T72 - Process Safety and Safety Instrumented Systems

Comprehensive Solutions Portfolio for Fail-Safe to TMR Safety Applications
Agenda

- Introduction To Process Safety
- Process Safety and Machine Safety
- Things to Consider When Choosing
- Rockwell Automation and Critical Control
- Questions
Agenda

Introduction To Process Safety

Process Safety and Machine Safety

Things to Consider When Choosing

Rockwell Automation and Critical Control

Questions
**Introduction to Process Safety**

**Terminology - BPCS and SIS**

**Basic Process Control System (BPCS)**

A system that responds to input signals from the equipment under control and/or from an operator and generates output signals, causing the equipment under control to operate in the desired manner.

**Safety Instrumented System (SIS)**

A system composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when pre-determined conditions are violated.
Introduction to Process Safety
What is Process Risk?

- **Prevent**
  - Basic Process Control System
  - Operator Intervention
  - Safety Instrumented System

- **Mitigate**
  - Plant and Emergency Response
  - Containment
  - Relief valve, Rupture disk

- **Emergency response layer**
  - Normal behavior
  - Process Control
  - Process shutdown
  - Process alarm

- **Process control layer**
  - Trip point
  - Safety layer
  - Emergency Shut Down

- **Active protection layer**
  - Pressure Relief

- **Passive protection layer**

- **Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved. 5**
Introduction to Process Safety
What Standards Apply

International Standards

IEC 61508  Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61511  Functional safety – Safety instrumented systems for the process industry sector

North American Standards

NFPA 85  Burner Management (Boilers, HRSGs, Stokers, etc.)

ANSI/ISA-84.00.01 (IEC 61511-1 Mod)  Functional Safety: Safety Instrumented Systems for the Process Industry Sector

API RP 14C  Safety Systems for Offshore Production Platforms

Reference Documents

CCPS  Guidelines for Safe Automation of Chemical Processes
Introduction to Process Safety
It is all about Tolerable Risk

Tolerable Risk 1 fatality in 10000 years
Safety Function: Close the valve if the pressure reaches a certain limit value

Safety Integrity Level (SIL) is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a Safety Instrumented Function (SIF).
SIL is a Way to Quantify Risk

Example Risks
- Hazards/Safety
- Security
- Environment
- Economic/PR

RISK reduction

How Bad?

Consequences

How Likely?

Chances

How Often?

Frequency

Same hazard – different location

- Hazards/Safety
- Security
- Environment
- Economic/PR
Introduction to Process Safety
Safety Integrity Levels

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Probability of Failure on Demand (PFD)</th>
<th>Risk Reduction Factor (1/PFD)</th>
<th>Safety Availability (1-PFD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>≥ .00001 to &lt; .001</td>
<td>&gt; 10,000 to ≤ 100,000</td>
<td>&gt; 99.99 to ≤ 99.999</td>
</tr>
<tr>
<td>3</td>
<td>≥ .001 to &lt; .01</td>
<td>&gt; 1,000 to ≤ 10,000</td>
<td>&gt; 99.9 to ≤ 99.99</td>
</tr>
<tr>
<td>2</td>
<td>≥ .01 to &lt; .1</td>
<td>&gt; 100 to ≤ 1,000</td>
<td>&gt; 99 to ≤ 99.9</td>
</tr>
<tr>
<td>1</td>
<td>≥ .1 to &lt; 1</td>
<td>&gt; 10 to ≤ 100</td>
<td>&gt; 90 to ≤ 99</td>
</tr>
<tr>
<td>0</td>
<td>Control (N/A)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For “Low Demand Mode” of operation

Performance requirements, not detailed implementation requirements
Table 5 – Minimum hardware fault tolerance of PE logic solvers

<table>
<thead>
<tr>
<th>SIL</th>
<th>Minimum hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SFF &lt; 60 %</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Special requirements apply (see IEC 61508)</td>
</tr>
</tbody>
</table>

3.2.63 redundancy

Use of multiple elements or systems to perform the same function; redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy).

NOTE 1 Examples are the use of duplicate functional components and the addition of parity bits.

NOTE 2 Redundancy is used primarily to improve reliability or availability.
Introduction to Process Safety
Control System Incidents

Changes After Commissioning 20%
Operations & Maintenance 15%
Installation & Commissioning 6%
Design & Implementation 15%
Incorrect & Incomplete Specification 44%

‘Out Of Control’ - A compilation of incidents involving control and safety systems by the UK Health & Safety Executive

Functional safety standards address all these issues
Industry Sectors - % of Process Safety Spend

- Oil & Gas (30%)
- Refining (19%)
- Petro Chemical (19%)
- Power (18%)
- Chemical (15%)

* Information source – IHS Technology 2015
Agenda

- Introduction To Process Safety
- **Process Safety and Machine Safety**
- Things to Consider When Choosing
- Rockwell Automation and Critical Control
- Questions
1. Introduction to IEC61511

1.1. What are IEC61508 and IEC61511?

IEC61508 is an international standard published by the International Electrotechnical Commission (IEC) and its primary objective is to address aspects to be considered when electrical, electronic or programmable electronic (E/E/PE) systems are used to perform safety functions.

