

# SIL bijeenkomst KiC 25 Januari 2018 Biobase

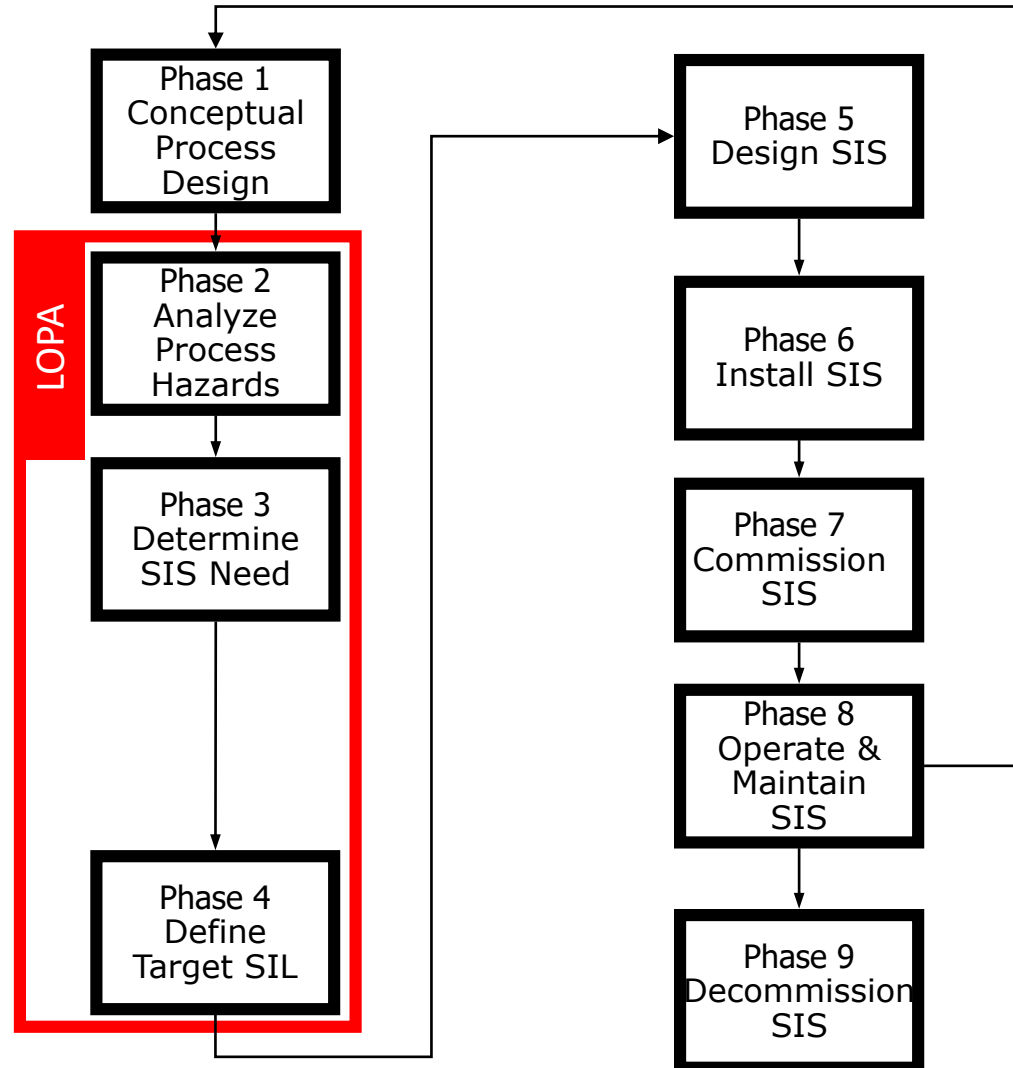
Kees Kaijser  
DOW

## IEC 61511 in Dow

- Algemeen ,
- Waarom ,
- IEC 61511 en Dow
- Wat doen we anders of verschillend of.....
- Wat maakt het moeilijk .
- Hebben we oplossingen ?

# SIS Life Cycle

SIS Life Cycle





# The Layer of Protection Analysis

DOW RESTRICTED							
Click to adjust row height			Delete Case	Add Case	Layer of Protection		
Protection		Scenario Definition					
Gap		Description of Undesired Consequence	LOPA Target Factor	Initiating Event Factor	Enabling Factor	Probability of Exposure	
Target is 0 or less	Scenario And Case Number	HELP For Consequence	HELP For TF	HELP For Initiating Event	HELP For Enabling	HELP For POE	
		Give a complete Description of the undesired consequence	List chemicals and quantity involved	Describe the initiating event	Record the Probability of Ignition or Toxic Enabling Factor.	Describe the condition of probability of exposure	
		Safety Analysis					
		Business Analysis					

Layer of Protection Analysis Worksheet								
	Independent Protection Layers							
	Ea Onafhankelijk ?Dus ook ale instrumenten etc.?					Other safety related protection systems		
Plant Integrity Design (Mechanical Integrity Issues)	BPCS Control Action	Operator responds to alarms and written procedures	SIS Function A	SIS Function B	Pressure Relief Device	SRPS 1	SRPS 2	SRPS 3

PERSONAL AND CONFIDENTIAL

January, 2018

## Beschermlagen Volledig Onafhankelijk ?

Wat als ze op 1 LS liggen?

Andere Instrumenten voor SIS ?

Richtlijnen voor control functies ( BPCS )

Fit for purpose ?

Bewezen performance ( Prior Use) ?

Testen ????



# IEC 61511 in Dow

## De start van de SIS specificatie ( SRS

Section 1		PE/Man Rep enters LOPA process information into Section 1 before leaving SIS WP Step 4.3 (GPM 12.17)	
PE/Man Rep names	<input type="text"/>		
Plant Name and Area	<input type="text"/>		
SIF Number:	<input type="text"/>	Computer Type & ID:	<input type="text"/>
		Required SIL:	<input type="text"/>
SIF Description	<input type="text"/>		
LOPA Reference	<input type="text"/>		
P&ID References	<input type="text"/>		
HIPS?	<input type="checkbox"/>	If yes, enter HIPS Tag No:	<input type="text"/>
Design Loop Response Time - dLRT (i.e. minimum MART)	<input type="text"/>	<input type="text"/>	(units)
	Assumptions & Calculations:	<input type="text"/>	
Allowable SIF Leak Rate	<input type="text"/>	(enter amount with units)	
	Assumptions & Calculations:	<input type="text"/>	
Sharing Analysis	<b>Show your work on the "Sharing Analysis" Tab</b>		
	Is there component sharing within a single Scenario?		<input type="checkbox"/>
			<input type="button" value="Go to Sharing Analysis"/>

PERSONAL AND CONFIDENTIAL



## Section 1

**PE/Man Rep** enters LOPA process information into Section 1 before leaving **SIS WP Step 4.3** (GPM 12.17)

PE/Man Rep names

Joe Manrep &amp; PE Bigwig

Plant name and area

Building 900 Chemical Process

SIF Number:

SIF-411

Computer type &amp; ID:

Mod5: A

Required SIL: SIL-2

SIF Description

The V-400 hot Dowtherm J supply block valves A:DO(045) and B:DO(042) are closed when the contents temperature of V-215 is greater than 100 deg C to prevent a vapor vent relief or equipment rupture caused by a loss of temperature control. The closing of the valves is announced by A:DC(983) of A:ALM(394) SIF loop tripped.

LOPA Reference

Chemical Process Master LOPA Scenarios 1000.01, 1001.01, 1002.01

P&amp;ID References

B-411-00900

HIPS?

☒ Yes

If yes, enter HIPS Tag No:

HIPS-411

Design Loop Response Time -  
dLRT (i.e. minimum MART)

394.0

Seconds

(units)

Assumptions &  
Calculations:

Using the MART MALR tab of the RAST tool when the V-215-DCEP\_Decom equipment is loaded, using DOWTHERM J as heating fluid, with a high temperature set point of 100 deg C. (see MART\_MALR tab of this form)

Allowable SIF Leak Rate

0.75 lb/min

(enter amount with units)

Assumptions &  
Calculations:

Using the MART MALR tab of the RAST tool when the V-215-DCEP\_Decom equipment is loaded, using DOWTHERM J as heating fluid, with a high temperature set point of 100 deg C. (see MART\_MALR tab of this form)

Sharing Analysis

**Show your work on the "Sharing Analysis" Tab**

Is there component sharing within a single Scenario?

