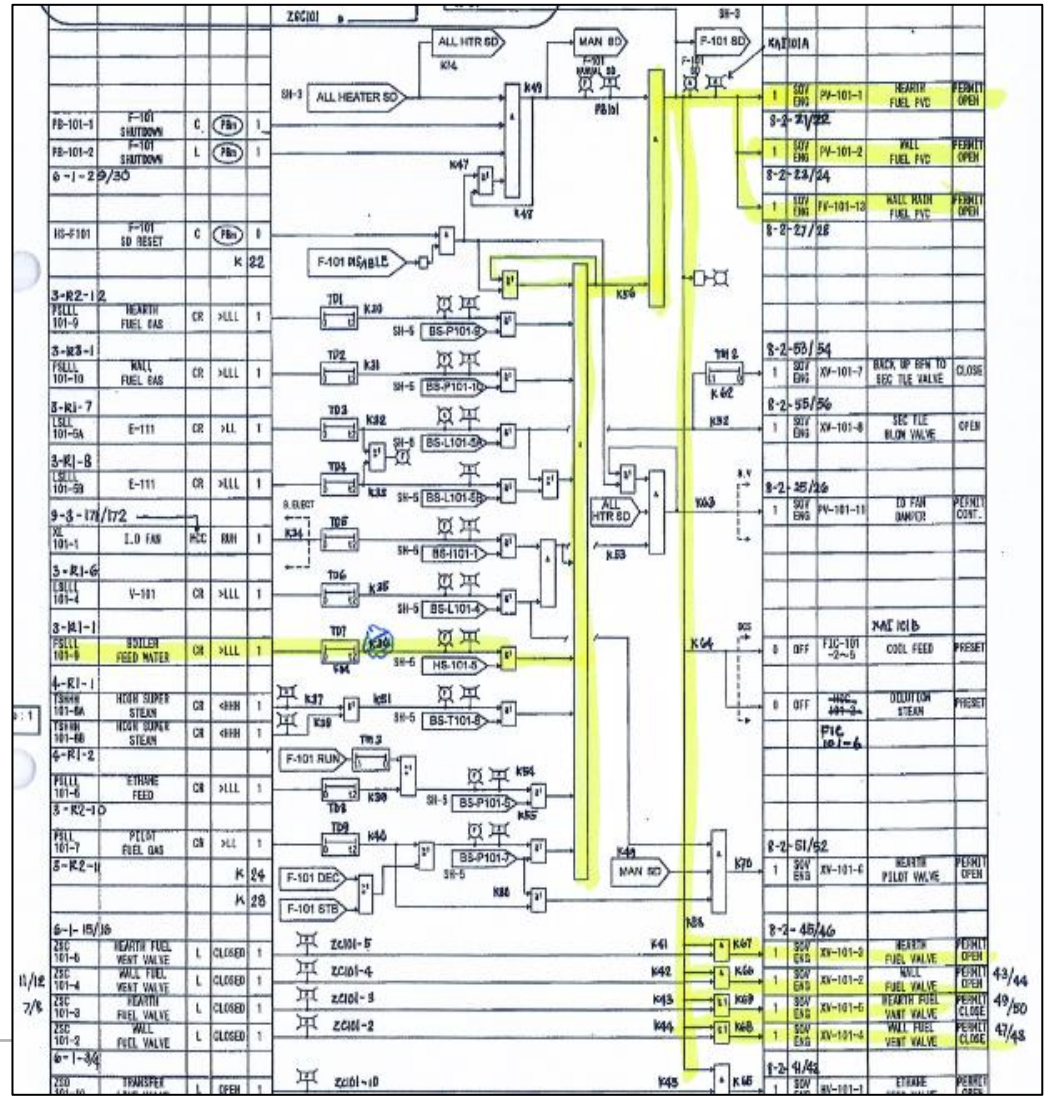
PTC ≠ DC

2. Proof test Preparation: Proof Test Procedure

What is needed to Creation of Proof test procedure

- IEC-61508/61511 Standards
- HSE UK crr02428
- Safety Manuals of each device in the SIF
  - Proof test procedure/methodology devices
  - Proof Test coverage of each device

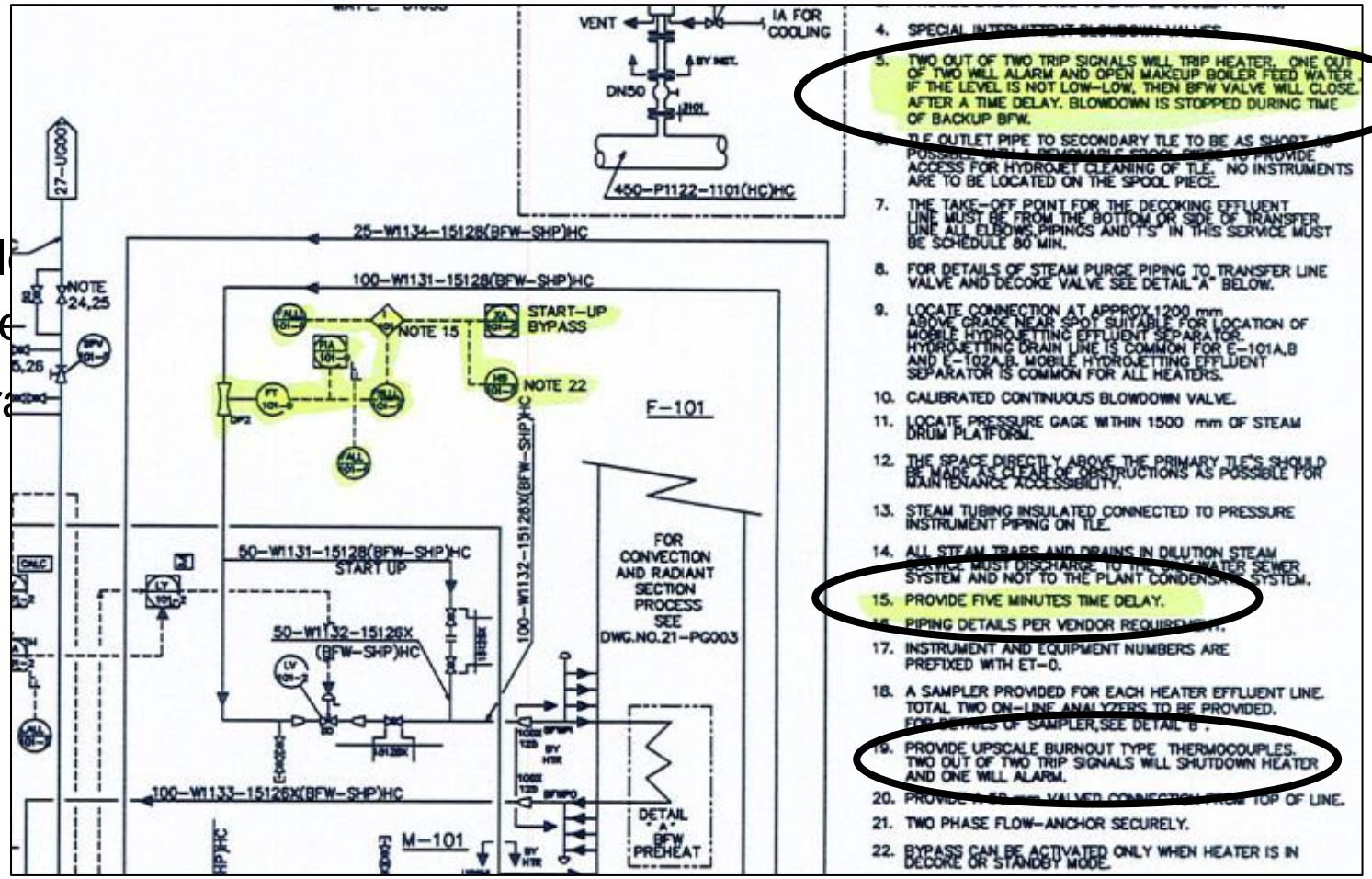
- **Functional Logic Diagrams and/or C&E and/or safety narratives and (any) settings/Parameters**
- P&ID
- Datasheets



