Certification from A Manufacturers Perspective

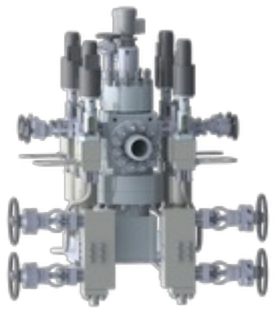
How lessons learned from the process industry can be applied in Balance of Plant applications

John van Gorsel
Sr. Product Manager Pressure Solutions, Europe

EMERSON

Emerson Automation Solutions

IEEE Std.323,
IEEE std 344
KTA 3505



ISO 14001:2015
PED 2014/68/EU
OHSAS 18001:2007
CSEI
SGU-Management System
HAF 604 and HAF601
10CFR50 Appendix B
CEFRI-E
ISO 29990

ASME Section I
ASME Section III N. NV. NPT
ASME Section V
ASME Section VIII UV
ASME Section IV
ASME Section XI
RCC-M
KTA 1401
DIN EN ISO 3834-2
DIN EN ISO 9001:2015

INSTRUMENTS

Magmeter & Vortex

Ultrasonic

DP Flow

Pervasive Sensing

Corrosion & Erosion Monitoring

Core Pressure

Temperature

Level

High Integrity

Liquid & Gas Analysis

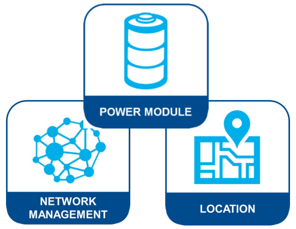
Flame & Gas Detection

SOLUTIONS

Integrated Systems

Tank Gauging

Plantweb Insight



Marine Systems

SERVICES

Plan & Design
- Site Audits & Consulting
- STO Project Management
- FEED

Improve & Modernize
- Turnaround Management
- Digital Transformation Implementation

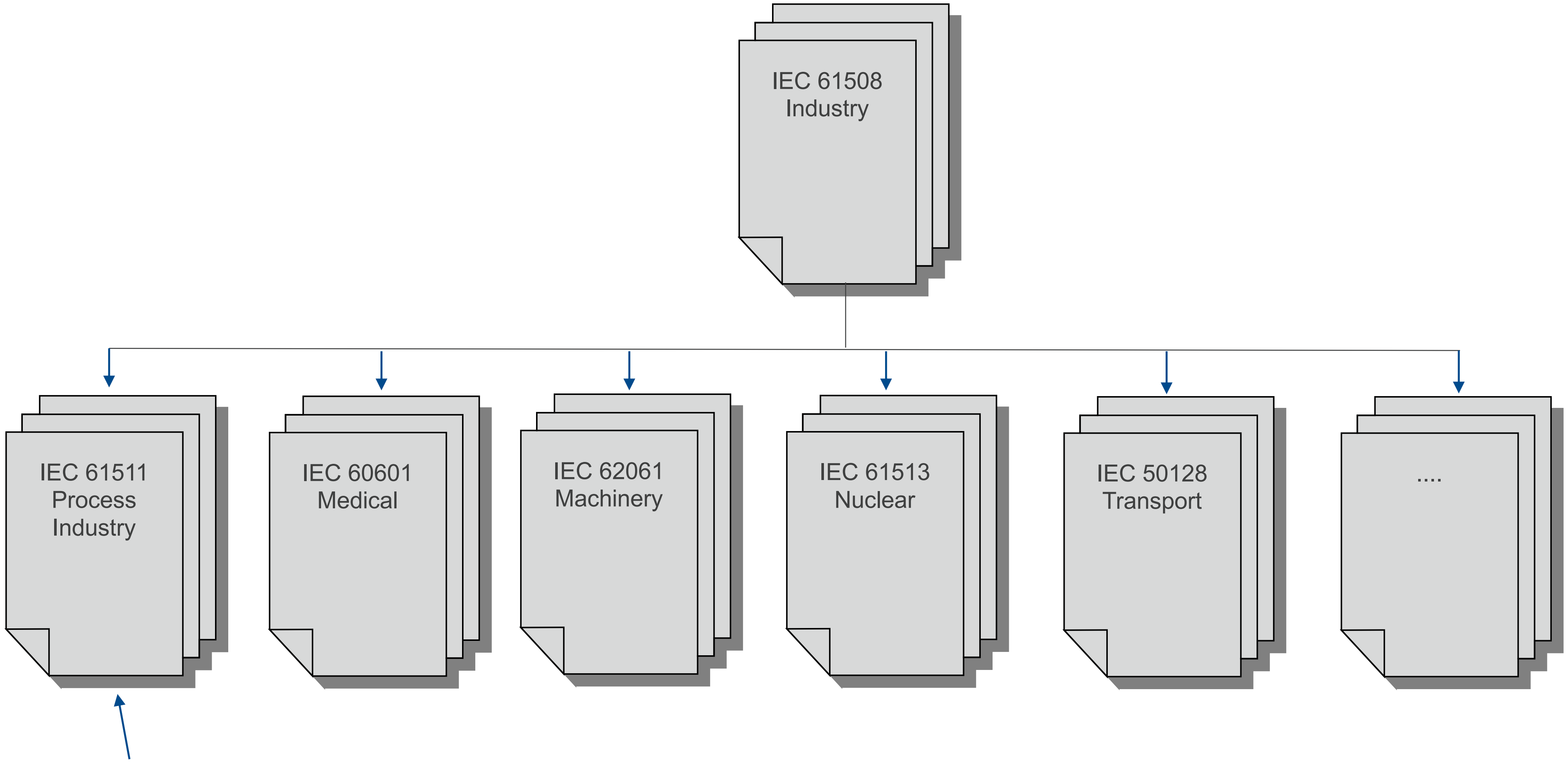
Operate & Maintain
- Long-term Service Agreements
- Certification
- Critical Spare Management
- Repairs