☒ Yes[Go to Sharing Analysis](#)

PERSONAL AND CONFIDENTIAL



# IEC 61511 in Dow

Analyse of we componenten sharen ?

Back to SRS Life Cycle

**Sharing Analysis:**  
Copy LOPA scenario information into table below (modify table as needed) OR Copy scenario information and paste directly from LOPA

Note the functions which have been identified as protection layers in LOPA in the table below.

LOPA credit	Sensors	Final Elements	Logic Solvers	Brief Functional Description
Initiating Event				
BPCS/Alarm #1 Protection				
BPCS/Alarm #2 Protection				
SIF Function A				
SIF Function B				
Pressure Relief				
Safety Related Protection Systems				





# IEC 61511 in Dow

Sharing Analysis																	
Show your work on the "Sharing Analysis" Tab																	
Is there component sharing within a single Scenario?																	
<input type="button" value="Go to Sharing Analysis"/>																	
Describe any <b>Sensor</b> SHARING between BPCS-IE-Alarm-and/or-SIF, including any enable/disable/compensation instruments:																	
Describe any <b>Logic Solver</b> SHARING between BPCS-IE-Alarm-and/or-SIF:																	
Describe any <b>Final Element</b> SHARING between BPCS-IE-Alarm-and/or-SIF:																	
SIF Design Requirements	<table><tr><td>Sensor Required Accuracy for SIF:</td><td></td></tr><tr><td>Business Reliability Requirement (False Trips per 100 years)</td><td></td></tr></table>	Sensor Required Accuracy for SIF:		Business Reliability Requirement (False Trips per 100 years)													
Sensor Required Accuracy for SIF:																	
Business Reliability Requirement (False Trips per 100 years)																	
Logic Solver Details	<table><tr><td>Trip Setpoint</td><td></td></tr></table>	Trip Setpoint															
Trip Setpoint																	
Final Element Details	<table><tr><td>Final Element Fail State</td><td></td></tr></table>	Final Element Fail State															
Final Element Fail State																	
Additional information	<table><tr><td>Is manual shutdown capability for the SIF loop needed?</td><td>Yes or No</td></tr><tr><td>Does SIS need to be manually reset after trip (latched trip)?</td><td></td></tr><tr><td>Will a Technology SME be involved to approve Final Design of the SIF Loop?</td><td></td></tr><tr><td>Are there any special requirements for SIF installation surviving a major accident (eg fire)?</td><td></td></tr><tr><td>Are there any enable/disable/compensation instruments needed for this SIS?</td><td></td></tr><tr><td>Is this SIF expected to perform in "Low Demand" mode (see comment)?</td><td></td></tr><tr><td>What is an acceptable outage interval for testing sensors?</td><td>Months</td></tr><tr><td>What is an acceptable outage interval for testing final elements?</td><td>Months</td></tr></table>	Is manual shutdown capability for the SIF loop needed?	Yes or No	Does SIS need to be manually reset after trip (latched trip)?		Will a Technology SME be involved to approve Final Design of the SIF Loop?		Are there any special requirements for SIF installation surviving a major accident (eg fire)?		Are there any enable/disable/compensation instruments needed for this SIS?		Is this SIF expected to perform in "Low Demand" mode (see comment)?		What is an acceptable outage interval for testing sensors?	Months	What is an acceptable outage interval for testing final elements?	Months
Is manual shutdown capability for the SIF loop needed?	Yes or No																
Does SIS need to be manually reset after trip (latched trip)?																	
Will a Technology SME be involved to approve Final Design of the SIF Loop?																	
Are there any special requirements for SIF installation surviving a major accident (eg fire)?																	
Are there any enable/disable/compensation instruments needed for this SIS?																	
Is this SIF expected to perform in "Low Demand" mode (see comment)?																	
What is an acceptable outage interval for testing sensors?	Months																
What is an acceptable outage interval for testing final elements?	Months																

PERSONAL AND CONFIDENTIAL



## Sharing Analysis

### Show your work on the "Sharing Analysis" Tab

Is there component sharing within a single Scenario?

Yes

Go to Sharing Analysis

Describe any **Sensor** SHARING between BPCS-IE-Alarm-and/or-SIF, including any enable/disable/compensation instruments:

Temperature Transmitters are shared between the BPCS IE and the SIL2 SIF loop

Describe any **Logic Solver** SHARING between BPCS-IE-Alarm-and/or-SIF:

MODV A is shared between the BPCS IE, the BPCS PF, and the SIL2 SIF loop

Describe any **Final Element** SHARING between BPCS-IE-Alarm-and/or-SIF:

None

## SIF Design Requirements

Sensor Required Accuracy for SIF: 1.00%

Business Reliability Requirement (False Trips per 100 years) Standard 97%

## Logic Solver Details

Trip Setpoint 100 Deg C

## Final Element Details

Final Element Fail State Fail Closed

## Additional information

Is manual shutdown capability for the SIF loop needed?

Yes or No

No

Does SIS need to be manually reset after trip (latched trip)?

Yes-for Safety

Will a Technology SME be involved to approve Final Design of the SIF Loop?

Yes

Are there any special requirements for SIF installation surviving a major accident (eg fire)?

No

Are there any enable/disable/compensation instruments needed for this SIS?

No

Is this SIF expected to perform in "Low Demand" mode (see comment)?

Low Demand

What is an acceptable outage interval for testing sensors?

12

Months

What is an acceptable outage interval for testing final elements?

12

Months

PERSONAL AND CONFIDENTIAL

# IEC 61511 in Dow

Overview SIS A Warnings & Remarks Calculation Schema MTTF Overview

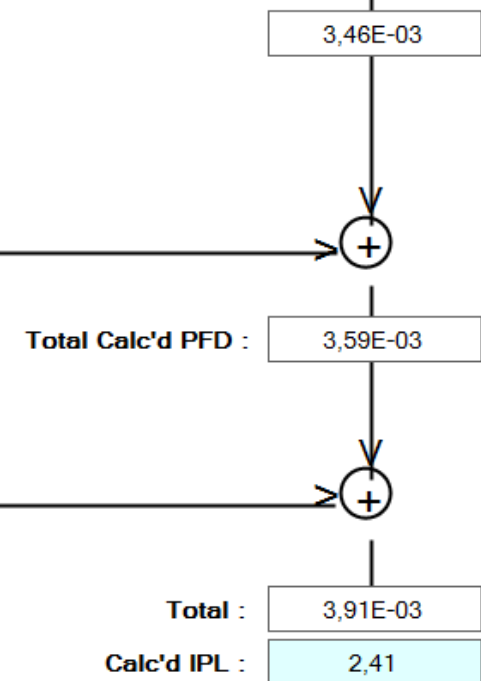
SIS A w/ BPCS Ctrl I.E.