2. Proof test Preparation: Proof Test Procedure

What is needed to Creation of Proof test procedure

- IEC-61508/61511 Standards
- HSE UK crr02428
- Safety Manuals of each device in
  - Proof test procedure/methodol
  - Proof Test coverage of each de
- Application logic and settings/Para
- **P&ID's**
- Datasheets



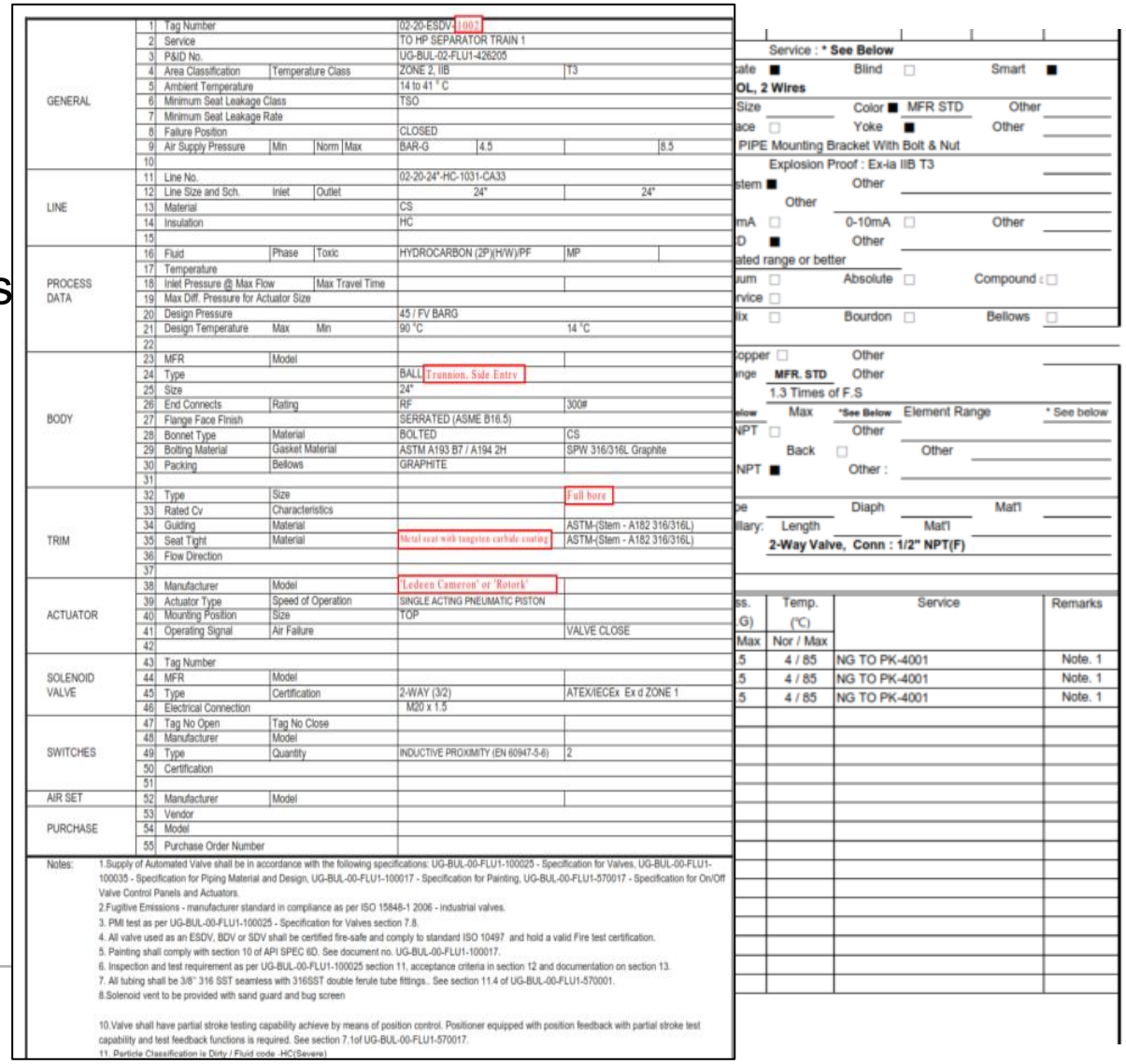
2. Proof test Preparation: Proof Test Procedure

What is needed to Creation of Proof test procedure

- IEC-61508/61511 Standards
- HSE UK crr02428
- Safety Manuals of each device in the SIF
  - Proof test procedure/methodology devices
  - Proof Test coverage of each device
- Application logic and settings/Parameters
- P&ID

- **Datasheets:**

  Sensors, Final Elements



GENERAL	1	Tag Number			02-20-ESDV-1003			
	2	Service			TO HP SEPARATOR TRAIN 1			
	3	P&ID No.			UG-BUL-02-FLU1-426205			
	4	Area Classification	Temperature Class		ZONE 2, IIB	T3		
	5	Ambient Temperature			14 to 41 ° C			
	6	Minimum Seat Leakage Class			TSO			
	7	Minimum Seat Leakage Rate						
	8	Failure Position			CLOSED			
	9	Air Supply Pressure	Min	Norm Max	BAR-G	4.5		8.5
	10							
LINE	11	Line No.			02-20-24"-HC-1031-CA33			
	12	Line Size and Sch.	Inlet	Outlet	24"	24"		
	13	Material			CS			
	14	Insulation			HC			
	15							
PROCESS DATA	16	Fluid	Phase	Toxic	HYDROCARBON (2P)(H/W)/PF	MP		
	17	Temperature						
	18	Inlet Pressure @ Max Flow	Max Travel Time					
	19	Max Diff. Pressure for Actuator Size						
	20	Design Pressure			45 / FV BARG			
	21	Design Temperature	Max	Min	90 °C	14 °C		
	22							
BODY	23	MFR	Model					
	24	Type			BALL Trunnion, Side Entry			
	25	Size			24"			
	26	End Connects	Rating		RF	300#		
	27	Flange Face Finish			SERRATED (ASME B16.5)			
	28	Bonnet Type	Material		BOLTED	CS		
	29	Bolting Material	Gasket Material		ASTM A193 B7 / A194 2H	SPW 316/316L Graphite		
	30	Packing	Bellows		GRAPHITE			
	31							
TRIM	32	Type	Size			Full bore		
	33	Rated Cv	Characteristics					
	34	Guiding	Material			ASTM-(Stem - A182 316/316L)		
	35	Seat Tight	Material		Metal seat with tungsten carbide coating	ASTM-(Stem - A182 316/316L)		
	36	Flow Direction						
	37							
ACTUATOR	38	Manufacturer	Model		'Ledeen Cameron' or 'Rotork'			
	39	Actuator Type	Speed of Operation		SINGLE ACTING PNEUMATIC PISTON			
	40	Mounting Position	Size		TOP			
	41	Operating Signal	Air Failure			VALVE CLOSE		
	42							
SOLENOID VALVE	43	Tag Number						
	44	MFR	Model					
	45	Type	Certification		2-WAY (3/2)	ATEX/IECEx Ex d ZONE 1		
	46	Electrical Connection			M20 x 1.5			
SWITCHES	47	Tag No Open	Tag No Close					
	48	Manufacturer	Model					
	49	Type	Quantity		INDUCTIVE PROXIMITY (EN 60947-5-6)	2		
	50	Certification						
	51							
AIR SET	52	Manufacturer	Model					
PURCHASE	53	Vendor						
	54	Model						
	55	Purchase Order Number						