Train & Develop

Challenges and Lessons Learned

- Balancing safety and availability
  - Certification is not the full story
    - Most measurement issues are caused by the process and not by the device
  - Saving on architectural cost may lead to increased maintenance cost
    - Example: using a single sensor in a SIL2 loop
  - Ignoring the Spurious Trip Rate may reduce availability
- Maintaining safety functions
  - How to test the devices and safety functions
- Ease of use
  - Companies initially found that most of the effort in implementing a safety framework was spent on educating personnel
  - Smart instruments can have many configurable parameters

Standards



USA equivalent: ANSI/ISA S84.00.01

Namur NE130
Guideline for Proven in Use

The Safety Lifecycle

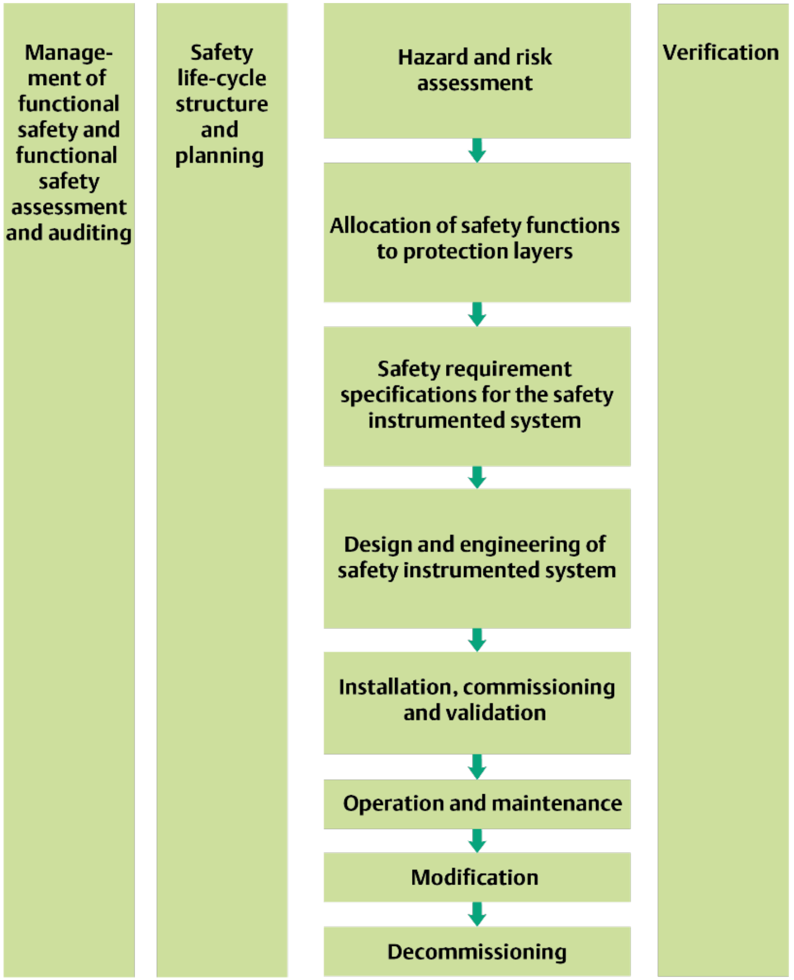
1. **Risk analysis**
   - The outcome of the risk analysis is the Safety Integrity Level (SIL) of the asset
   - The risk analysis is an iterative process

2. **Select architecture and components for the safety loop**
   - 1oo1, 2oo3, diversity, etc.

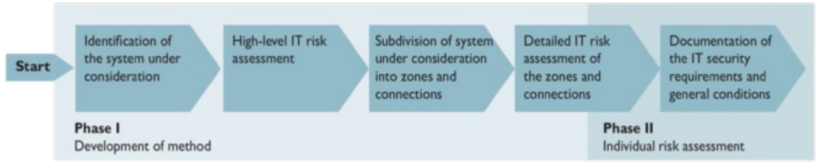
3. **Calculate and document**
   - Calculate the loop Probability of Failure on Demand (PFD_{avg})

4. **Maintain the safety loop**
   - Proof Testing is required to maintain a certain PFD_{avg} over the lifecycle

5. **Evaluate**



IEC 61511 Life Cycle



Namur NE193 Step Process

Observed Approach of the Process Industry

- The IEC61508 and IEC61511 methodology is used
  - In Safety Instrumented Systems (as intended)
  - In applications that could cause environmental damage (leaks, overspill)
  - In applications that could cause significant production loss
- Preference for using IEC61508 certified devices
  - Reduced cost for maintaining safety documentation
    - Device hardware and firmware revision management
- Preference for universal devices
  - Same device for Basic Process Control and Safety
    - Same functionality and performance
    - Same configuration tools