SIS A		
SE	LS	FE
5,55E-04	2,66E-04	2,64E-03
3,46E-03		

Sharing and/or Common Cause		
SE	LS	FE
1,30E-05	N/A	1,11E-04
1,24E-04		

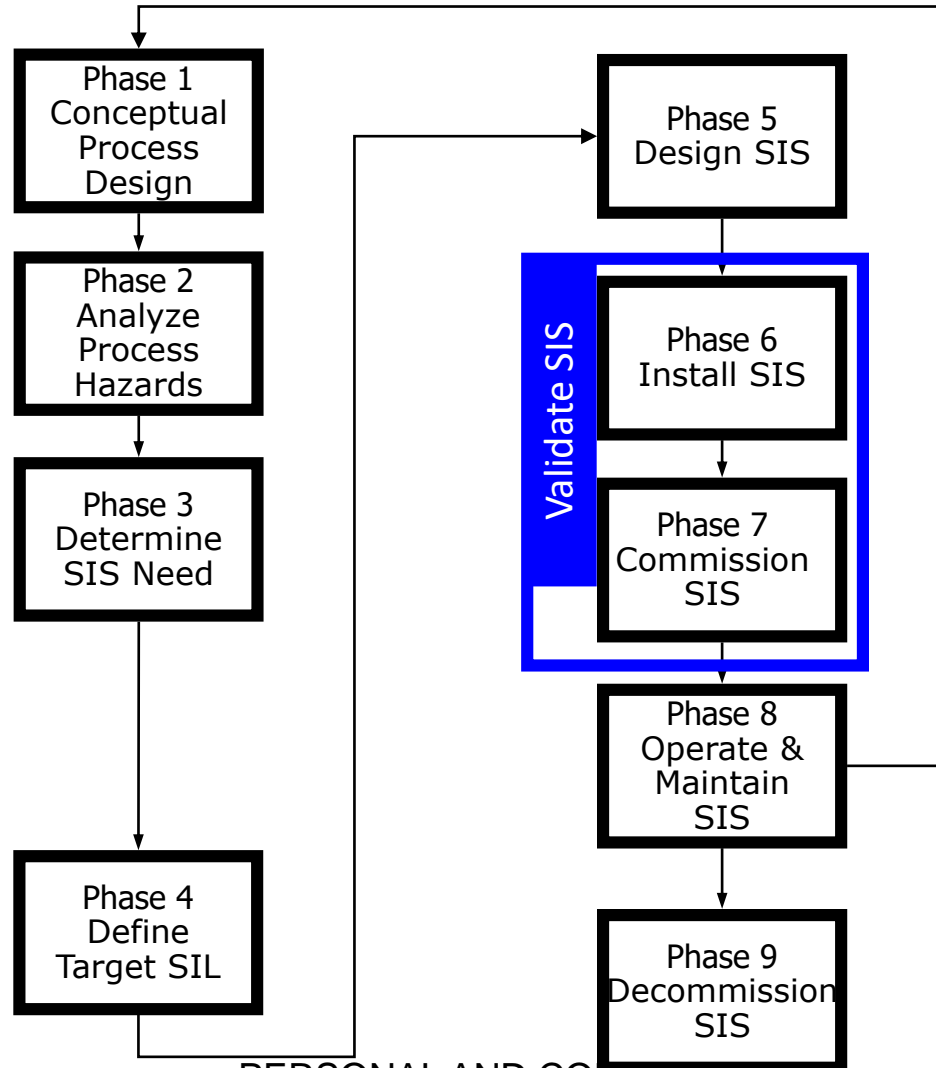
System Failure		
SE	LS	FE
1,81E-04	1,40E-04	N/A
3,21E-04		

De berekening om de invloed van de Sharing te bepalen op de totale Risico reductie



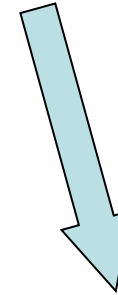
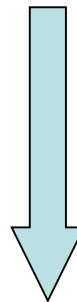
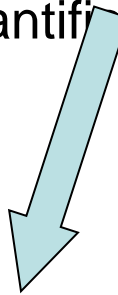
# SIS Life Cycle

SIS Life Cycle



# Loss Prevention Principles relationships

**LPP 1.8** (Hazard identification & quantification)



**LPP 15.1**

(Instrument  
Installation)

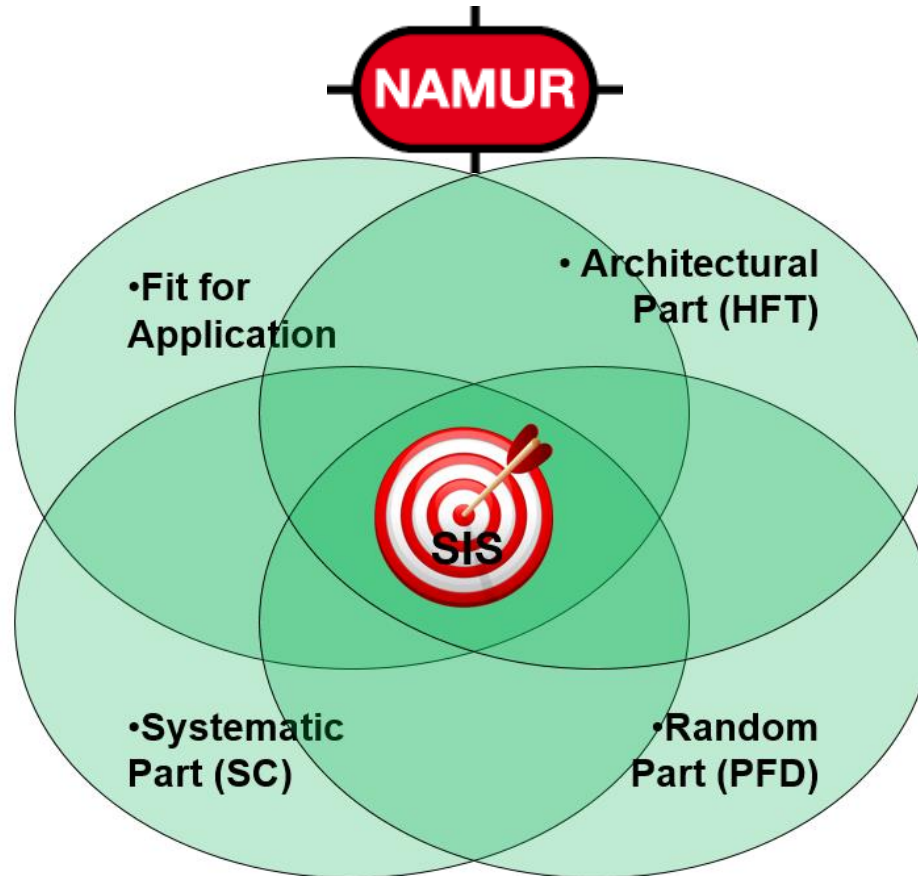
**LPP 15.2**

(BPCS & ALARM  
protection layers)

**LPP 15.4**

(SIS protection  
layers)

