Proof Testing of Safety Instrumented Systems (SIS)
3-15-2014
Presenter

William (Bill) Sholette
Level Products Business Manager
Endress + Hauser in Northeast USA.
Safety Instrumented Systems (SIS) in the Process Industry

- Definition of “Risk“
- Risk assessment and Risk reduction by SIS
- Safety Integrity Level (SIL)
- Functional Proof Testing
Reason:
- safety systems ignored during maintenance process
- inappropriate design of safety systems
- uncontrolled release of fuel from a vent stack
- inappropriate behavior of workers trying to start and remove a truck
- control room with many workers located close to distillation column

Consequence:
- 15 People KILLED
- 180 INJURED
- estimated costs
  US$1,000,000,000
Elk River Spill West Virginia January 2014

- Chemical Spill contaminates water supply for 300,000
What is „Risk“?

- Risk = Probability (P) of Event Occurrence x Damage (D)
- **Tolerable risk** = maximum risk, which is acceptable according to moral concepts (VDE 2180)
- Risk reduction: Reduction of initial risk below tolerable risk by organizational, constructional or protection measures (e.g. Safety Instr. Systems)
- Concept of Functional Safety:
  
  - Risk analysis
  - Quantification of Risk
  - Quantification of required Safety Level of Protection measures

**Safety Integrity Level (SIL)**
Tolerable Risk?
IEC 61508 & IEC 61511: Functional Safety of Electrical/Electronic/Programmable Electronic Systems

Manufacturer

IEC 61508
7 parts Manufacturers & suppliers of devices

IEC 61511
3 parts Safety Instrumented Systems Designers, Integrators & Users

American Standard: ANSI/ISA 84.01

safety related system standards

User

Functional Safety in the Process Industry
## Layers Of Protection

<table>
<thead>
<tr>
<th>Mitigation</th>
<th>Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plant emergency response</strong></td>
<td><strong>Emergency response layer</strong></td>
</tr>
<tr>
<td><strong>Embankment</strong></td>
<td><strong>Passive protection layer</strong></td>
</tr>
<tr>
<td><strong>Relief valve, rupture disk, F+G system</strong></td>
<td><strong>Active protection layer</strong></td>
</tr>
<tr>
<td><strong>Safety instrumented system</strong></td>
<td><strong>Emergency Shutdown</strong></td>
</tr>
<tr>
<td><strong>Alarm &amp; operator intervention</strong></td>
<td><strong>“Wild” process</strong></td>
</tr>
<tr>
<td><strong>Basic process control system or DCS</strong></td>
<td><strong>Normal process</strong></td>
</tr>
<tr>
<td><strong>Plant and process design</strong></td>
<td><strong>Inherent safe plant design</strong></td>
</tr>
</tbody>
</table>

| **Isolated protection layer** | **Trip level alarm** |
| **Process control layer** | **High level alarm** |
| **Process control layer** | **between high level and low level** |
Hazard and Risk Assessment of a Process

Risk graph:

Risk parameters:
W - Occurrence Probability
  W1: very low probability < 0.03/year
  W2: low probability < 0.3/year
  W3: relative high probability > 0.3/year
C - Extent of damage
  C1: slight injury
  C2: severe irreversible injury to one or more persons or death of a person
  C3: Death of several persons
  C4: Catastrophic consequences, multiple deaths
F - Exposure time
  F1: seldom to relatively frequent
  F2: frequent to continuous
P - Hazard Avoidance
  P1: possible under certain conditions
  P2: hardly possible

a - no special requirements
b - single system is not sufficient
Risk Reduction by Safety Instrumented Systems

Functional Safety in the Process Industry

Process Risk = P x D x PFD

Safety Instrumented System (SIS)
SIL x

Sensor

Logic unit

Actuator

Communikation e.g. 4…20 mA

Process interface

Residual Risk = P x D x PFD
# Functional Safety in the Process Industry

## „Quantification“ of Risk and Protection Measures

<table>
<thead>
<tr>
<th>Risk</th>
<th>SIL</th>
<th>Accepted frequency of a failure of the protection measure</th>
<th>Failure rate PFH</th>
<th>Failure probability PFD*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>SIL 1</td>
<td>&lt; 1 dangerous fault in 10 years</td>
<td>&lt;10⁻⁵ 1/h</td>
<td>&lt;10⁻¹</td>
</tr>
<tr>
<td>Mean</td>
<td>SIL 2</td>
<td>&lt; 1 dangerous fault in 100 years</td>
<td>&lt;10⁻⁶ 1/h</td>
<td>&lt;10⁻²</td>
</tr>
<tr>
<td>High</td>
<td>SIL 3</td>
<td>&lt; 1 dangerous fault in 1000 years</td>
<td>&lt;10⁻⁷ 1/h</td>
<td>&lt;10⁻³</td>
</tr>
<tr>
<td>Very high</td>
<td>SIL 4</td>
<td>&lt; 1 dangerous fault in 10,000 years</td>
<td>&lt;10⁻⁸ 1/h</td>
<td>&lt;10⁻⁴</td>
</tr>
</tbody>
</table>

PFH – Probability of Failure per Hour
PFD – Probability of Failure on Demand

* per demand, assuming 1 demand/year
Random Failures of Electronic Components

Note: Failure rate often specified in FIT = 1 Failure/10^9 h = 10^-9/h
Component failure modes
- Short circuit
- Interruption
- Drift
...

