Functional Safety Activities

(1)

ALBA – CERN workshop

Borja Fernández Adiego BE/ICS
Functional safety in ICS

• 2 different teams performing Functional Safety solutions:
  
  • **Process control & safety** (*Thursday afternoon module of the workshop*)
    
    Agenda
    • Introduction: standards and SIL (just some tips)
    • Examples of SISs
    • SIS specification and development
    • SIL compliance

  • **Personnel safety, access control** (*Friday morning module of the workshop*)
Process control and safety

• Functional safety activities following the IEC 61508 and IEC 61511 standards (a bit of IEC 62061)

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

• **IEC 61511**: specific for the process industry

• **IEC 62061**: specific for the machinery industry

• SIL (Safety Integrity Level) concept:
  • **Not only about hardware random failures** (PFD or PFH)
  • Hardware safety integrity (random failures & Architectural constrains)
  • Systematic safety integrity

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Demand Mode of Operation (average probability of failure to perform its design function on demand - PFD)</th>
<th>Continuous / High Demand Mode of Operation (probability of a dangerous failure per hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
<td>$\geq 10^{-6}$ to $&lt; 10^{-5}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
<td>$\geq 10^{-6}$ to $&lt; 10^{-5}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
</tr>
</tbody>
</table>
IEC 61508 safety lifecycle

1. Analysis
   • Risk analysis
   • Safety Instrumented Functions definitions

2. Realization
   • Implementation of the Safety Instrumented System
   • Steps to prove the SIL of one SIF

3. Commissioning, operation and management of the SISs
How can we reduce the risk?

- Reducing the severity of the consequence
- **Reducing the likelihood** of the consequence
  - SIS, SIFs, SIL
How can we reduce the **likelihood** of the risk?
Differences between IEC 61508 and IEC 61511


- IEC 61508 is a generic standard and useful for various industry sectors

- But some parts of the realization phase are applicable to equipment manufacturers

- IEC 61511 is user focused

- **They both have same lifecycle and SIL concepts**, but 61511 has a more specific language and context

<table>
<thead>
<tr>
<th>IEC 61508</th>
<th>IEC 61511</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety-related system</td>
<td>Safety Instrumented system (SIS)</td>
</tr>
<tr>
<td>Safety Function</td>
<td>Safety Instrumented Function (SIF)</td>
</tr>
<tr>
<td>EUC</td>
<td>Process</td>
</tr>
<tr>
<td>EUC control system</td>
<td>BPCS</td>
</tr>
</tbody>
</table>