# IEC 61511 in Dow



# Prior-use Instruments

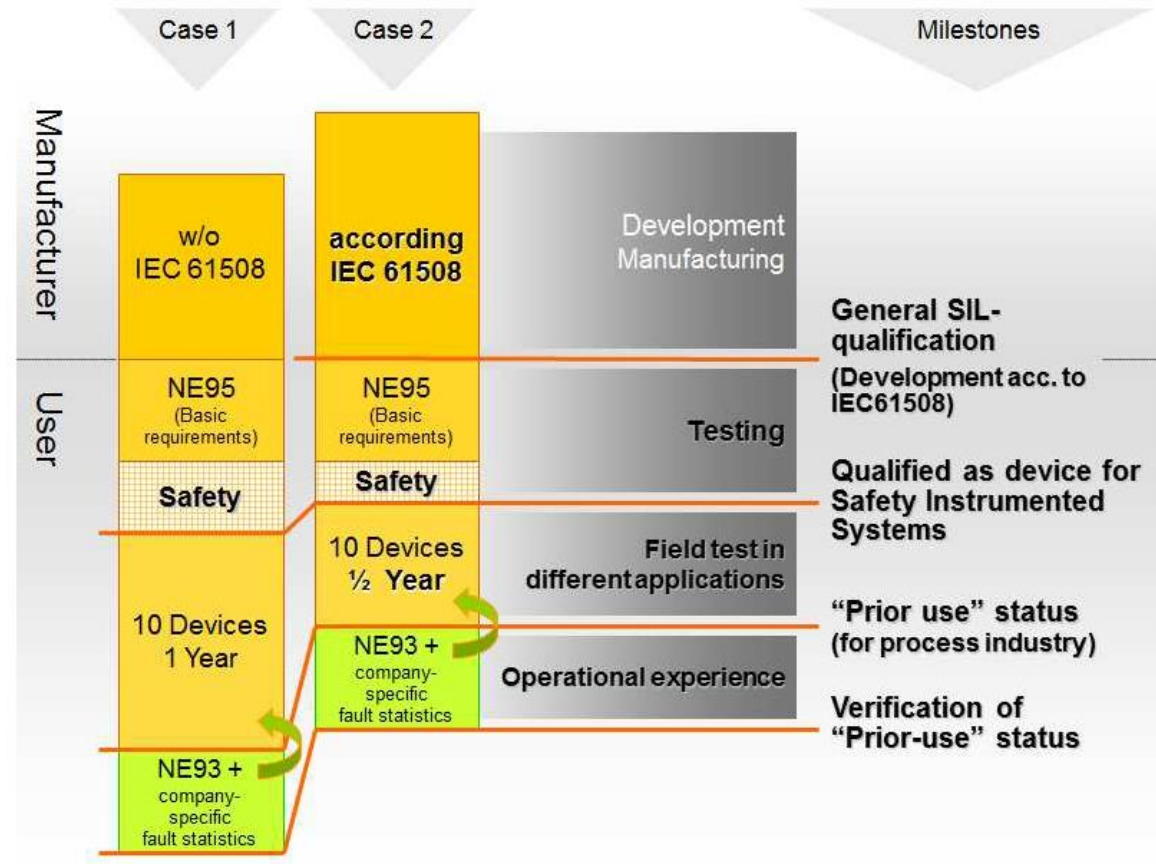
EMETL G6A-1020-00

- Objective: Establish a positive identification of instruments used in SIS.
- Ensures that the devices selected are designed, manufactured, and managed for safety applications and operate successfully in the intended application (e.g., application induced failures are accounted for). Documentation of compliance with IEC 61508 is normally provided by the instrument vendor in the form of a “SIL certificate” and may also include a Failure Modes and Effects Analysis (FMEA) report done by an external agency such as Exida or TÜV.
- Similar ways are described in ISA TR84.00.04 Part 1, Annex L or NAMUR recommendation NE130 (“Prior-use”-devices for Safety Instrumented Systems”).



## IEC 61511 in Dow

# Prior-use Instruments



PERSONAL AND CONFIDENTIAL





# IEC 61511 in Dow

Prior Use Evidence Nr.	responsible TRN	Devicetyp	Manufacturer	Modell Nr.	AMSL STATUS	AMSL Database Name	AMSL Description
EMETL_xxxx	PLT	Vibrating switch	Endress+Hauser	Soliphant II FTM 50, 51 or 52 FTL 50 & 70 Series with FEL 57 & FTL 325P or	Acceptable	ENDRESS+HAUSER (INSTRUME	SOLIDS (SILO / HOPPERS) - VIBRATING SWITCH - LEVEL MEASUREM
EMETL_xxxx	PLT	Vibrating switch	Endress+Hauser	FDL 60 Series w/FTL 670	Acceptable	ENDRESS+HAUSER (INSTRUME	SWITCHES - VIBRATING - LIQUID (SIS APPLICATIONS) - LEVEL MEAS
EMETL_xxxx	PLT	Nuclear	Endress+Hauser	Gammapiot M FMG60	Acceptable	ENDRESS+HAUSER (INSTRUME	TRANSMITTER - NUCLEAR - LEVEL MEASUREMENT
EMETL_xxxx	PLT	Nuclear	Vega	PROTRAC series 30	Acceptable	VEGA	TRANSMITTER - NUCLEAR - LEVEL MEASUREMENT
EMETL_xxxx	PLT	Free space radar	Endress+Hauser	FMR 50, FMR 51, FMR 52, FMR 57	Acceptable	ENDRESS+HAUSER (INSTRUME	TRANSMITTER - FREE SPACE RADAR (PROCESS CONTROL) - LEVEL
EMETL_xxxx	PLT	Free space radar	Vega	Vegapuls 60 Series	Acceptable	VEGA	TRANSMITTER - FREE SPACE RADAR (PROCESS CONTROL) - LEVEL
EMETL_xxxx	PLT	Free space radar	Endress+Hauser	Micropilot FMR56, 57	Acceptable	ENDRESS+HAUSER (INSTRUME	TRANSMITTER - FREE SPACE RADAR - SOLIDS LEVEL MEASUREME
EMETL_xxxx	PLT	Free space radar	Vega	Vegapuls 68	Acceptable	VEGA	TRANSMITTER - FREE SPACE RADAR - SOLIDS LEVEL MEASUREME
EMETL_xxxx	PLT	Ultrasonic	Vega	Vegason 51-56 (60?) Series	Acceptable	VEGA	TRANSMITTER - ULTRASONIC - LEVEL MEASUREMENT
EMETL_xxxx	PLT	Pressure	Emerson	3051 series	Acceptable	EMERSON (ROSEMOUNT PRES	TRANSMITTERS - STANDARD P & D/P CELL - LEVEL MEASUREMENT
EMETL_xxxx	PLT	Pressure	Yokogawa	EJA series	Acceptable	YOKOGAWA ELECTRIC CORPO	TRANSMITTERS - STANDARD P & D/P CELL - LEVEL MEASUREMENT
EMETL_xxxx	PLT	Pressure	Emerson	3051 series	Acceptable	EMERSON (ROSEMOUNT PRES	TRANSMITTERS - REMOTE OR DIRECT MOUNT SEAL SYSTEM - LEVE
EMETL_xxxx	PLT	Pressure	Yokogawa	EJA series	Acceptable	YOKOGAWA ELECTRIC CORPO	TRANSMITTERS - REMOTE OR DIRECT MOUNT SEAL SYSTEM - LEVE
EMETL_xxxx	PLT	Guided wave rada	Vega	Vegaflex 80 Series	Acceptable	VEGA	TRANSMITTER - GUIDED WAVE RADAR (PROCESS CONTROL) - LEVE
EMETL_xxxx	PLT	Guided wave rada	Endress+Hauser	Levelflex FMP5x series	Acceptable	ENDRESS+HAUSER (INSTRUME	TRANSMITTER - GUIDED WAVE RADAR (PROCESS CONTROL) - LEVE

PERSONAL AND CONFIDENTIAL

# Prior Use Instruments Spreadsheet



- <https://workspace.bsnconnect.com/sites/Instrument/GSISTRN/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2FInstrument%2FGSISTRN%2FShared%20Documents%2FPrior%20Use%20Documents&View=%7B343CBCD8%2D147C%2D46FA%2D8D63%2D9DDFFEA46F75%7D>

## B1 Checklist Example – Level Rosemount ERS

- <https://workspace.bsnconnect.com/sites/Instrument/GSISTRN/Shared Documents/Prior Use Documents/Level/Rosemount ERS>
- Checklists and following documentation (manuals, certificates, quality studies) on Sharepoint.
- Spreadsheet to be located perhaps as a link at the AMSL or SIS website



# IEC 61511 in Dow

Automated Valve TRN    Flow TRN    Instrument Maintenance TRN    Press/Lvl/Temp T

## vel ▸ Rosemount\_ERS ⓘ

⌵w document or drag files here











Documents

Explorer View



Find a file



 Name	Modified	Modified By
 01_Datasheet	... July 26	<input type="checkbox"/> Santos, Michele (MJ)
 02_User_Manual	... July 26	<input type="checkbox"/> Santos, Michele (MJ)
 03_Safety_Manual	... July 26	<input type="checkbox"/> Santos, Michele (MJ)
 04_SIL_Certificate	... July 26	<input type="checkbox"/> Santos, Michele (MJ)
 05_Quality_Test_Reports	... July 26	<input type="checkbox"/> Santos, Michele (MJ)
 3051_S_ERS	... August 10	<input type="checkbox"/> Santos, Michele (MJ)
 00809-0100-4804	... July 26	<input type="checkbox"/> Santos, Michele (MJ)
 fmeda_3051s_ers	... July 26	<input type="checkbox"/> Santos, Michele (MJ)
 Prior use 3051S ERS System Rosemount	... October 18	<input type="checkbox"/> Santos, Michele (MJ)

PERSONAL AND CONFIDENTIAL



# IEC 61511 in Dow

THE DOW CHEMICAL COMPANY	CHECKLIST/PERMIT/FORM
INSTRUMENTATION	G6A-1020-01
GLOBAL	11-APR-2011
Page 1 of 3	

## Form B1

Safety Datasheet / Evidence Nr.:

PLT\_TRN\_xxxx

1 MANUFACTURER			
#1.1	Manufacturer	Rosemount	
#1.2	Address	Emerson, Chanhassan, MN, USA	Address to contact for safety related questions
#1.3	AM/SL Identification	Suitable for SIS	
#1.4	X	Manufacturer's quality management system (ISO 900x) has been evaluated as part of the AM/SL approval process.	
2. GENERAL INFORMATION (1/2)			
#2.1	Device designation and permissible types	3051S Electronic Remote Sensors (ERS) System	
#2.2	Specification	According to Emetl documents ( numbers )	
#2.3	Manufacturers Safety Manual	00809-0100-4804 Rev AB	
#2.4	Safety related output signal	Analog output's can be used for safety function	

PERSONAL AND CONFIDENTIAL



# IEC 61511 in Dow

#2.4	Safety related output signal	Analog output's can be used for safety function	
#2.5	Fault current	mA values , ( acc NE 43)	
#2.6	Process variable/function	Level.	
#2.7	Safety function	High , low level,	
#2.8	Device type acc. to IEC 61508-2	<input type="checkbox"/> Type A	X Type B
#2.9	Operating mode	<input checked="" type="checkbox"/> Low demand	<input type="checkbox"/> High demand or continuous
#2.10	Systematic Capability (SC) of the device	SIL 2 for random integrity @ HFT = 0 SIL 3 for random integrity @ HFT = 1 SIL 3 for systematic integrity	
#2.11	Valid hardware version	3051SAM, 3051SAL_P, or 3051SAL_S	
#2.12	Valid software version	Software revision should be 57 or higher	

Page 2 of 3

2. GENERAL INFORMATION (2/2)		
#2.12	Application Restrictions	Use Emet1(guidance , installation) and selection tools .
#2.13	Application specific industrial standards	
#2.14	Type of evaluation (check only one box)	<input checked="" type="checkbox"/> Complete HW/SW evaluation parallel to development incl. FMEDA and change request acc. to IEC 61508-2, -3 <input type="checkbox"/> Evaluation of "Proven-in-use" performance for HW/SW incl. FMEDA and change request acc. to IEC 61508-2, -3 <input type="checkbox"/> Evaluation of HW/SW field data to verify "prior-use" acc. to IEC 61511 for most of our instruments the prior use criteria applies <input type="checkbox"/> Evaluation by FMEDA acc. to IEC 61508-2 for devices w/o software
#2.15	Evaluation through Report No.	Exida report number Nr./No.: ROS 10/04-83 R001
#2.16	Test documents	Int Users Ass WIS , XXXX

PERSONAL AND CONFIDENTIAL



THE DOW CHEMICAL COMPANY	CHECKLIST/PERMIT/FORM
INSTRUMENTATION	G6A-1020-01
GLOBAL	11-APR-2011
	Page 3 of 3

### 3. FMEDA DATA

Device	$\lambda_{SD}$	$\lambda_{SU}$	$\lambda_{DD}$	$\lambda_{DU}$	SFF
3051 ERS System, Primary Sensor with Coplanar Sensor+Secondary Sensor with Coplanar Sensor	--	319 FIT	897 FIT	131 FIT	90%
3051 ERS System, Primary Sensor + Secondary Sensor with In-line Sensor or Model	--	237 FIT	996 FIT	114 FIT	92%
3051S ERS System, Primary Sensor with In- Line Sensor + Secondary Sensor with Coplanar Sensor	--	156 FIT	1095 FIT	97 FIT	93%
3051 ERS System, Primary Sensor with In- line Sensor + Secondary Sensor with In-Line Sensor	--	156 FIT	1095 FIT	97 FIT	93%

\*1) Failure rate in FIT (failures in time = number of failures in 1E09 hours)

\*2) Proof Test Coverage (Diagnostic coverage for manual proof tests)