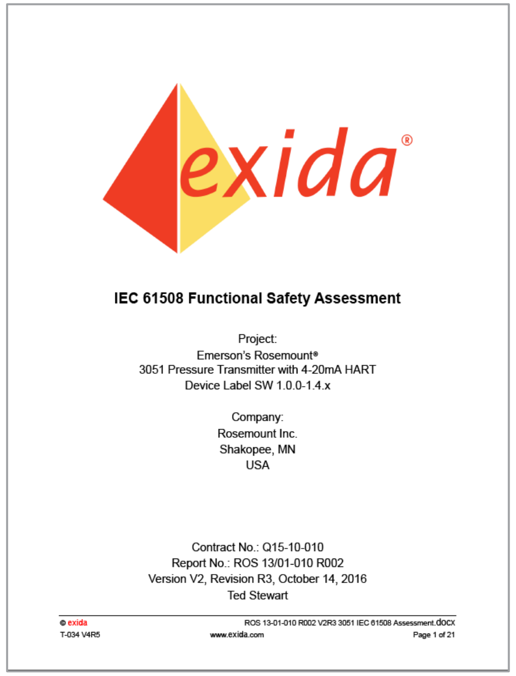
Health	Asset	Environment	Company image	>0.1/yr Likely	<0.1/yr Probable	$<10^{-2}$/yr Occasional	$<10^{-3}$/yr Remote	$<10^{-4}$/yr Improbable
Multiple fatalities ($<10^{-5}$/yr)	Extensive damage (>$10M)	Massive effect	International impact	Stop	Stop	SIL 3	SIL 2	SIL 1
Single fatality ($<10^{-4}$/yr)	Major damage (<$10M)	Major effect	National impact	Stop	SIL 3	SIL 2	SIL 1	
Major injury ($<10^{-3}$/yr)	Major damage (<$500K)	Localized effect	Considerable impact	SIL 3	SIL 2	SIL 1		OK
Minor injury ($<10^{-2}$/yr)	Minor damage (<$100K)	Minor effect	Minor impact	SIL 2	SIL 1		OK	OK
Slight injury (<0.1/yr)	Slight damage (<$10K)	Slight effect	Slight impact	SIL 1		OK	OK	OK
None	None	None	None	OK	OK	OK	OK	OK

Extended risk-matrix

Selecting Instruments for Safety Applications

- Devices certified to IEC61508 (route 1_H and 2_H)
  - Supplier provides the failure rates and effectiveness of suggested Proof Tests of the device
  - The end user must assess the failure rates of process interface, cabling, etc.
  - It is recommended to use a dedicated tool such as exSILentia for the overall calculation
- Following the IEC61511 Prior Use route
  - End user is responsible for obtaining the failure rate and effectiveness of Proof Tests
  - There are specific requirements for the collection of data
  - Namur NE093 and NE130 provide guidelines on how to collect data


Certificate / Certificat
Zertifikat / 合格証
ROS 061218 C001
exida hereby confirms that the:
3051S Pressure Transmitter
Software Revision 7.0 and Above
Emerson Automation Solutions
(Rosemount Inc.)
Shakopee, MN - USA
Has been assessed per the relevant requirements of:
IEC 61508 : 2010 Parts 1-7
and meets requirements providing a level of integrity to:
Systematic Capability: SC 3 (SIL 3 Capable)
Random Capability: Type B Element
SIL 2@HFT=0 SIL 3@HFT=1, Route 1_H
For models where SFF ≥ 90%
SIL 2@HFT=0 SIL 3@HFT=1, Route 2_H
PFD_{AVG} and Architecture Constraints must be verified for each application
Safety Function:
Emerson's Rosemount 3051S Pressure Transmitter will measure pressure/level/flow within stated performance specifications when operated within the environmental limits found in the product manual. Extended ambient operating temperature range options (down to -60C) must be specified in the model code along with option code QT for this certificate to remain valid across the extended ambient temperature limits.
Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.
Evaluating Assessor
Certifying Assessor
Page 1 of 2