Notes:
1.Supply of Automated Valve shall be in accordance with the following specifications: UG-BUL-00-FLU1-100025 - Specification for Valves, UG-BUL-00-FLU1-100035 - Specification for Piping Material and Design, UG-BUL-00-FLU1-100017 - Specification for Painting, UG-BUL-00-FLU1-570017 - Specification for On/Off Valve Control Panels and Actuators.
2.Fugitive Emissions - manufacturer standard in compliance as per ISO 15848-1 2006 - industrial valves.
3. PMI test as per UG-BUL-00-FLU1-100025 - Specification for Valves section 7.8.
4. All valve used as an ESDV, BDV or SDV shall be certified fire-safe and comply to standard ISO 10497 and hold a valid Fire test certification.
5. Painting shall comply with section 10 of API SPEC 6D. See document no. UG-BUL-00-FLU1-100017.
6. Inspection and test requirement as per UG-BUL-00-FLU1-100025 section 11, acceptance criteria in section 12 and documentation on section 13.
7. All tubing shall be 3/8" 316 SST seamless with 316SST double ferule tube fittings.. See section 11.4 of UG-BUL-00-FLU1-570001.
8.Solenoid vent to be provided with sand guard and bug screen

10.Valve shall have partial stroke testing capability achieve by means of position control. Positioner equipped with position feedback with partial stroke test capability and test feedback functions is required. See section 7.1of UG-BUL-00-FLU1-570017.
11. Particle Classification is Dirty / Fluid code -HC(Severe)

Service : * See Below
ate ■ Blind □ Smart ■
OL, 2 Wires
Size Color ■ MFR STD Other
ace □ Yoke ■ Other
PIPE Mounting Bracket With Bolt & Nut
Explosion Proof : Ex-ia IIB T3
stem ■ Other
Other
mA □ 0-10mA □ Other
D ■ Other
ated range or better
ium □ Absolute □ Compound □
rvice □
lix □ Bourdon □ Bellows □
opper □ Other
nge MFR. STD Other
1.3 Times of F.S
elow Max *See Below Element Range * See below
NPT □ Other
Back □ Other
NPT ■ Other :
pe Diaph Mat'l
illary: Length Mat'l
2-Way Valve, Conn : 1/2" NPT(F)

ss. G) Max	Temp. (°C) Nor / Max	Service	Remarks
.5	4 / 85	NG TO PK-4001	Note. 1
.5	4 / 85	NG TO PK-4001	Note. 1
.5	4 / 85	NG TO PK-4001	Note. 1

2. II. Creation of Proof Test Dossier

What is needed for the Proof test Procedure?

- First check **(Inspection):** Basic Preparation, Visual Inspection and Spare parts
- Combine all SIF devices proof test procedures in 1 comprehensive SIF proof test procedure

Also include all possible application functions to reveal **undetected faults**, e.g.:

- Out of range behavior
- MOS/Interlock behavior
- di/dt behavior / Rate of rise behavior
- Voting (1oo2 / 2oo2/ 2oo3/ 2oo4 /1oo3)
- Line fault behavior
- HH/LL trip(s)
- Hysteresis behavior
- Input Discrepancy Behavior
- Hart settings for Smart equipment
- Cybersecurity (Smart Devices: Write protect)
- Valve position (and/or other) feedback requirements. Leak test requirements

Result:

Simple SIF 1oo1 (I/O)	app. 20-25 steps	Actual test takes app. 1 -1.5 hour
Complex SIF 2oo3 (I)/1oo2 (O)	app. 40-60 steps	Actual test takes app. 3 - 4 hours

2. II. Pressure Transmitter Low Test (1oo1) ; Yokogawa EJX Pressure transmitter.

Step	Pressure Transmitter Test (1oo1) Sequence	OK
1.	JHA completed. Valid PERMIT TO WORK available.	
2.	Inform Technician(s) in the field which pressure transmitter and valves are to be tested.	
3.	Verify Mechanical Integrity pressure transmitter & Valves. Refer to calibration test report results.	
4.	Follow end-user bypass procedures to bypass the RS logic solvers. Pressure transmitter ready to be proof tested with handheld terminal	
5.	Parameter settings verification: Burnout direction switch: Output to 21.6 mA upon detection of internal Failure. Write protection Switch: Enabled	
6.	Execute HART/BRAIN command to send value to high alarm (21.5 mA /109.4%) and verify that current has reached this level. • Verify transmitter Fault (High) alarm at 21mA/106.3%) in SIS and DCS	
7.	Execute HART/BRAIN command to send value to low alarm (3.6 mA/--2.5%) and verify that current has reached this level. • Verify transmitter Fault (Low) alarm at 3.8mA/-1.25%) in SIS and DCS	
8.	Restore RS logic solvers operation and verify. *Note: Point 5-8 provides a transmitter proof test coverage of 52%.*	
9.	Remove the bypass and confirm pressure transmitter is operational.	
10.	Re-confirm with the Technician(s) in the field which pressure transmitter and which valves are to be tested.	
11.	Isolate the Impulse Lines, Slowly open the Vent Valve to allow the pressure to fall **SLOWLY.**	
12.	The **Low (Low)** process alarm (1st point calibration) will be initiated. • Record the Field value reading (via Handheld terminal) • Record the SIS reading. • Verify Annunciator alarm on SIS and DCS (& SOE recorder)	
13.	Continue to allow pressure to fall until the **Low Low (Low)** process trip (2nd point calibration) is initiated. • Record the Field value reading (via Handheld terminal) • Record the SIS reading. • Record the time of initiation. • Verify the Trip alarm on SIS and DCS (& SOE recorder)	

Step	Pressure Transmitter Test (1oo1) Sequence	OK
14.	Check that the valve(s) (XV, FV and/or PV) have tripped closed in accordance with the Interlock Diagrams. • Verify the for XV's the limit switch ZSC is activated. • Record the time of valve closure	
15.	Check and record the zero reading of the transmitter at process pressure (3rd point calibration). If the error is more than 2% (EJX Safety Accuracy) then the test has Failed. Note: Point 6-8, 12, 13 and 15 provides a transmitter proof test coverage of 99%.	
16.	Recommission the pressure transmitter.	
17.	When process conditions are stable reset the trip via the SD reset button	
18.	Check that the annunciator & Trip alarms returned to a healthy condition.	
19.	If any part of the system failed to operate correctly or if the reading did not correspond with the required (on the P&ID) annunciator or trip setting then the test has failed. Check each item of the loop. Repair and re-test where necessary. If extensive repair has to be carried out then a punchlist will be created and the end-user will be informed.	
20.	Check that process conditions and annuciation(s) have returned to normal. Ensure valves are return to normal.	
21.	Inform Technician(s) in the field that testing is completed	
22.	**End of Pressure Transmitter Test (1oo1) Sequence**	

2. II. Creation of Proof Test Dossier

Appendices for the used Documents (Mark up to show proof test results)

- SIL report Particular SIF
- P&ID
- Interlock Logic Diagram (FLD's)
- Loop drawings
- Termination Diagrams
- Application Logic printout
- Punch item record
- SIL Calculation
- Proof Test Check sheet (Inspection)
- Data sheets of all Equipment
- Safety Manuals of all equipment

Appendix I
Punch List Proof Test
Number of pages that follow : 1

Appendix II
Proof Test Check Sheet F-101 SIF PSLLL-101-7
Number of pages that follow: 1