\*3) Safe Failure Fraction

PERSONAL AND CONFIDENTIAL



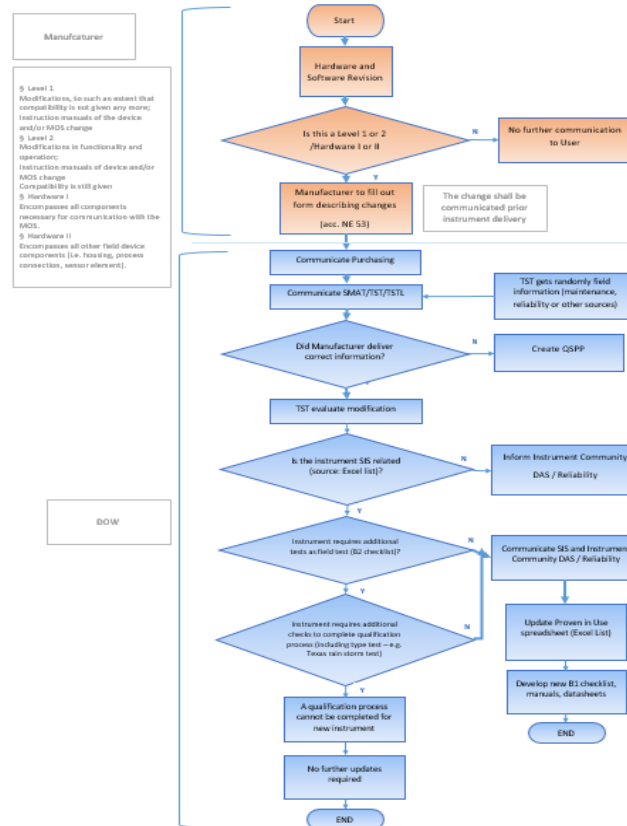
IEC 61511 in Dow

# Prior use

What when type , model ,  
software changes

PERSONAL AND CONFIDENTIAL

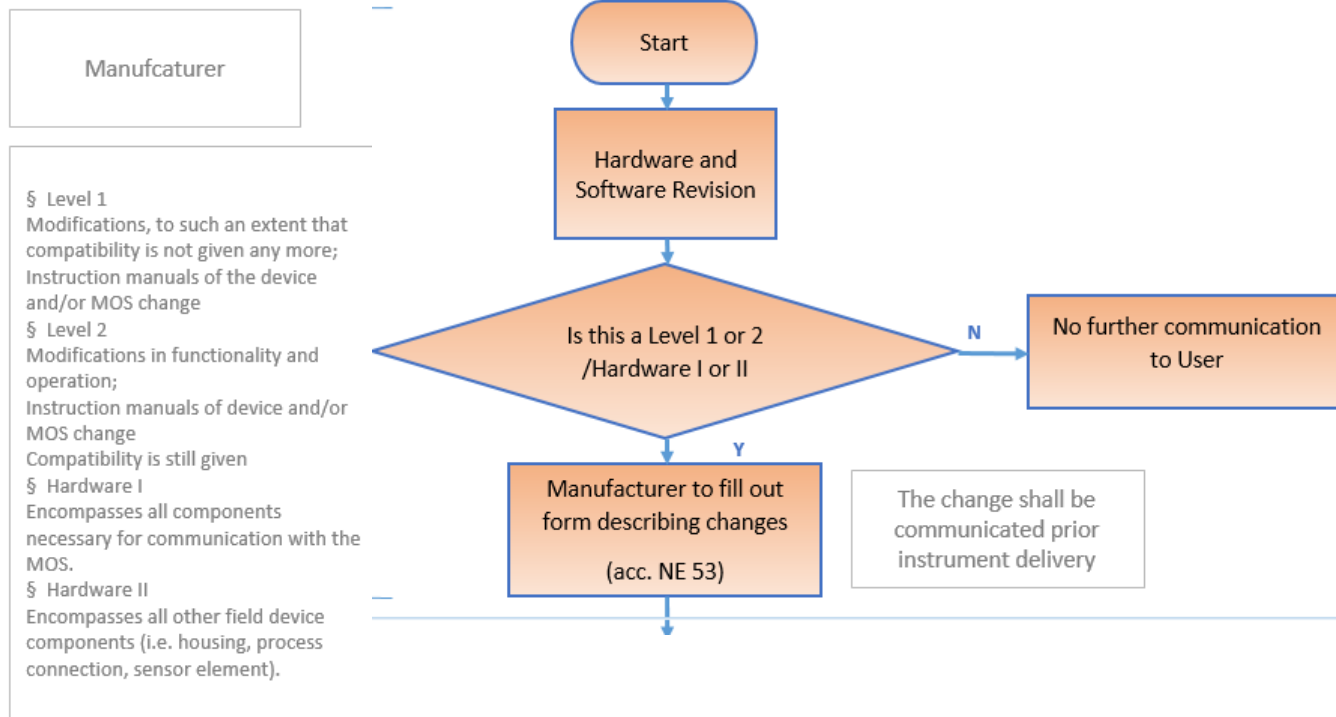
# Prior use



2018 , KK

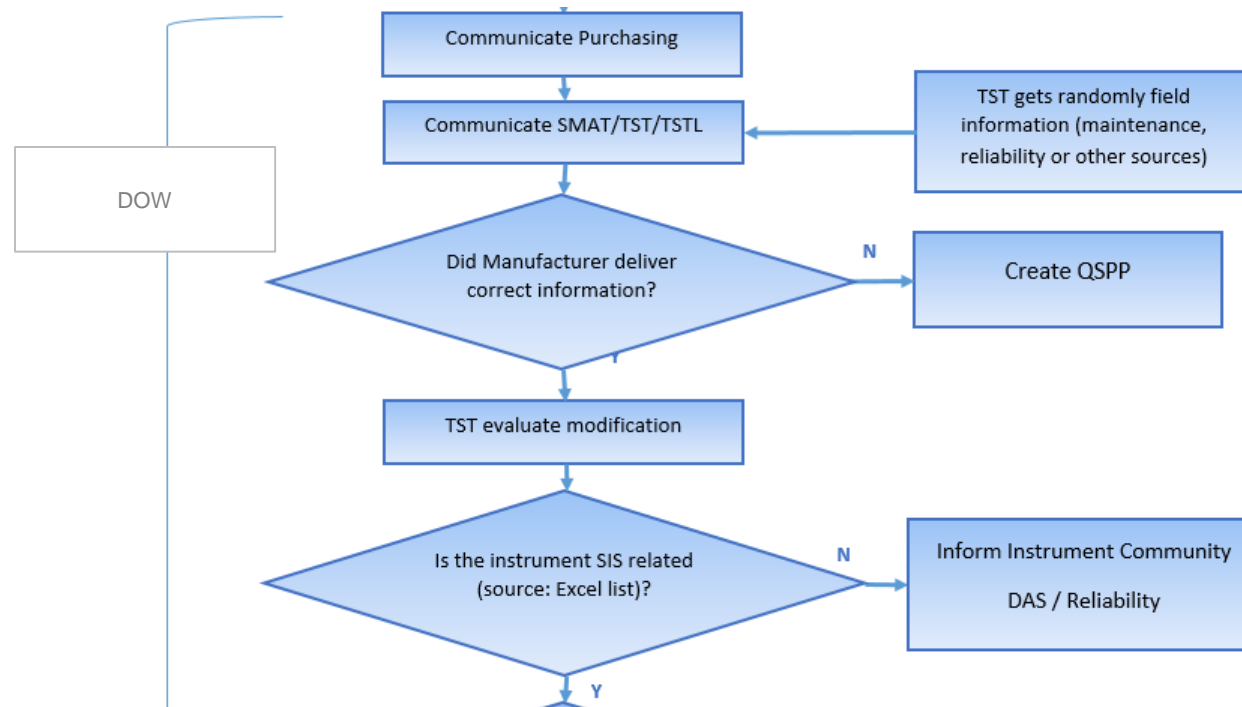


# Prior use



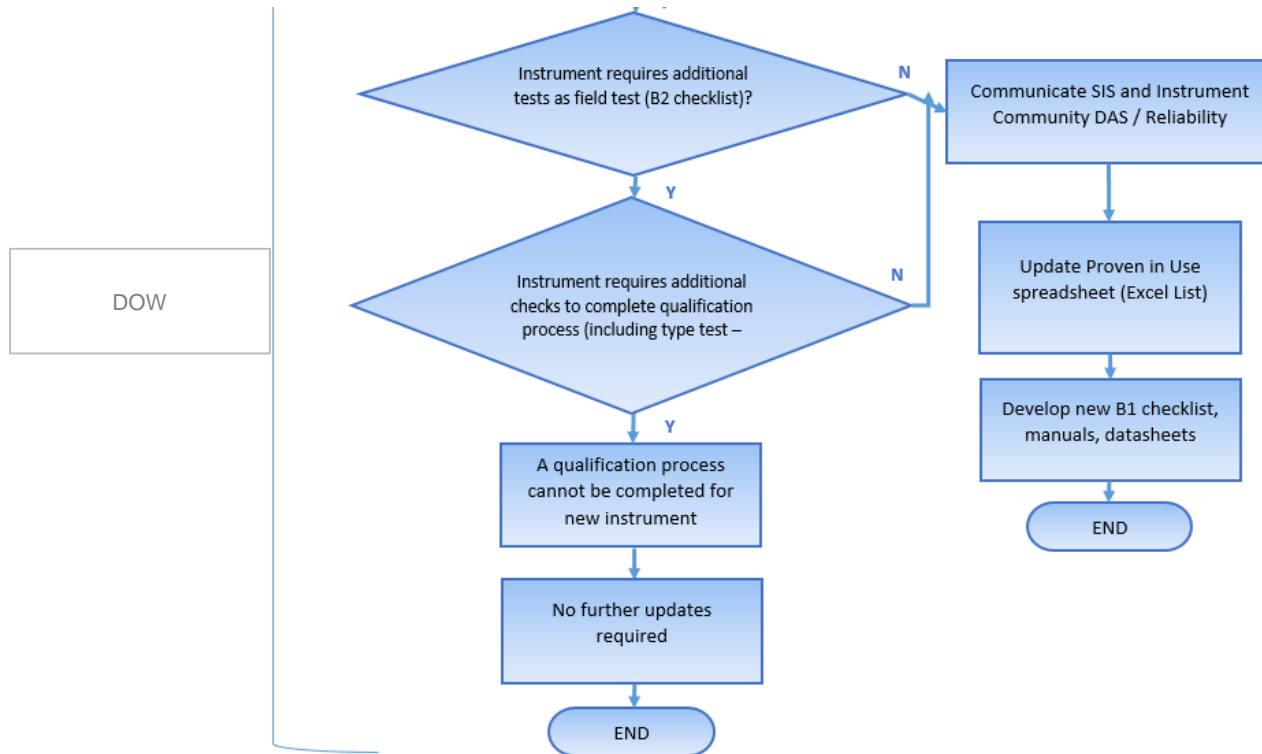
2018, KK

# Prior use



2018, KK

# Prior use



2018 , KK

TESTEN ???????????

# Testing of in line flow devices

Proof test of Rosemount Micro Motion 1700/2700 series coriolis flow meters

**Partial proof test every 12 month , full calibration/inspection every 6 years**

**Single meter in a SIL 2**



# Testing of in line flow devices

When we have a **single** coriolis meter in a **SIL2** application . Performing a proof test with a coverage of 99 % , this gives a proof test frequency of 24 month. For a plant which has a turn around frequency of 6 to 8 years , this may give problems.

