Safety Instrumented Systems and the AWAKE Plasma Cell Control as a Use Case

THCPA01, Functional safety and machine protection

Enrique Blanco (CERN)
B. Fernandez, R. Speroni (CERN), Falk Braunmueller (MPI)
Outline

1. Goals
2. AWAKE plasma cell
3. Requirements
4. Project lifecycle engineering: design
5. Lessons learned and conclusions
Goals

Overview the **LIFECYCLE** of the safety instrumented system engineering

- Highlight the importance of the **REQUIREMENTS**: hazard identification and risk assessment
- Focus on the **DESIGN phase** using **standards**
  1. Machine/installation/process was not designed with a safe mission
  2. Use of not safety certified components

**Functionality**

- Show the integration with a basic **process control system (BPCS)**
AWAKE

- It is a proof-of-principle experiment which explores the use of plasma to accelerate particles to high energies over short distances.

- Use SPS accelerator protons to create wakefields and then a second beam of electrons is accelerated to TeV energies.

ILC Cavity: 35 MV/m

Plasma cell: 35 GV/m → 35 MV/mm !!
No need of vacuum, no magnets nor RF

http://www.cern.ch/awake
AWAKE plasma cell

Plasma cell = 10 meters
2 rubidium sources reservoirs
4 viewports (Rb density)
Operational requirements

1. Keeping the 10 meters plasma cell **isothermal** (~220 °C) avoiding cold spots and possible intermediate rubidium condensation.

2. Avoiding temperature dispersion larger than **0.05 °C** in some specific places

3. Providing a **safe environment** during operation with rubidium
Standards in Functional Safety Engineering

**IEC 61508**: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

**IEC 61511**: Functional safety for the Process Industry

**ISA 84**: Safety Instrumented Systems (SIS)

ISA 84.01-1996 did not require a quantitative assessment of PFDavg. Instead, it stated that the user could rely on past performance of an existing SIS design as the basis for justification of its continued use.
Simplified lifecycle

(1) Analysis
- Hazard identification
- Risk assessment
- Safety functions

(2) Realization
- Design
- Installation
- Commissioning

(3) Operation
- Maintenance for SIL
- Management of change

Management of safety
(1) Analysis

- Hazard analysis
- Risk assessment
- SIL determination

- Safety instrumented function determination (requirement)

Failures
Source: Yokogawa 2016
Analysis @ AWAKE

- **Safety file** or the result of the hazard analysis and risk assessment
- FMEA like document:
  - Hazards
  - Causes
  - Hazardous events
  - Consequences
  - Risk
  - Actions

FMEA: Failure Modes and Effects Analysis

27 hazardous events analyzed
### Table 1: Hazard analysis summary

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Cause</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rb</td>
<td>Oxygen contact</td>
<td>Burning, fire</td>
</tr>
<tr>
<td>Beam</td>
<td>Collisions</td>
<td>Radiation injury</td>
</tr>
<tr>
<td>Laser</td>
<td>Exposure</td>
<td>Eye damage</td>
</tr>
<tr>
<td>Toxic</td>
<td>Overheating</td>
<td>Respiratory</td>
</tr>
</tbody>
</table>

#### Risk evaluation table

<table>
<thead>
<tr>
<th>Potential severity</th>
<th>Risk evaluation [R]</th>
<th>Probability of the hazardous event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>1, 2, 3, 4</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>1, 2, 3, 4</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>1, 2, 3, 4</td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>1, 2, 3, 4</td>
</tr>
</tbody>
</table>

Weakest point on the viewports: SIS Control system

Access Control

Thermo-switch

SIL 2
Safety Instrumented Function (SIF): **SIL 2**

Isolate the **rubidium** inside the plasma cell by closing the valves behind the viewports once a leak of the plasma cell is detected.

![Plasma cell (viewports)](image1.png)

![Safety Instrumented Function Loop](image2.png)
(2) Realization

Procedure to achieve specified SIL

Hardware Safety Integrity
- Quantify random hardware failures AND
- Comply with requirements for Architectural Constraints

Systematic Safety Integrity
- Comply with requirements for systematic safety integrity OR
- Comply with requirements for Proven in Use (PIU)

IEC 61508
Hardware Safety Integrity

Quantify *random* hardware failures

**PFD** (Probability of failure under demand)

<table>
<thead>
<tr>
<th>SIL</th>
<th>$\text{PFD}_{\text{avg}}$</th>
<th>Risk Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$10^{-5} \leq \text{PFD} &lt; 10^{-4}$</td>
<td>100,000 to 10,000</td>
</tr>
<tr>
<td>3</td>
<td>$10^{-4} \leq \text{PFD} &lt; 10^{-3}$</td>
<td>10,000 to 1,000</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-3} \leq \text{PFD} &lt; 10^{-2}$</td>
<td>1,000 to 100</td>
</tr>
<tr>
<td>1</td>
<td>$10^{-2} \leq \text{PFD} &lt; 10^{-1}$</td>
<td>100 to 10</td>
</tr>
</tbody>
</table>

IEC 61508 *Low demand* SIL determination

Safety Instrumented Function architecture

Reliability Block Diagram
Quantify **random** hardware failures

PFD (Probability of failure under demand) simplified calculation:

\[ PFD = \lambda_D \times \frac{T}{2} \]  

(1) \( \lambda_D \): failure rate  
\( T \): proof test frequency

PFD of the selected architecture:

\[ PFD_{\text{Total}} = PFD_1 + PFD_2 + PFD_3 \]  