→ Resulting failure modes of safety function?
**Hardware-Failure Tolerance (HFT)**

- **HFT = 0** → no redundancy
  - 1 fault ➞ loss of safety function

- **HFT = 1** → redundant architecture
  - 2 faults ➞ loss of safety function

- **HFT = 2** → 3 channel architecture
  - 3 faults ➞ loss of safety function
Functional Safety in the Process Industry

Failure Mode Effect and Diagnostics Analysis (FMEDA)

Pre-condition: - determine safety path (e.g. 4…20 mA output)
- determine accuracy under fault condition (e.g. ± 2 %)

Failure modes:
- dangerous faults
- safe faults
- undetected faults
- detected faults

<table>
<thead>
<tr>
<th>Probability of Failure Modes</th>
<th>Detected faults</th>
<th>Undetected faults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe faults</td>
<td>( \lambda_{sd} )</td>
<td>( \lambda_{su} )</td>
</tr>
<tr>
<td>Dangerous faults</td>
<td>( \lambda_{dd} )</td>
<td>( \lambda_{du} )</td>
</tr>
</tbody>
</table>

\[ \lambda_{\text{tot}} = \lambda_{su} + \lambda_{sd} + \lambda_{du} + \lambda_{dd} (+\lambda_{\text{not relevant}}) \]

MTBF = \( 1/\lambda_{\text{tot}} \)

PFD, PFH
# Failure Modes of Safety Function

<table>
<thead>
<tr>
<th>Failure Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda_{sd}$</td>
<td>Safe detected Failure</td>
</tr>
<tr>
<td>$\lambda_{su}$</td>
<td>Safe undetected Failure</td>
</tr>
<tr>
<td>$\lambda_{dd}$</td>
<td>Dangerous detected Failure</td>
</tr>
<tr>
<td>$\lambda_{du}$</td>
<td>Dangerous undetected Failure</td>
</tr>
</tbody>
</table>

**Example (cont. overfill protection):**
Short circuit of 4..20 mA-output

- Current >20 mA indicates overfilling and

- “f”

**Example (limit switch 8/16 mA):**
Failure leads to 8 mA output

- Safety function activated (fault alarm!)

**Example:**
Ceramic cell broken in Deltabar

- Broken cell could result in a “valid” measured value but...

- Internal “Diagnostics” results in active sensor alarm

**Example:**
Output „frozen“ between 4...20 mA independent of the process variable

- no warning

- safety function not available
Safe Failure Fraction (SFF)

$$SFF = \frac{\sum \lambda_{sd} + \sum \lambda_{su} + \sum \lambda_{dd}}{\sum \lambda_{tot}}$$

Safe Failure Fraction (SFF) (in %)

Diagnostic measures
PFD – Probability of Failure on Demand

• What is the probability that an element in a Safety Instrumented System will fail when it is required to operate.
  – Example – A High-High level switch is used to prevent a tank overfill in the event the High level “Stop Fill” switch fails to operate.

What if it too failed to operate?
Proof Testing

- Partial Proof Testing
  Returns the PFD (Probability of Failure On Demand) to a percentage of the original.

- Full Proof Test
  Returns the PFD to almost 100% of the original. Because of time in service, reaching 100% is not attainable.

- The percentage of recovery is based on the tests ability to exercise Dangerous Undetected faults.
**Proof Testing**

**Example: point level measurement system**

- **Remove Instrument for "Bucket Test"**
  - Risk of sensor damage
  - Risk of environmental release
  - Risk to personnel who remove and re-install instrument
  - Downtime Impact
  - Maintenance resource impact

- **Raise Material in Vessel to Switch Level**
  - Risk of overfilling
  - Downtime Impact
  - Maintenance resource impact

- **In-Situ Instrument Test**
  - Provides capability to extend physical test interval via 99% partial proof test coverage (PTC)
  - Provides capability to reduce/maintain PFDavg in in-situ testing
  - Safe Failure Fraction (SFF) >99% with Continuous diagnostics coverage (DC) 70.5% and internal redundancy supports SIL3 1oo1 design
API (American Petrochemical Institute) recommended practice 2350 states:

“The High-High level overfill prevention switch must be tested without raising the level to a dangerously high condition”
Proof Testing
All Technologies Are Not Created Equal

• High- High Level Overfill
  – A Tuning Fork tested in a bucket of material is a valid full proof test.
  – A capacitance switch tested in a bucket of material is Not a valid full proof test.

Why Not?
Probability of a failure on demand - PFD

PFD \approx \lambda_{du} \cdot t \quad (\lambda t \ll 1)

Ti = Proof test interval
PTC = Proof test coverage = 92%
Partial Proof Testing (PTC < 98%)

\[ \text{PFD}_{\text{avg}} \approx \frac{1}{2} \lambda_{\text{du}} \times T_i \times \text{PTC} + \frac{1}{2} \lambda_{\text{du}} \times \text{LT} \times (1-\text{PTC}) \]

- PTC = Proof test coverage (1=98%)
- Ti = Test interval
- LT = life time
In-Situ Testing

What is the value of In-Situ testing in Dollars?

• A full proof test which removes the switch from the process for testing means:

• Process Downtime – lost production -10 hours at $10,000 per hour ($100,000)

• Maintenance Resource Time - $1500

• $101,500 per year X 12 years = $1,218,000 lifetime

Multiplied by the number of Overfill Switches in the facility
Other considerations:

- Possible damage to sensor
- Re-Installed incorrectly
- Exposure of personal and environment to process
- Disposal of process material
Summary

• Safety Instruments can protect personal, facilities, and the environment
• Periodic testing of safety instruments is critical to ensure operational integrity
• In-Situ testing can provide the required testing while saving millions of dollars
Thank You For Your Attention!

Questions?