The safety manual from the supplier gives an option to do a proof test with a coverage of **56%** ( see Exida rapport attached). For this test there is no need to remove the meter from service. When we do this proof test every **12 month**, the calculation shows that we can set the mission time at **6 years** . the mission time is the time that a component ( the coriolis meter) is removed from service and full calibration is done ( assuming 100% coverage)



# Testing of in line flow devices

## Propix input /output

Overview SE\_01

Instr. Type: Flow, coriolis Test Interval [months]: 12 User Defined MTTF: ☐

P&ID Tag Copy From

SE Data Proof Test Coverage & Mission Time

Proof Test Coverage [%]: 56.0

Mission Time (Overhaul Interval) [y]: 6

SIF Output: Warnings & Remarks MTTF Overview

PFD Overall :

	PFD Budget	PFD Calc'd	PFD budget used [%]	FTF [/100Y]	Hardware Config.	Beta [%]	MTTR (Hr.)	SFF subsys	HFT Avail	HFT Req'd
Sensor Elements :	3.50E-03	3.503E-03	35.0	0.17	1001	-	N/A	0.84	0	0
Logic Solver :	1.50E-03	N/A	N/A	N/A	N/A	-	-			
Final Elements :	5.00E-03	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
----- PFD Total :	N/A	N/A	N/A	N/A						

Sensor Elements :

	Test interv.	MTTF	MTTF	SFF	SFF	DC	Lambda	Lambda	Lambda	Lambda	User def.	PFD
Sensor Type	[month]	Base	Calc'd	Base	Calc'd	Calc'd	DU	DD	SU	SD	MTTF	Calc'd
SE_01 : Flow, coriolis	12	76.0	75.5	0.35	0.84	0.75	2.45E-07	7.38E-07	1.32E-07	3.97E-07	No	3.50E-03



# Proof test from the manual



## Appendix B: Proof tests to reveal dangerous undetected faults

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

### B.1 Proof test 1

Proof test 1 consists of a simple HART driven min to max output test, as described in Table 12. This test will detect approximately 56% of possible DU failures in the transmitter.

Table 12 Steps for Proof Test 1

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value <sup>8</sup> .
3	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value <sup>9</sup> .
4	Use the HART communicator to view detailed device status to ensure no alarms or warnings are present in the transmitter
5	Verify all safety critical configuration parameters
6	Restore the loop to full operation
7	Remove the bypass from the safety PLC or otherwise restore normal operation

### B.2 Proof test 2

An alternative proof test 2 consisting of proof test 1 with meter verification, verification of the flowtube temperature measurement and a restart of the sensor (to detect soft errors in RAM) will detect approximately 91% of possible DU failures in the flowmeter resulting in a Proof Test Coverage of 91% for the flowmeter.





## Proof test of Rosemount 8800 series vortex flow meters

When we have a **single** vortex meter in a **SIL2** application . Performing a proof test with a coverage of 99 % , this gives a proof test frequency **of 24** month. For a plant which has a turn around frequency of 6 to 8 years , this may give problems.



The safety manual from the supplier gives an option to do a proof test with a coverage of **82%** ( see Exida rapport attached). For this test there is no need to remove the meter from service. When we do this **prooftest every 12 month**, the calculation shows that we can set the mission time **at 8 years** . The mission time is the time that a component ( the vortex meter) is removed from service and full calibration is done ( assuming 100% coverage)





## Appendix B Proof test to reveal dangerous undetected faults

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

### B.1 Suggested proof test

A suggested proof test is described in Table 10. This test will detect approximately 82% of possible DU failures in the 8800D.

Table 10 Steps for Proof Test

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Connect a HART communicator to the flowmeter. Connect a current measuring device into the loop. (The safety PLC can be used for this purpose if it can display the current while bypassing the 8800D in the logic solver.)
3.	Use the HART communicator to force the output current to 22.6mA and ensure this is measured at the output.
4.	Use the HART communicator to force the output current to 12mA and ensure this is measured at the output.
5.	Use the HART communicator to force the output current to 3.6mA and ensure this is measured at the output. Remove the output current force. Remove the HART communicator.
6.	Ensure that with no flow the output is 4mA.
7.	Provide flow through the Flowmeter; ensure that the current output corresponds to the flow. (Reasonability check)
8.	Restore the loop to full operation.
9.	Remove the bypass from the safety PLC or otherwise restore normal operation.



## Proof test of Rosemount 8800 series vortex flow meters

Propix for SIS input and output

Overview SE\_01

Instr. Type: Flow, vortex Test Interval [months]: 12 User Defined MTTF: ☐

P&ID Tag Copy From

SE Data Proof Test Coverage & Mission Time

Proof Test Coverage [%]: 82.0

Mission Time (Overhaul Interval) [y]: 8.0

Propix for SIS - [Output Calculations]

File Help

Legend: OK Acceptable Not Acceptable

Return to Input Execute Menu

SIF Output: Warnings & Remarks MTTF Overview

PFD Overall :

	PFD Budget	PFD Calc'd	PFD budget used [%]	FTF [/100Y]	Hardware Config.	Beta [%]	MTTR (Hr.)	SFF subsys	HFT Avail	HFT Req'd
Sensor Elements :	3.50E-03	3.635E-03	36.4	0.38	1001	-	N/A	0.85	0	0
Logic Solver :	1.50E-03	N/A	N/A	N/A	N/A	-	-			
Final Elements :	5.00E-03	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
----- PFD Total :	N/A	N/A	N/A	N/A						

Sensor Elements :

Sensor Type	Test interv. [month]	MTTF Base	MTTF Calc'd	SFF Base	SFF Calc'd	DC Calc'd	Lambda DU	Lambda DD	Lambda SU	Lambda SD	User def. MTTF	PFD Calc'd
SE_01 : Flow, vortex	12	50.0	49.14	0.5	0.85	0.69	3.59E-07	8.03E-07	3.59E-07	8.03E-07	No	3.64E-03



An other example

Proof test of Endress & Hauser 80/83 series coriolis  
EO/PO/BO flow meters IPG

**Partial proof test every 24 month , full  
calibration/inspection every 15 years for EO/PO/BO  
feed flow meters as a 3oo3**



An other example

When we have **2 redundant** coriolis meters in a **SIL2** application . Having 10% of the PFD budget available , because of **3 parallel feeds** to a reactor Performing a proof test with a coverage of 99 % , this gives a proof test frequency of **48 month**.



## An other example

The safety manual from the supplier gives an option to do a proof test with a coverage of 90 % ( see safety manual attached). For this test there is no need to remove the meter from service. When we do this proof test every **24 month**, the calculation shows that we can set the mission time at **15 years** . the mission time is the time that a component ( the coriolis meter) is removed from service and full calibration is done ( assuming 100% coverage)





Nu de kleppen nog



# SIS - Final elements

## The challenge of Seat Leakage Testing

Roy Lim  
Kees Meliefste  
Dow Benelux Terneuzen BV



# Content

- ✓ Introduction
  - ✓ Seat Leakage Test Criterion
- ✓ Seat Leakage Possible Test Methods
  - ✓ Conclusions

# Introduction

- ✓ Why Seat Leakage Testing:
  - ✓ Proof testing IEC 61511-1:
- ✓ Test to reveal **undetected faults** in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality.
- ✓ Proof Test Frequency determined by the PFD-calculation