Appendix III
Reliability Calculation PSLLL-101-7 SIF 30
Number of pages that follow : 3

Appendix IV
IPF Report F-101 Safety Function Classification Sheet
Number of pages that follow : 1

Appendix V
P&ID Cracking Heater Absorbed Duty F-101
Number of pages that follow : 2

Appendix VI
Interlock Logic Diagram
Number of pages that follow : 1

Appendix VII
Loop Drawings F-101 SIF 30
Number of pages that follow : 10

Appendix VIII
Termination Drawings
Number of pages that follow : 3

Appendix IX
Application Logic (Furnace)
Number of pages that follow : 4

2. II. Creation of Proof Test Dossier: Appendix Proof test Check Sheet

TOP SECT

Plant ID

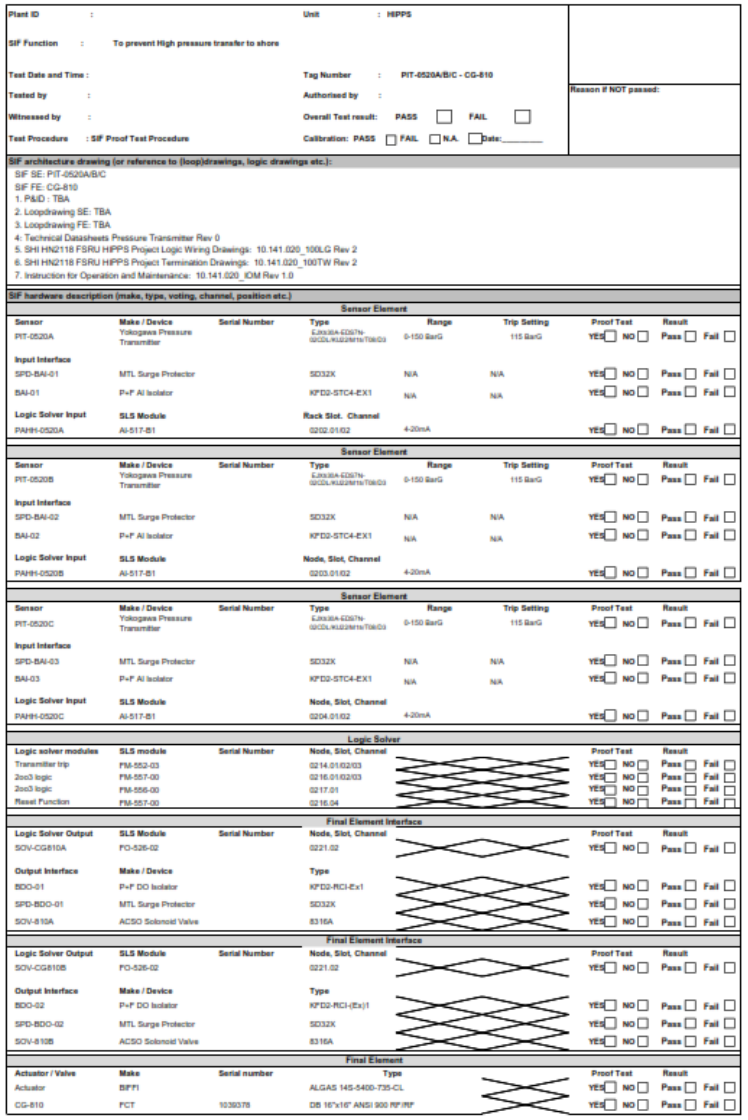
SIF Function

Test Date and Tir

Tested by

Witnessed by

Test Procedure



Plant ID : Unit : HIPPS

SIF Function : To prevent High pressure transfer to shore

Test Date and Time : Tag Number : PIT-0520A/B/C - CG-810

Tested by : Authorised by :

Witnessed by : Overall Test result: PASS ☐ FAIL ☐

Test Procedure : SIF Proof Test Procedure Calibration: PASS ☐ FAIL ☐ N.A. ☐ Date:_____

Reason if NOT passed:

SIF architecture drawing (or reference to (loop)drawings, logic drawings etc.):

SIF SE: PIT-0520A/B/C
SIF FE: CG-810
1. P&ID : TBA
2. Loopdrawing SE: TBA
3. Loopdrawing FE: TBA
4: Technical Datasheets Pressure Transmitter Rev 0
5. SHI HN2118 FSRU HIPPS Project Logic Wiring Drawings: 10.141.020_100LG Rev 2
6. SHI HN2118 FSRU HIPPS Project Termination Drawings: 10.141.020_100TW Rev 2
7. Instruction for Operation and Maintenance: 10.141.020_IOM Rev 1.0

SIF hardware description (make, type, voting, channel, position etc.)

Sensor Element

Sensor	Make / Device	Serial Number	Type	Range	Trip Setting	Proof Test	Result
PIT-0520A	Yokogawa Pressure Transmitter		EJX530A-ED57N-0/CDL/KU02/NS1/TG6/D3	0-150 BarG	115 BarG	YES☐ NO☐	Pass☐ Fail☐
Input Interface							
SPD-BAI-01	MTL Surge Protector		SD32X	N/A	N/A	YES☐ NO☐	Pass☐ Fail☐
BAI-01	P+F AI Isolator		KFD2-STC4-EX1	N/A	N/A	YES☐ NO☐	Pass☐ Fail☐
Logic Solver Input	**SLS Module**		**Rack Slot. Channel**				
PAHH-0520A	AI-517-B1		0202.01/02	4-20mA		YES☐ NO☐	Pass☐ Fail☐

Sensor Element

Sensor	Make / Device	Serial Number	Type	Range	Trip Setting	Proof Test	Result
PIT-0520B	Yokogawa Pressure Transmitter		EJX530A-ED57N-0/CDL/KU02/NS1/TG6/D3	0-150 BarG	115 BarG	YES☐ NO☐	Pass☐ Fail☐
Input Interface							
SPD-BAI-02	MTL Surge Protector		SD32X	N/A	N/A	YES☐ NO☐	Pass☐ Fail☐
BAI-02	P+F AI Isolator		KFD2-STC4-EX1	N/A	N/A	YES☐ NO☐	Pass☐ Fail☐
Logic Solver Input	**SLS Module**		**Node, Slot, Channel**				
PAHH-0520B	AI-517-B1		0203.01/02	4-20mA		YES☐ NO☐	Pass☐ Fail☐

Sensor Element

Sensor	Make / Device	Serial Number	Type	Range	Trip Setting	Proof Test	Result
PIT-0520C	Yokogawa Pressure Transmitter		EJX530A-ED57N-0/CDL/KU02/NS1/TG6/D3	0-150 BarG	115 BarG	YES☐ NO☐	Pass☐ Fail☐
Input Interface							
SPD-BAI-03	MTL Surge Protector		SD32X	N/A	N/A	YES☐ NO☐	Pass☐ Fail☐
BAI-03	P+F AI Isolator		KFD2-STC4-EX1	N/A	N/A	YES☐ NO☐	Pass☐ Fail☐
Logic Solver Input	**SLS Module**		**Node, Slot, Channel**				
PAHH-0520C	AI-517-B1		0204.01/02	4-20mA		YES☐ NO☐	Pass☐ Fail☐

Logic Solver

Logic solver modules	SLS module	Serial Number	Node, Slot, Channel	Proof Test	Result
Transmitter trip	FM-552-03		0214.01/02/03	YES☐ NO☐	Pass☐ Fail☐
2oo3 logic	FM-557-00		0216.01/02/03	YES☐ NO☐	Pass☐ Fail☐
2oo3 logic	FM-556-00		0217.01	YES☐ NO☐	Pass☐ Fail☐
Reset Function	FM-557-00		0216.04	YES☐ NO☐	Pass☐ Fail☐

