



HIPPS Safety Requirements

Carsten Thoegersen SME - Actuation Technologies February 2016



Agenda

- Safety Requirement General Overview
- Safety Requirements related to:
 - Safety Lifecycle causes of failure
 - Lifecycle activities
 - SRS Safety Requirement Specification
 - Proof Test & Inspection
 - Test and Diagnostic Coverage Final Elements
 - Safety Integrity Level and Architectural constraints
 - Response Time for HIPPS
- A solution addressing all the safety requirements
- Questions





Safety Lifecycle-The causes of failure and the answers

All components of any solution can fail dangerously

Systematic failures

- Occur due to:
 - Designed in
 - Engineered in
 - Procedural
- Reduced by:
 - Better processes
 - Regular Verification
 - Consistent behaviour
- People make mistakes

Random failures

- Occur due to:
 - Inappropriate application
 - Bad design
 - Fatigue
- Reduced by
 - Material quality
 - Consistent appropriate design
 - Performance monitoring
- Everything breaks eventually



Safety Lifecycle-The causes of failure and the answers

Systematic failures Answer - The safety lifecycle

Random Failures Answer – Safety Integrity Levels





Primary Cause of Failure



Source: Out of Control, Health & Safety Executive, UK



IEC61511 Lifecycle Activities



According to IEC 61 511, a Clear SRS shall contain . _ _ _ _



NOTE 1 Whenever practicable, the safety instrumented functions should be separated from the non-safety instrumentad function

Proof Test and Inspection



- Safety devices usually do nothing
- We have to test them regularly so we know they still work!
 - How often?
 - How extensively?

The Proof Test Interval (TI) is defined during SIL Verification SIL Verification will also assume a certain "Proof Test coverage"; how many of the dangerous failures are revealed by the test?

• And we have to inspect them to check for damage, tamper or unauthorised modification





Where are failures most likely?



Increase Diagnostic Coverage – Final Elements



Safety Integrity Level and Architectural constrains

HIPPS is often required to meet SIL3, Some even specify SIL4. The different Safety Requirements/Considerations are:

| | HIPPS – SIL3 | HIPPS – SIL4 |
|------------------------|--|--|
| RRF | RRF of 1,000 – 10,000 | RRF > 10,000 |
| Logic Solver | Solid State and Programmable | Solid State only |
| Design | Acc. to IEC 61 508 and 511 | Acc. to IEC 61 508 only |
| Test and Inspection | Acc. to IEC 61 508 using the defined safety lifecycle | Acc. to IEC 61 508 re. Operation and Maintenance phases |
| HFT | According to IEC 61 511 HFT = 2 (Table 6) HFT = 1 for elements with Prior use justification | Acc. to 61 508 = Complex and rigorous, so expert guidance required |

Response Time for the HIPPS



Response Time of Final Element

HIPPS are often specified with a Response time of **3-5** seconds for **Gas** and **6-20** seconds for **liquid** pipelines.

We also see requirements down to **1** second, but to maintain a high integrity and avoid introducing risks, considerations should be given to:

Inertia of the Mass in the FE (mechanical integrity)



Water hammer effect for liquid pipelines





A Solution addressing all challenges



Questions