# Introduction

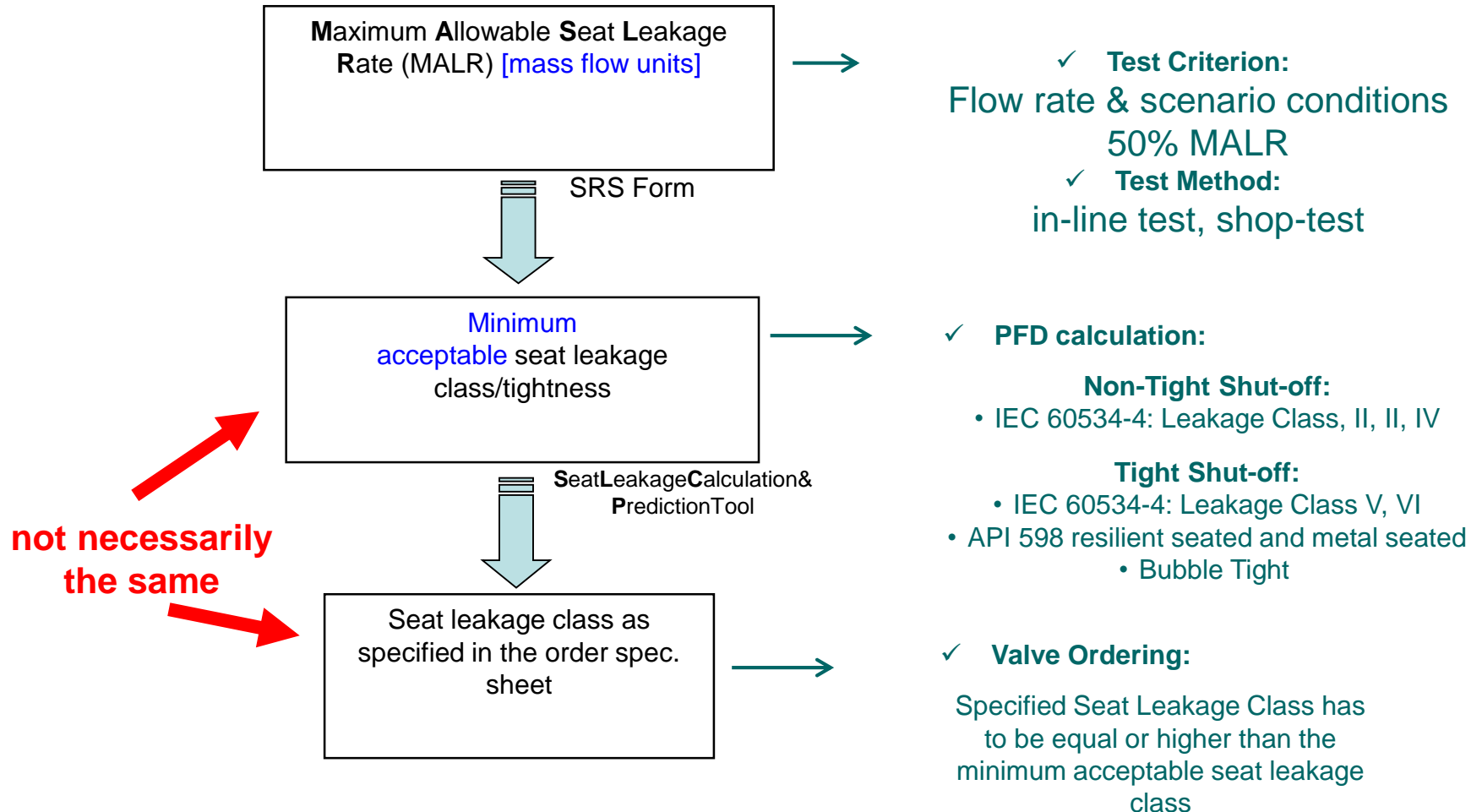
- ✓ Proof test includes:
  - ✓ Visual inspection
  - ✓ required stroke time
- ✓ required fail action (signal- and air supply)
  - ✓ required seat leakage tightness



## Challenges:

- ✓ test criterion
- ✓ test method

# Test Criterion



# Possible Test Methods

- ✓ Test Method:
  - ✓ Test criterion (MALR)
  - ✓ Available measurements
  - ✓ Piping/system configuration

# Possible Test Methods

- ✓ Test criterion (MALR):
  - ✓ 50% of MALR
- ✓ Not always possible to test at scenario conditions
- ✓ Convert MALR into MALR<sub>test</sub> with pre-defined test medium, pressures and temperature
  - MALR @ scenario conditions
    - ↳ Cv-calculation
      - ↳ MALR<sub>test</sub> @ test conditions

# Possible Test Methods

- ✓ In-Line testing ~ preferred method:
  - ✓ Testing with valve installed in-line
- ✓ Depending the MALR and the system and/or piping configuration
  - ✓ Test category F or M
  - ✓ Off-line testing:
- ✓ System and/or piping configuration is not suitable to do the in-line test
  - ✓ Tight-shutoff requirements
    - ✓ Test category S



# Possible Test Methods

## Test Categories:

### ✓ **Category F:**

- ✓ Function test & Travel test incl. visual confirmation
  - No direct seat leakage test
    - ✓ DC-proof test ~95%
  - 'Deferred' seat leakage test

E.g. once per 16 year instead of once per 8 year

### ✓ **Category M:**

- ✓ Seat leakage testing by e.g. flow meter, bubble pot, pressure measurement etc.

### ✓ **Category S:**

- ✓ Seat leakage test in shop

# Possible Test Methods

Realistic Max. Allowable Leak rate in Mass Flow  
(SRS Form or Appendix C)

## Function test + Travel test incl. visual confirmation:

- MALR has to be >>
- Non-severe application
- Maintenance history ok
- Visual Confirmation
- DI/DO check

## In-line flow meter or clamp-on etc:

- max. allowed inaccuracy ~5%
- validate flow meter performance
- .....

## Pressure test:

- required resolution of measurement
- convert pressure loss into leak rate
- Cost to set up test versus shop test
- .....

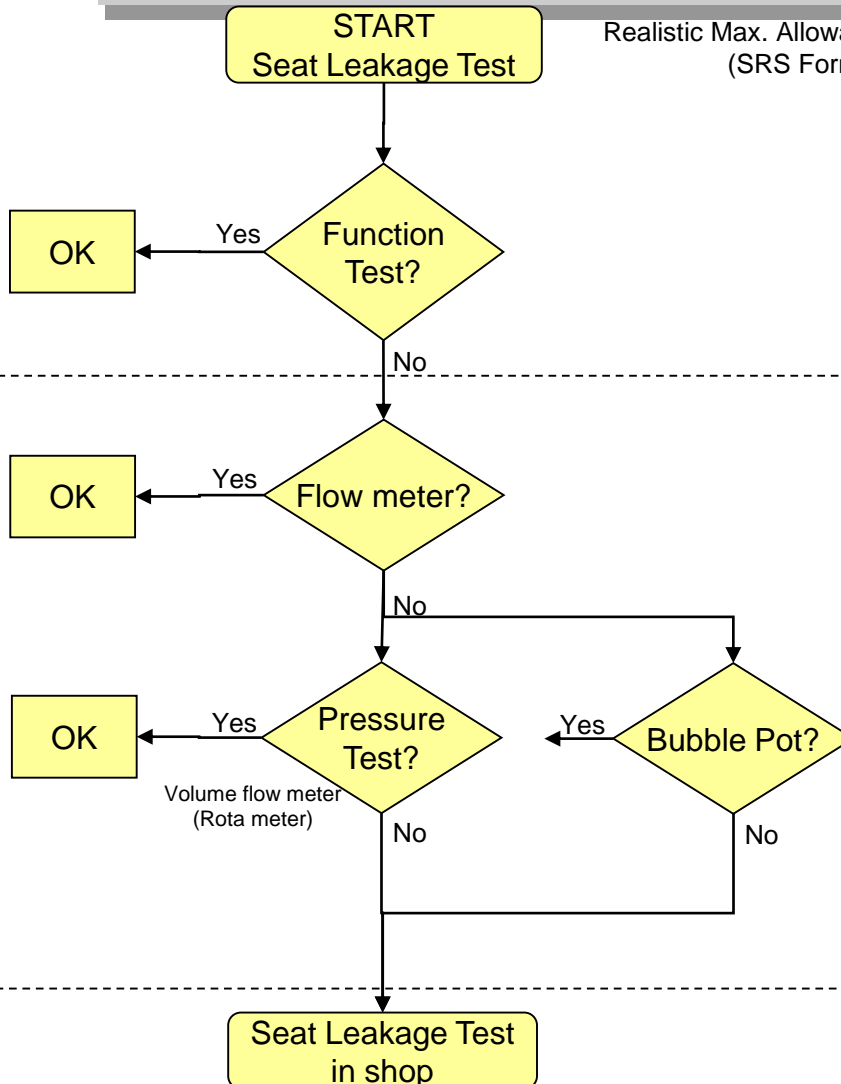
## Bubble Pot:

- max number of bubbles that can be counted
- convert leak rate into number of bubbles
- Cost to set up test versus shop test
- .....

Category F

Category M

Category S



# Kleppen response tijden

Realistisch ?

Wat als bepaald is dat vanwege  
waterhammer de response tijd lang  
wordt ??

nd.nl/cartoons



# SIL bijeenkomst KiC BEDANKT

Kees Kaijser  
DOW