Final Element Interface

Logic Solver Output	SLS Module	Serial Number	Node, Slot, Channel	Proof Test	Result
SOV-CG810A	FO-526-02		0221.02	YES☐ NO☐	Pass☐ Fail☐
Output Interface	**Make / Device**		**Type**		
BDO-01	P+F DO Isolator		KFD2-RCI-Ex1	YES☐ NO☐	Pass☐ Fail☐
SPD-BDO-01	MTL Surge Protector		SD32X	YES☐ NO☐	Pass☐ Fail☐
SOV-810A	ACSO Solonoid Valve		8316A	YES☐ NO☐	Pass☐ Fail☐

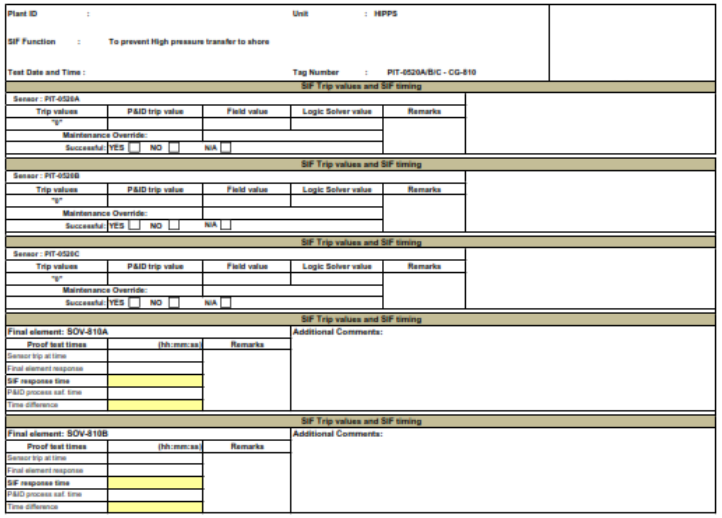
Final Element Interface

Logic Solver Output	SLS Module	Serial Number	Node, Slot, Channel	Proof Test	Result
SOV-CG810B	FO-526-02		0221.02	YES☐ NO☐	Pass☐ Fail☐
Output Interface	**Make / Device**		**Type**		
BDO-02	P+F DO Isolator		KFD2-RCI-(Ex)1	YES☐ NO☐	Pass☐ Fail☐
SPD-BDO-02	MTL Surge Protector		SD32X	YES☐ NO☐	Pass☐ Fail☐
SOV-810B	ACSO Solonoid Valve		8316A	YES☐ NO☐	Pass☐ Fail☐

Final Element

Actuator / Valve	Make	Serial number	Type	Proof Test	Result
Actuator	BIFFI		ALGAS 145-5400-T35-CL	YES☐ NO☐	Pass☐ Fail☐
CG-810	FCT	1039378	DB 16"x16" ANSI 900 RF/RF	YES☐ NO☐	Pass☐ Fail☐

PIT-0502 ABC Page 1 of 3 CHECK SHEET HIPPS PROOF TEST



Plant ID : Unit : HIPPS

SIF Function : To prevent High pressure transfer to shore

Test Date and Time : Tag Number : PIT-0520A/B/C - CG-810

SIF Trip values and SIF timing

Sensor : PIT-0520A

Trip values	P&ID trip value	Field value	Logic Solver value	Remarks
"0"				
Maintenance Override:				
Successful: YES ☐ NO ☐ N/A ☐				

SIF Trip values and SIF timing

Sensor : PIT-0520B

Trip values	P&ID trip value	Field value	Logic Solver value	Remarks
"0"				
Maintenance Override:				
Successful: YES ☐ NO ☐ N/A ☐				

SIF Trip values and SIF timing

Sensor : PIT-0520C

Trip values	P&ID trip value	Field value	Logic Solver value	Remarks
"0"				
Maintenance Override:				
Successful: YES ☐ NO ☐ N/A ☐				

SIF Trip values and SIF timing

Final element: SOV-810A Additional Comments:

Proof test times	(hh:mm:ss)	Remarks
Sensor trip at time		
Final element response		
SIF response time		
P&ID process saf. time		
Time difference		

SIF Trip values and SIF timing

Final element: SOV-810B Additional Comments:

Proof test times	(hh:mm:ss)	Remarks
Sensor trip at time		
Final element response		
SIF response time		
P&ID process saf. time		
Time difference		

PIT-0502 ABC Page 3 of 3 CHECK SHEET HIPPS PROOF TEST

☐ FAIL ☐

☐ N.A. ☐ Date:_____

Appendix: Proof test Check Sheet

SIF Hardware components Sensor configuration

SIF hardware description (make, type, voting, channel, position etc.)							
Sensor Element							
Sensor	**Device**	**Make**	**Type**	**Range**	**Trip Setting**	**Proof Test**	**Result**
PIT-0520A	PRESSURE TX	YOKOGAWA	EJX 530A			YES ☐ NO ☐	Pass ☐ Fail ☐
Input Interface	**Device**	**Make**	**Type**				
SPD-BAI-01	SURGE PROTECTOR	MTL	SD32X	N/A	N/A	YES ☐ NO ☐	Pass ☐ Fail ☐
BAI-01	AI BARRIER	P&F	KFD2-STC4-EX1	N/A	N/A	YES ☐ NO ☐	Pass ☐ Fail ☐
Logic Solver Input	**SLS Module**	**Make**	**Rack, Slot, Channel**				
PAHH-0520A	AI-517-B1	YOKOGAWA	TBA			YES ☐ NO ☐	Pass ☐ Fail ☐

SIF hardware description (make, type, voting, channel, position etc.)							
Sensor Element							
Sensor	**Device**	**Serial Number PT**	**Type**	**Range**	**Trip Setting**	**Proof Test**	**Result**
27-PT-1501A	EJX530A		GAUGE	0-110 bar	102 barg	YES ☐ NO ☐	Pass ☐ Fail ☐
Input Interface	**Device**	**Make**	**Type**				
N/A	N/A	N/A	N/A			YES ☐ NO ☐	Pass ☐ Fail ☐
Logic Solver Input	**RS Module**	**Serial Number RS**	**Node, Slot, Channel**				
27-PT-1501A	SAI143-H53		N01S01C01	Tag name - _27PT1501A		YES ☐ NO ☐	Pass ☐ Fail ☐

Appendix: Proof test Check Sheet

SIF Hardware components logic solver

Programmable Logic Solver (PE)

Logic Solver					
Controller	**RS module**	**Serial Number RS**	**Node, Slot**	**Proof Test**	**Result**
SCS0101	S2CP471-01	/	N01S09, N01S10	YES ☐ NO ☐	Pass ☐ Fail ☐

Solid state Logic Solver (E)

Logic Solver					
Logic solver modules	**SLS module**	**Serial Number**	**Node, Slot, Channel**	**Proof Test**	**Result**
Transmitter trip	FM-552-03		0214.01/02/03	YES ☐ NO ☐	Pass ☐ Fail ☐
2oo3 logic	FM-557-00		0216.01/02/03	YES ☐ NO ☐	Pass ☐ Fail ☐
2oo3 logic	FM-556-00		0217.01	YES ☐ NO ☐	Pass ☐ Fail ☐
Reset Function	FM-557-00		0216.04	YES ☐ NO ☐	Pass ☐ Fail ☐