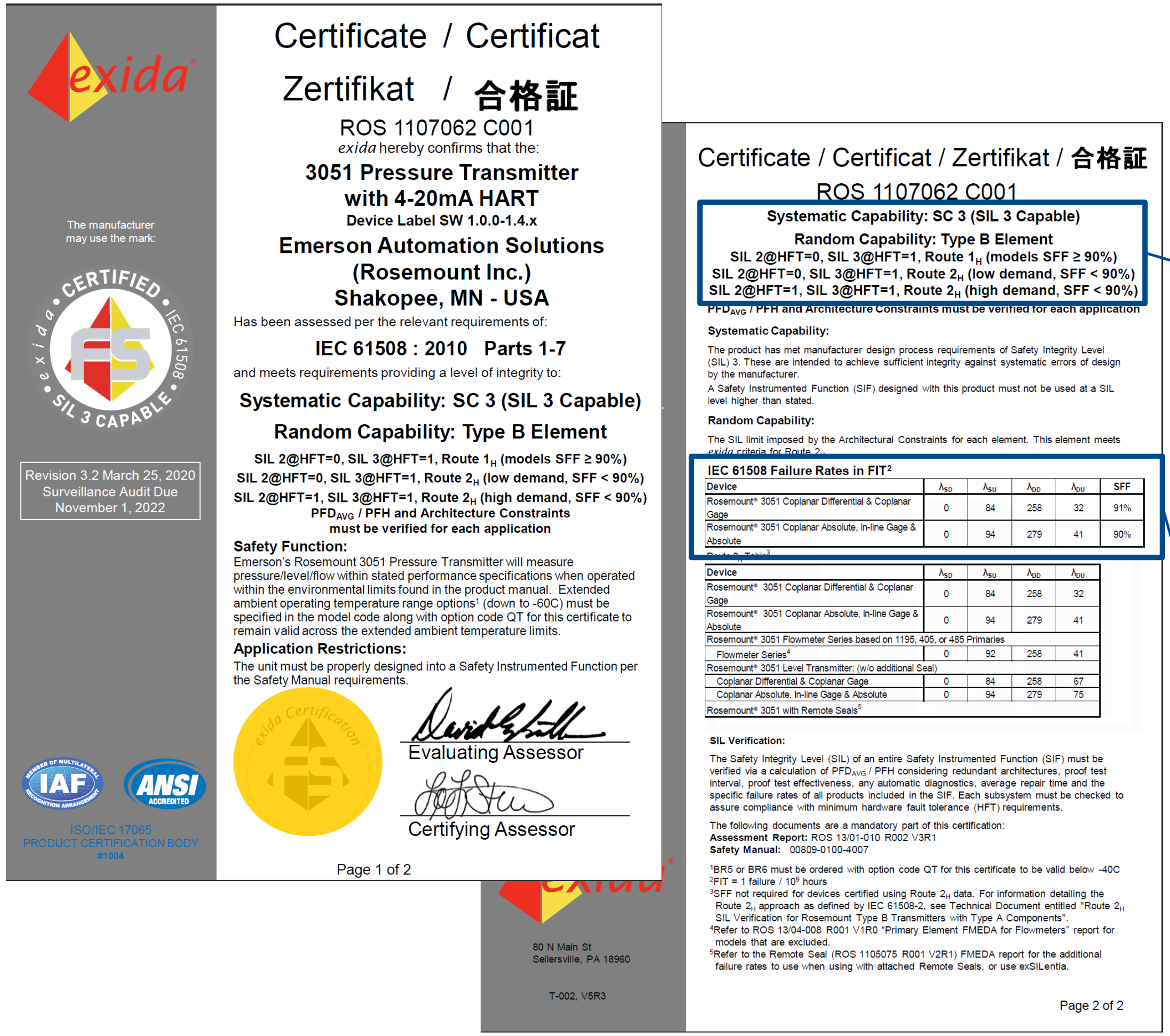

IEC 61508 Functional Safety Assessment

Project:
Emerson's Rosemount®
3051 Pressure Transmitter with 4-20mA HART
Device Label SW 1.0.0-1.4.x

Company:
Rosemount Inc.
Shakopee, MN
USA

Contract No.: Q15-10-010
Report No.: ROS 13/01-010 R002
Version V2, Revision R3, October 14, 2016
Ted Stewart

Certificates in Detail



Certificate / Certificat

Zertifikat / 合格証

ROS 1107062 C001

exida hereby confirms that the:

3051 Pressure Transmitter with 4-20mA HART

Device Label SW 1.0.0-1.4.x

Emerson Automation Solutions (Rosemount Inc.) Shakopee, MN - USA

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2@HFT=0, SIL 3@HFT=1, Route 1_H (models SFF ≥ 90%)

SIL 2@HFT=0, SIL 3@HFT=1, Route 2_H (low demand, SFF < 90%)

SIL 2@HFT=1, SIL 3@HFT=1, Route 2_H (high demand, SFF < 90%)

PFD_{AVG} / PFH and Architecture Constraints must be verified for each application

Safety Function:

Emerson's Rosemount 3051 Pressure Transmitter will measure pressure/level/flow within stated performance specifications when operated within the environmental limits found in the product manual. Extended ambient operating temperature range options[1] (down to -60C) must be specified in the model code along with option code QT for this certificate to remain valid across the extended ambient temperature limits.

Application Restrictions:

The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

The manufacturer may use the mark:

Revision 3.2 March 25, 2020
Surveillance Audit Due November 1, 2022

ISO/IEC 17065 PRODUCT CERTIFICATION BODY #1004

Evaluating Assessor

Certifying Assessor

Page 1 of 2

Certificate / Certificat / Zertifikat / 合格証

ROS 1107062 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2@HFT=0, SIL 3@HFT=1, Route 1_H (models SFF ≥ 90%)

SIL 2@HFT=0, SIL 3@HFT=1, Route 2_H (low demand, SFF < 90%)

SIL 2@HFT=1, SIL 3@HFT=1, Route 2_H (high demand, SFF < 90%)

PFD_{AVG} / PFH and Architecture Constraints must be verified for each application

Systematic Capability:

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints for each element. This element meets *exida* criteria for Route 2_H.

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} / PFH considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of this certification:

Assessment Report: ROS 13/01-010 R002 V3R1

Safety Manual: 00809-0100-4007

80 N Main St Sellersville, PA 18960

T-002, V5R3

Page 2 of 2

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2@HFT=0, SIL 3@HFT=1, Route 1_H (models SFF ≥ 90%)

SIL 2@HFT=0, SIL 3@HFT=1, Route 2_H (low demand, SFF < 90%)

SIL 2@HFT=1, SIL 3@HFT=1, Route 2_H (high demand, SFF < 90%)

SIL2 can be achieved with a single device

SIL3 requires redundancy

IEC 61508 Failure Rates in FIT[2]

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
Rosemount® 3051 Coplanar Differential & Coplanar Gage	0	84	258	32	91%
Rosemount® 3051 Coplanar Absolute, In-line Gage & Absolute	0	94	279	41	90%

Route 2_H Table[3]

Determine false trip rate

Determine safety

Emerson Portfolio of Safety Certified Measuring Devices

Pressure

Rosemount 3051S with Advanced Diagnostics	
Rosemount 3051S Transmitter	
Rosemount 3051 Transmitter	
Rosemount 2051 Transmitter	
Rosemount Primary Elements	
Rosemount 1199 Diaphragms	