(2)

Non safety certified

\[ PFD_1 = \frac{\lambda_D^2 \times T^2}{3} + \beta \frac{\lambda_D \times T}{2} \]

\( \beta \): 20% (fraction of failures that have a common cause)  
\( T \): 4 weeks  
\( MTTF \): 156 years* (MTTF=\(1/\lambda_D\))  
* Pfeiffer notification

Fail safe Siemens PLC (including ET200M)

Certified **SIL 3**

\( 10^{-4} \leq PFD_2 < 10^{-3} \)

**SIL PFD avg Risk Reduction**

1. \( 0^{-5} \leq PFD < 10^{-4} \)  
   100,000 to 10,000

2. \( 10^{-4} \leq PFD < 10^{-3} \)  
   10,000 to 1,000

3. \( 10^{-3} \leq PFD < 10^{-2} \)  
   1,000 to 100

4. \( 10^{-2} \leq PFD < 10^{-1} \)  
   100 to 10

\( \beta \): 20% (fraction of failures that have a common cause)  
\( T \): 4 weeks  
\( MTTF \): 156 years* (MTTF=\(1/\lambda_D\))  
* Pfeiffer notification

IEC 61508 Low demand SIL determination

![Reliability Block Diagram](image)
Hardware Safety Integrity

Architectural Constraints (IEC 61508 places an upper limit on the SIL that can be claimed for any SIF on the basis of the HFT of its subsystems)

Route 1_H: based on:
- HFT: Hardware failure tolerance
- SFF: Safe Failure Fraction

Route 2_H: gives more importance on components reliability given by users feedback.

SFF = \frac{\text{Safe Failures} + \text{DD failures}}{\text{All Failures}}

<table>
<thead>
<tr>
<th>SFF</th>
<th>Type A</th>
<th>Type B</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;60%</td>
<td>SIL 1</td>
<td>SIL 1</td>
</tr>
<tr>
<td>60% ≤ 90%</td>
<td>SIL 2</td>
<td>SIL 2</td>
</tr>
<tr>
<td>90% ≤ 99%</td>
<td>SIL 3</td>
<td>SIL 3</td>
</tr>
<tr>
<td>≥ 99%</td>
<td>SIL 3</td>
<td>SIL 3</td>
</tr>
</tbody>
</table>

Solenoid valves
Type A: simple
HFT=0
Unknown SFF
SFF > 60%
Otherwise need redundancy
Systematic safety integrity

- Systematic capability (SC[1..4]). Measure of the confidence that the systematic safety integrity meets the requirements of the specified SIL.

**Route 1s**

Based on techniques and measures for avoidance & control of systematic failure tables

1. **TPG300**
   - SC1 compliant Design (EMI, env. stress, online monitoring)
   - Separated and redundant
   - TPG300 SC1 -> SC2

2. **S7-315F (fail safe PLC)**
   - SIL 3 compliant for systematic fail.
   - (IEC 61511) Application software must be SIL2
   - Low variability Language (ladder)
   - Verification by formal methods*

3. **Solenoid valves**
   - Basic information from supplier
   - The four valves must have an SC2 to claim the required SIL 2

* Formal verification:
  - PLCVerif: THPHA159
  - ITER use case: THPHA161
(3) Operation

Proof test

- Living system: Proof coverage is crucial for the SIL maintenance.
- Proof coverage includes the full SIF and not only a particular element.

Operational procedures

- Operators receive a full document on the safety functions
- Alarms and events are included in the supervision HMIs (alarm systems)
- Sometimes override of a SIF is possible, but this must be carefully monitored and detected

Management of change

- Procedure ISA-84.00.01
- All changes are traced and follow a strict procedure on validation before deployment.
- Standard gives guidelines on what to test/verify again in case of a change.
BPCS: UNICOS-CPC framework

Control functionalities
- PLC + SCADA based application
- Based on the UNICOS-CPC framework (ISA-88)
- 100 TT (PT100), 6 PT, 8 OnOff valves, 17 PWM
- Get an isothermal behavior till ~ 220 °C

Integration & safety
- BPCS: first layer of protection (no credit given)
- Second layer of protection (important alarms)
- Natural integration with the SIS
- Monitoring of the SIS events & alarms (interface)
Lessons learned & conclusions

✔ AWAKE plasma cell: equipment already designed without “safe” considerations:
  • Meeting the specified SIL would need to replace the solenoid valves by other with safe characteristics, or proven reliability data, or a different architecture.
  • Or the viewports could be reinforced, hence the SIL requirement lowered

✔ Design engineering based on sector specific standards: IEC 61508 & IEC 61511 (ISA 84)
  • SIL compliance: reliability of the hardware (random) and the architecture constraints and systematic capabilities.
  • Non safety classified equipment can be employed but requires additional information (maintenance database and user experience). But “Prior in use” or “Proven in use” claims require substantial evidence and cannot be easily be used
  • Proof test frequency is a key factor
  • Allocate safety instrumented functions to the SIS and not to the BPCS.

✔ Formal verification of the solver logic becomes significant for the systematic capabilities
Acknowledgements

Industrial Controls & Safety group
Beams Department
CERN, Geneva (Switzerland)

AWAKE team

MPI (Max Plank Institute, Germany)

Wright Design Limited (UK)
Enrique Blanco Viñuela
Automation engineer, PhD in systems and process engineering.
Head of the Control Systems Engineering (AP) section
Industrial controls & safety group in the beams department at CERN