Appendix: Proof test Check Sheet

SIF Hardware components Final Element Configuration

Final Element					
Logic Solver Output	**RS Module**	**Serial Number RS**	**Node, Slot, Channel**	**Proof Test**	**Result**
_27HY080A	SDV531-L53		N01S03C01	YES☐ NO☐	Pass☐ Fail☐
_27HY080B	SDV531-L53		N01S03C02	YES☐ NO☐	Pass☐ Fail☐
Output Interface	**Device**	**Make**	**Type**		
27-EV-080	Solonoid Valve	BIFOLD	FP05	YES☐ NO☐	Pass☐ Fail☐
27-EV-080	Actuator	Servovalve	RSOM 6000/160S	YES☐ NO☐	Pass☐ Fail☐
Valve	**Device**	**Serial Number**	**Type**		
27-EV-080	Ball Valve		T3 Type 18"	YES☐ NO☐	Pass☐ Fail☐
Logic Solver Output	**RS Module**	**Serial Number RS**	**Node, Slot, Channel**	**Proof Test**	**Result**
_27HY081A	SDV531-L53		N01S03C04	YES☐ NO☐	Pass☐ Fail☐
_27HY081B	SDV531-L53		N01S03C05	YES☐ NO☐	Pass☐ Fail☐
Output Interface	**Device**	**Make**	**Type**		
27-EV-081	Solonoid valve	BIFOLD	FP05	YES☐ NO☐	Pass☐ Fail☐
27-EV-081	Actuator	Servovalve	RSOM 6000/160S	YES☐ NO☐	Pass☐ Fail☐
Valve	**Device**	**Serial Number**	**Type**		
27-EV-081	Ball Valve		T3 Type 18"	YES☐ NO☐	Pass☐ Fail☐

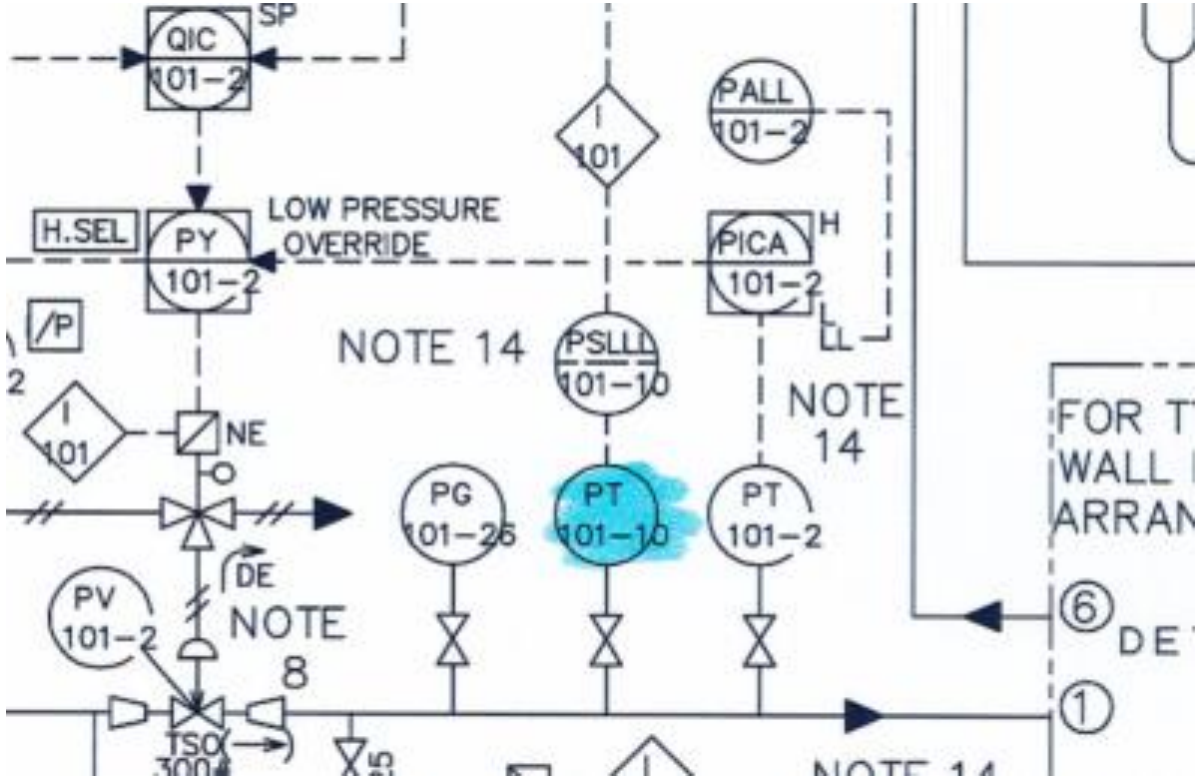
SIF Trip Values and SIF response time Timing

SIF Trip values and SIF timing				
Sensor : PIT-0520C				
Trip values	P&ID trip value	Field value	Logic Solver value	Remarks
"0"				
Maintenance Override:				
Successful:	YES ☐	NO ☐	N/A ☐	

SIF Trip values and SIF timing			
Final element: SOV-810A			Additional Comments:
Proof test times	(hh:mm:ss)	Remarks	
Sensor trip at time			
Final element response			
SIF response time			
P&ID process saf. time			
Time difference			

2. III. Proof Test: Execution at Site

What proof test scope is possible?



Proof testing of PT101-10 & PT101-2

HOW?

- Only a block valve (no bleed).

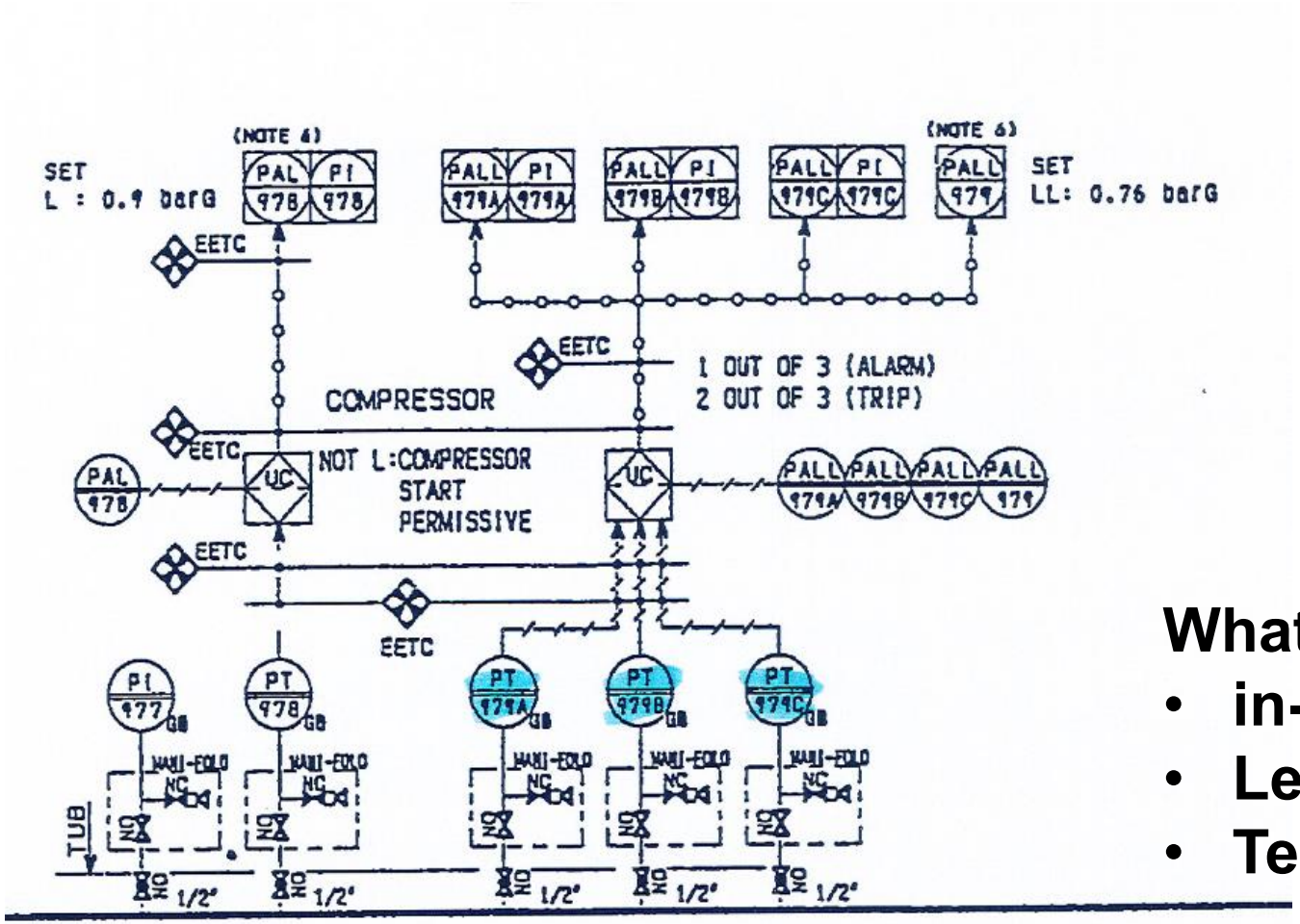
  Proof test options:
  - Remove Transmitter to test wetted part
    Or
  - No disconnection …. Use HART Communicator