Temperature

Rosemount 3144P Transmitter	
Rosemount 644 Transmitter	
Rosemount 248 Transmitter	

Tank Gauging

Rosemount 5900C Guided Wave Radar	
Rosemount 5900S 2-in-1 Radar Level Transmitter	

Level

Rosemount 5408 Non-Contacting Radar	
Rosemount 5300 Guided Wave Radar	
Rosemount 2140 SIS Level Switch Vibrating Fork	
Rosemount 2130 Level Switch Vibrating Fork	
Rosemount 2120 Level Switch Vibrating Fork	

Flow

Micro Motion 5700 Transmitter	
Micro Motion 4200 Transmitter	
Micro Motion 1700/2700 Transmitter	
Rosemount 8800 Vortex Flowmeter	

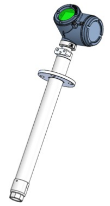
Flame Detectors

Rosemount 975 Multi-Spectrum Infrared Flame Detector	
Rosemount 936 Open Path Combustible	
Rosemount 935 Open Path Combustible	

Flame & Gas

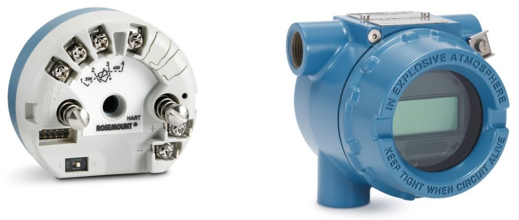
Rosemount 925/625 Point Gas Detector	

Combustion (FY23 H1)

Rosemount CX2100	

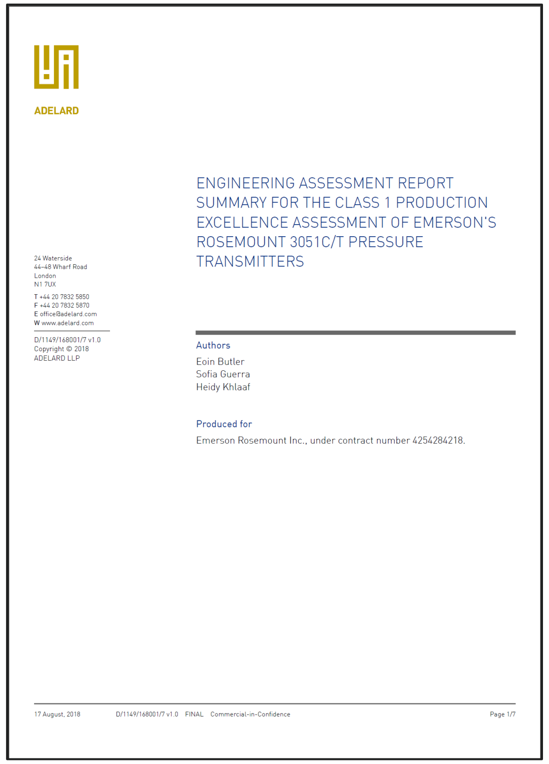
Emphasis Assessment

- Assessment required for UK Nuclear industry
  - Two “legged” approach
    - Production Excellence (PE)
    - Independent confidence-building measures (ICBMs)
  - Builds on IEC61508



644: Class 2

3051: Class 1 and Class 2



ADELARD

ENGINEERING ASSESSMENT REPORT SUMMARY FOR THE CLASS 1 PRODUCTION EXCELLENCE ASSESSMENT OF EMERSON'S ROSEMOUNT 3051C/T PRESSURE TRANSMITTERS

24 Waterside
44–48 Wharf Road
London
N1 7UX

T +44 20 7832 5850
F +44 20 7832 5870
E office@adelard.com
W www.adelard.com

D/1149/168001/7 v1.0
Copyright © 2018
ADELARD LLP

Authors

Eoin Butler
Sofia Guerra
Heidy Khlaaf

Produced for

Emerson Rosemount Inc., under contract number 4254284218.

17 August, 2018 D/1149/168001/7 v1.0 FINAL Commercial-in-Confidence Page 1/7

GRADING
(Use strategy triangle to define scope and approach)

Class 3
- Type tests
- Review of hardware reliability calculations
- Commissioning tests
- Review of field data
- Consideration of manufacturer’s pedigree

Class 2 - source code	Class 2 - no source code
As for Class 3 plus: - Dynamic analysis - Static analysis And possibly: - Statistical testing	As for Class 3 plus: - Dynamic analysis - Statistical testing - Justification of use in spite of no access to code

Class 1 - source code always required
As for Class 2 (static analysis to include functional analysis) plus:
- Statistical testing
- Justification of tools used (including compiler validation)

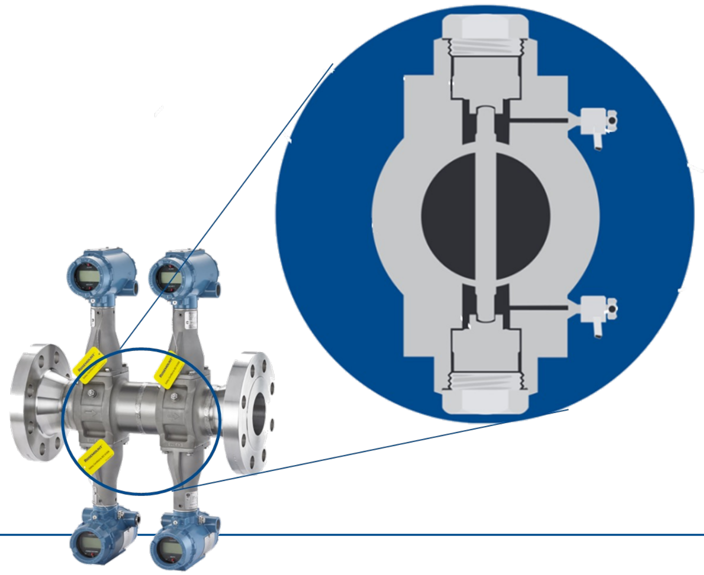
SIL per IEC61508	PFD_{avg} range	Emphasis class
1	$\geq 10^{-2}$ to $< 10^{-1}$	Class 3
2	$\geq 10^{-3}$ to $< 10^{-2}$	Class 2
3	$\geq 10^{-4}$ to $< 10^{-3}$	Class 1
4	$\geq 10^{-5}$ to $< 10^{-4}$	Class 1

Hardware Supporting Safety

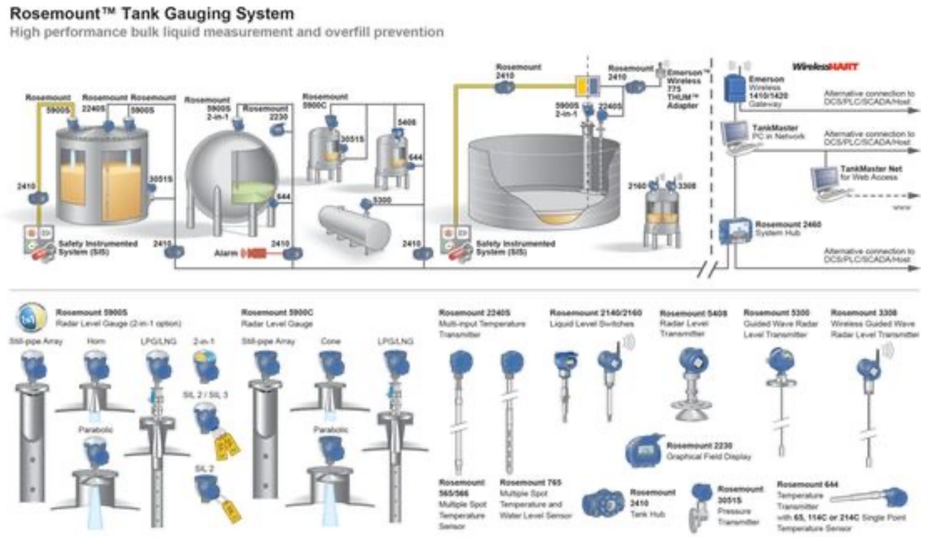
Dual and Quad Vortex

2-in-1 Radar Level Gauge

- Redundant sensors without flow disturbance
- Safety certified with SIL2 capability
  - SIL3 systematic capability with redundant sensors



- Dual radar in a single housing
- Safety certified with SIL2 and SIL3 capability



Proof Testing

B.1 Suggested Partial Proof Test

The suggested proof test described in Table 8 will detect 51% of possible DU failures in the Rosemount 3051 Coplanar Differential & Coplanar Gage and 41% of possible DU failures in the Rosemount 3051 Coplanar Absolute, In-Line Gage & Absolute.

Table 8 Steps for Partial Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to
2.	Use HART communications to retrieve any diagnostics an
3.	Send a HART command to the transmitter to go to the high that the analog current reaches that value[8].
4.	Send a HART command to the transmitter to go to the low that the analog current reaches that value[9].
5.	Inspect the Transmitter for any leaks, visible damage or c
6.	Remove the bypass and otherwise restore normal operati

B.2 Suggested Comprehensive Proof Test

The suggested proof test described in will detect 90% of possible DU failures in both the Rosemount 3051 Coplanar Differential & Coplanar Gage and the Rosemount 3051 Coplanar Absolute, In-Line Gage & Absolute.

Table 9 Steps for Comprehensive Proof Test

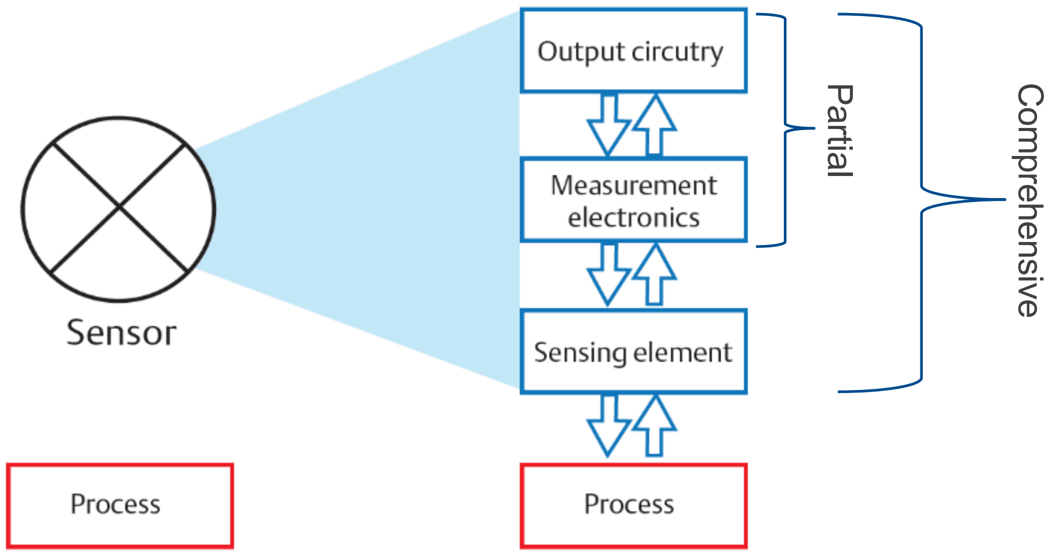
Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip
2.	Use HART communications to retrieve any diagnostics and take appropriate action.
3.	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value[10].
4.	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value[11].
5.	Inspect the Transmitter for any leaks, visible damage or contamination.
6.	Perform a two-point calibration of the transmitter over the full working range.
7.	Remove the bypass and otherwise restore normal operation