What about the Note:

14. SETTINGS TO BE CONFIRMED BASED ON BURNER TEST.

2. III. Proof Test: Execution at Site

What proof test scope is possible?



Proof testing of PT-979A/B/C

How?

- Manifold Block / Bleed valve

Proof test options:

- Calibrated Pressure source
  Or
- No pressure source available - HART Communicator

What about Proof Test possibilities for

- **in-line Flow transmitters,**
- **Level Switches/transmitters,**
- **Temperature transmitters**

2. III. Proof Test: Execution at Site; Proof Test limitations

Testing the sensors and final elements was done in different ways:

- Via simulation (HART) the Sensor output side (only HART PTC can be claimed)
- Via simulation on the sensor input side (maximum PTC can be claimed)
- Via Jumpers on the sensor output (at device terminals) side (PTC claim??)
- Via Calibration field equipment (e.g. for TT) and the HART simulation in the field (maximum PTC can be claimed)

- The simulations on the sensor input side are mainly done by using HART, instead of actual field simulation, as requested by client.
- Final elements partly included due to the parallel valve overhaul activities/Time constrain.

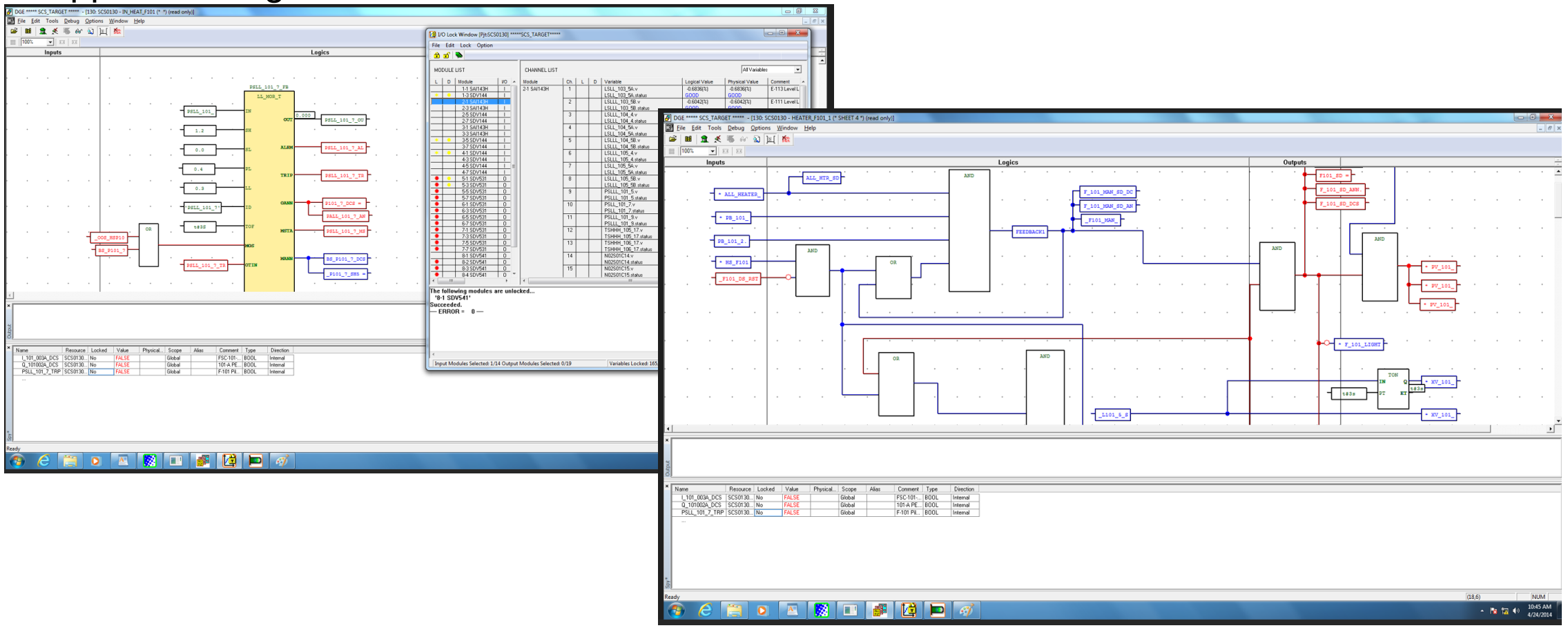
  Resulted in limited valve testing (PTC claim??)

- Proof Test Scope to be recorded as part of the auditable trail: Against what design basis the SIF was tested (e,g. filled in procedures, revision, and completeness) is recorded, incl. limitations

2. III. Proof Test: Execution at Site

Recording of the results

- Application logic Printscreen.



2. III. Proof Test: Execution at Site

Recording of the results

- Application Logic Print screen.
- BPCS HMI Graphics / Face Plates.
- Complete check sheet records with field equipment data.

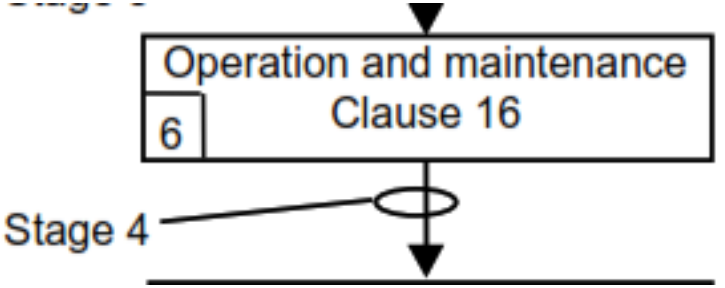
In addition, other records collected (when available)

- Sequence of Even Recorder @ SIS and / or BPCS
- Alarm Management system (Hardwired based / Software based)
- Other systems (e.g. PI-server)

  and

- Maybe pictures (Dated): Visual inspection
  Proof of activation.