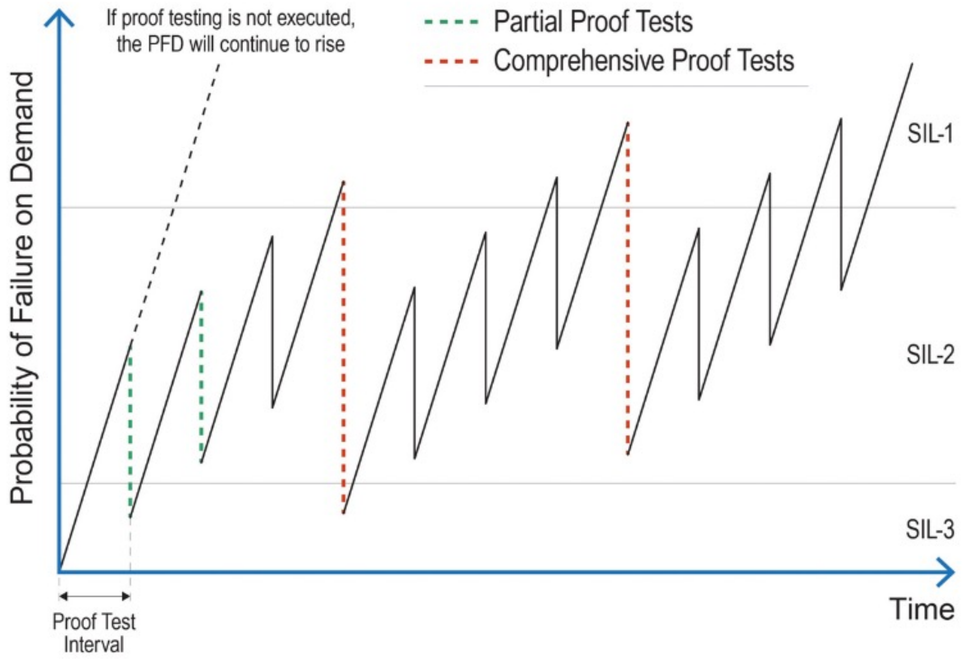
From the Safety Manual

- The chance of failure (PFD) increases with time
- A Proof Test checks for hidden failures and will (partly) reset the PFD
  - The magnitude of the reset is determined by the “Proof Test Effectiveness” or “Proof Test Coverage”
- Manufacturers can support this process by providing recommended Proof Tests with their effectiveness as a percentage of λ_{DU}

Table 10 Proof Test Coverage – Rosemount 3051

Device	Coplanar Differential & Coplanar Gage	Coplanar Absolute, In-Line Gage & Absolute
Rosemount 3051 - Partial	51%	41%
Rosemount 3051 - Comprehensive	90%	90%

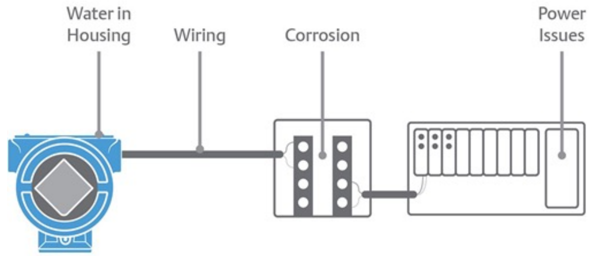




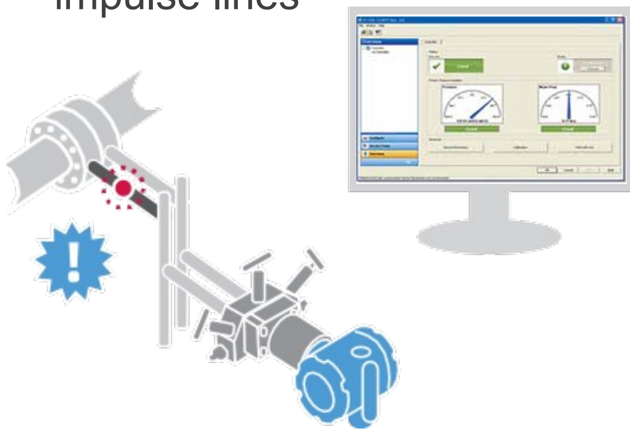
Diagnostic Capabilities Supporting Safety