2. IV. Proof Test results: Independent Stgae 4 FS Assessment

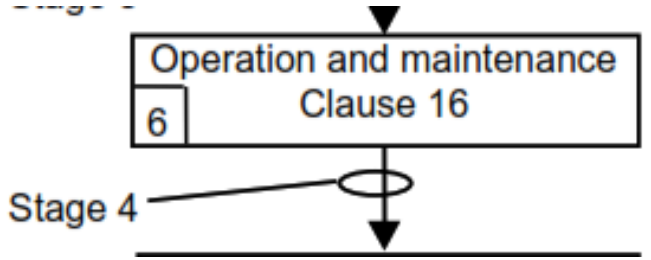


What is done:

- Verify all SIF's which are proof tested.
- Any assessment limitations and the safety impact analysed.
- Verify Proof test coverage – affects PFDavg calculation and next proof test interval

- Verify Document basis for Proof test
- Proof Test Engineering process with the Verification/Validation checks
- Actual equipment installed and failure data used.
  - Sensors, 3rd party interfaces, Logic Solver Final element Configuration.

2. IV. Proof Test results: Independent Stage 4 FS Assessment



What is done:

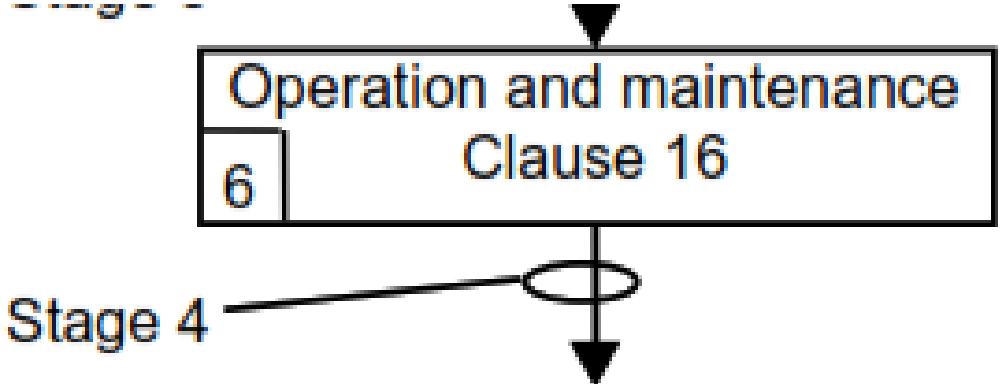
- Actual proof test records verification
  - General assessment and assessment by area
  - Proof test results
- Completed the FSM for Operation and Maintenance Phase checklist; How good/bad is client FSM

- Final Assessment of this proof test project –

199 open items for the SIF's - mainly Systematic issues and many SIF's did not meet SIL 3 (Mostly Financial SIL)

- SIF Re- Calculation based on actual PTC;
  Still meets SIL or Recommend new proof test period to meet SIL.

3. Results of recent Proof Test Execution
-
Independent Stage 4 FS Assessment



Project 2: Proof Test deficiencies for improvement

1. Provide Safety Requirement Specification based on a Hazard and Risk Analysis. See IEC61511 Ed 2, Part 1 chapter 10.3 for SRS requirements.

2. Include basis of design and other operational documents as part of the Proof Test results to verify if the assumptions done with respect to expected demand/Failure rate of the system and documentation are still matching. E.g. (false) trip evidence over the past period.

3. Specify and Inspect the installed hardware components against the components of the original specification.

4. Specify the proof test intervals and process safety times on which the PFDavg calculations are based.

5. Compare the current proof test results with the latest proof test results to detect behavioral changes and/or trends.

Project 2: Proof Test deficiencies for improvement

6.Consider process trips as proof tests and document them accordingly. These to be noted with the proof test results for comparison purposes.

7. Overall Loop response time of 2.7 and 2 seconds, respectively.

Valves closing times are recorded and show closing within this response time, but the transmitter and logic solver response time has not been recorded.

As such no conclusion can be made if the overall Loop Response Time meet the Process Safety time for the 5 HIPPS system (Trains).

8. Proof test shows that the valves closed on the high trip but no conclusion can be made that all undetected faults that prevent the HIPPS from operating in accordance with the SRS are fulfilled. Valve proof test requirements are not available.

Specify a detailed proof test to meet the IEC61511 Ed 2, Part 1 chapter 16.3.1 requirements

Project 3: FSM Deficiencies in Proof Test Report

Item	Issue	IEC61511 Ed. 2 Pt.1Clause
1	The document front sheet with names of author, reviewers, approvers, revision etc. is missing. There is no review, approval and control scheme applied. Table of Contents does not match the report order, format and pages.	19.2.6 / 7 / 8
2	Report indicates no information on achieving and maintaining functional safety of the SIS.	19.2.9
3	The Recommendation for improvements & observations are referred to appendices but no information is provided. Therefore, it is unclear what is the conclusion	16.3.2 / 16.3.1.3 / 16.3.1.6
4	Some “major” observations are not supported/elaborated by the report. As such there there is no design/operational basis for these observations	16.3.2 / 19.2.9
5	There is no analysis to justify the claim that the installed equipment are still within the useful lifetime.	16.3.1.6 16.3.2
6	No information provided on the SRS and Design documents.	19.2 / 16.3.1.6

Project 3: FSM Deficiencies in Proof Test Report

Item	Issue	IEC61511 Ed. 2 Pt.1 Clause
9	Prerequisite for proof test has not been defined.	16.3.1.1. / 19.2
8	The used (Calibrated) test equipment for Proof Test is not recorded.	16.2.2
9	No information on end-user responsibility for proof testing.	16.3.1.1/ 16.3.1.5
10	No schedule information on proof test.	16.3.1.3
11	Punch list form incl impact Analysis is not available.	16.3.1.4 / 16.3.1.6
12	No project information is available on the HIPPS itself.	16.3.3 / 19.2.29
13	Signature missing of the recorded and involved (customer) persons.	16.3.3
14	System drawings not available at site.	16.3.3 / 19.2.9
15	Visual inspection not based on any drawings and lacking references. Items cannot be confirmed as done. Actual measuring points are unclear and not documented. No measurements provided as proof that it is ok.	16.3.3
16	Visual inspection of field equipment is not recorded.	16.3.2

Project 3: FSM Deficiencies in Proof Test Report

Item	Issue	IEC61511 Ed. 2 Pt.1 Clause
17	Unclear how application logic is checked. Not covered in the proof test procedure.	16.3.1.1/ 16.3.3
18	Chapter name is Annual test and set on 1 year, but the project Safety Validation Plan specifies 18 months. There is no record to show that this time interval is maintained since the last record in 2018.	16.3.1.3 / 16.3.1.5
19	Proof test table: This proof test procedure is severely incomplete and lacking any test to reveal undetected faults. It is just a limited function check. A SIF 2oo3 Transmitters and 1oo2 Valves must be tested for every possible functionality and identify failures and possible common cause issues. Further the Proof Test Coverage is not defined. No Datasheet and Loop test check sheet of the installed equipment is provided.	16.3.1.1 / 16.3.3 / 19.2.9
20	No punch form with impact analysis provided. Punch items overview is incomplete and not matching the punch items recorded.	16.3.1.4 / 16.3.1.6

4. Key Take Aways

- Proof test “Buzz word” - Easier said then done.
- Proof test is to detect dangerous undetected failures in the SIF.
- Good proof testing require a detailed planning, proper documentation, manpower, time and budget.
- Proof test during TA schedule is limited due to time constrain and many parallel activities/pressure to complete on time.
- Inspection is required as part of Proof Test

4. Key Take Aways

- The Proof Test Coverage can be a serious limitation – which can result in additional Proof testing to meet the SIF SIL requirement.
- FSM in the Operational Phase is mostly not established - No Systematic Capability (SC) for the Operator of the Facility
- Analyze Proof test results – limited follow up due to budget/time/ knowledge constrain
- Most of the verification process is still a manual (Human) activity. Still Limited possibilities to improve this process with digitalization.

YOKOGAWA

Terimah Kasih (Thank you)

Co-innovating tomorrow™

Arjen.de.Koning@yokogawa.com
Safetyassessments@yokogawa.com