3051S Pressure Transmitter

- Loop Integrity
  - Monitors and detects power supply issues

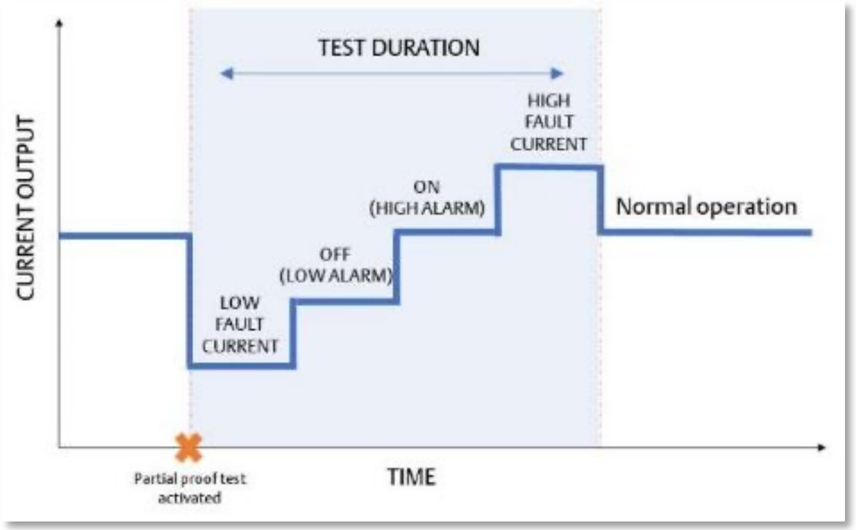


- Plugged Line Diagnostics
  - Monitors and detects plugging of impulse lines



2140 Level Switch

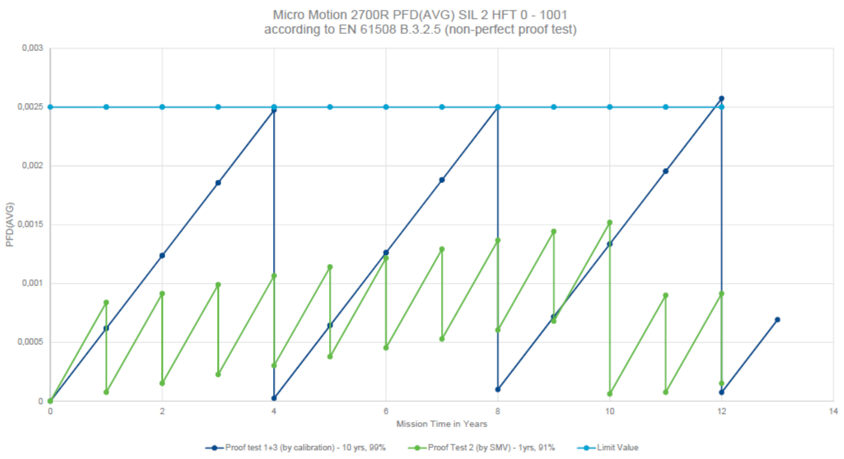
- Remote Proof Testing
  - Allows a proof test without the need to remove the device from the process



Micro Motion Flowmeter

- Smart Meter Verification
  - Monitors and detects mechanical changes to the internal tubing

	Proof Test Procedures	Proof Test Coverage (PTC)
1	4-20 mA loop check	50 %
2	**SMV** + 4-20 mA loop check	91 %
3	**Calibration** + 4-20 mA loop check	99 %

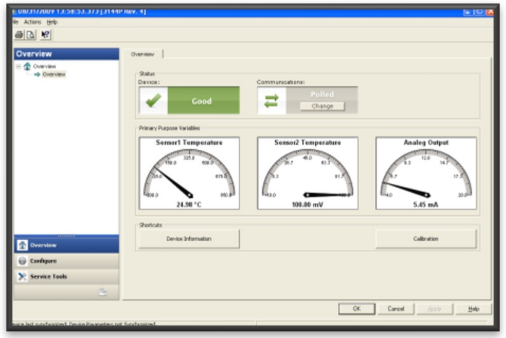


Ease of Use

Human Centered Design

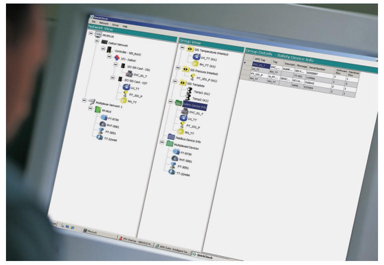
- Common look and feel

- Device Dashboards
  - Similar for different devices
  - Similar for different tools
    - eDD, DTM, or FDI based



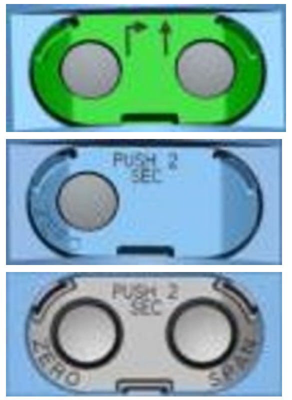
Common Tools

- HART Protocol based
  - Common terminology across vendors
  - Vendor-independent tools
- AMS Device Manager
  - Device configuration
  - Maintenance log, event log
  - Calibration log
- AMS Quick Check
  - Voting and interlock checking



Others

- Suggested Proof Test
- Guided Proof Testing
- Configuration Data Sheet
- Hardware options
  - Optional zero and/or span buttons
  - Write protect jumper/switch



Challenges and Lessons Learned – in Summary

- Balancing safety and availability
  - Certification is not the only thing consider
    - Devices must be suitable for the application
  - The right voting architecture and redundancy will optimize the balance between safety and availability
    - Redundancy requires assessment of common cause failures
  - Consider λs to assess the spurious trip rate
- Maintaining safety functions
  - Manufacture guidelines will make Proof Testing more robust
  - Guided Proof Testing will reduce time and avoid mistakes
  - A limited number of “critical parameters” reduces the risk of incorrect configurations
- Ease of use
  - Having the same instruments for safety and basic process control reduces cost and risk
  - A Human Centered Design strategy and well-designed tools will reduce complexities for personnel