IEC61508 [19.1], is a generic standard that applies to all E/E/PE safety-related systems, irrespective of their use or application. The title of the standard is:


The standard is founded upon the primary principle that there is a process that may pose a risk to safety or the environment, should something go wrong with the process or equipment. The standard is consequently aimed at process upsets and system failures, as distinct from health and safety hazards such as trips and falls, and allows process safety to be managed in a systematic, risk-based manner.

The standard assumes that safety functions are to be provided to reduce those risks. Safety functions may together, form a Safety Instrumented System (SIS) and their design and operation must be based on an assessment and understanding of the risks posed.

A secondary objective of IEC61508 is to enable the development of E/E/PE safety-related systems where application sector standards may not exist. Such second tier guidance in the process industry is covered by international standard IEC61511 [19.2]. The title of this standard is:


IEC61511 is not a design standard but a standard for the management of safety throughout the entire life of a system, from conception to decommissioning. Fundamental to this approach is the overall safety lifecycle which describes the activities that relate to the specification, development, operation or maintenance of a SIS.
Process Safety and Machine Safety

Different standards - Machinery

SAFEBOOK 4
Safety related control systems for machinery

SIL and IEC/EN 62061

IEC/EN 62061 describes both the amount of risk to be reduced and the ability of a control system to reduce that risk in terms of SIL (Safety Integrity Level). There are three SILs used in the machinery sector, SIL 1 is the lowest and SIL 3 is the highest.

Because the term SIL is applied in the same manner in other industrial sectors such as petro-chemicals, power generation and railways, IEC/EN 62061 is very useful when machinery is used within those sectors. Risks of greater magnitude can occur in other sectors such as the process industry and for that reason IEC 61508 and the process sector specific standard IEC 61511 include SIL 4.

A SIL applies to a safety function. The subsystems that make up the system that implements the safety function must have an appropriate SIL capability. This is sometimes referred to as the SIL Claim Limit (SIL CL). A full and detailed study of IEC/EN 62061 is required before it can be correctly applied.

PL and EN ISO 13849-1:2008

EN ISO 13849-1:2008 will not use the term SIL; instead it will use the term PL (Performance Level). In many respects PL can be related to SIL. There are five performance levels, PLa is the lowest and PLe is the highest.

Comparison of PL and SIL

This table shows the approximate relationship between PL and SIL when applied to typical circuit structures.

<table>
<thead>
<tr>
<th>PL (Performance Level)</th>
<th>$PFH_0$ (Probability of dangerous failure per hour)</th>
<th>SIL (Safety Integrity Level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>$\geq 10^{-5}$ to $&lt;10^{-4}$</td>
<td>None</td>
</tr>
<tr>
<td>b</td>
<td>$\geq 3 \times 10^{-5}$ to $&lt;10^{-5}$</td>
<td>1</td>
</tr>
<tr>
<td>c</td>
<td>$\geq 10^{-5}$ to $&lt;3 \times 10^{-6}$</td>
<td>1</td>
</tr>
<tr>
<td>d</td>
<td>$\geq 10^{-6}$ to $&lt;10^{-6}$</td>
<td>2</td>
</tr>
<tr>
<td>e</td>
<td>$\geq 10^{-7}$ to $&lt;10^{-7}$</td>
<td>3</td>
</tr>
</tbody>
</table>

Approximate correspondence between PL and SIL

IMPORTANT: The table shown above is for general guidance and must NOT be used for conversion purposes. The full requirements of the standards must be referenced.
Agenda

Introduction To Process Safety

Process Safety and Machine Safety

Things to Consider When Choosing

Rockwell Automation and Critical Control

Questions
Things To Consider When Choosing

Types of Questions we Ask

- What is the Target SIL level or SIL levels in single architecture?
  - SIL 1, Low Integrity; SIL 2, Medium Integrity; SIL 3, High Integrity

- What Levels of Fault Tolerance are Required?
  - Fail-Safe (Simplex), Fault Tolerance (Dual or Triplicated)

- What level of Integration with the Control Platform (BPCS) is required?
  - Separate & Diverse Logic Solvers, Common Logic Solvers

- Centralized or distributed safety
  - Central Processing, Remote I/O; Central Engineering Interface, Distributed Processing

- 3rd party communication & device interfaces
  - Smart Devices (HART); 3rd Party Logic Solvers (DCS or PLC)
Agenda

- Introduction To Process Safety
- Process Safety and Machine Safety
- Things to Consider When Choosing
- Rockwell Automation and Critical Control
- Questions
Targeted for applications where customers prefer a single/common architecture

Key Features:

• Safety Add-On Instruction
• Integrated Control & Safety
• I/O on EtherNet/IP
• Up-to-date with Logix releases
• Supports fail-safe and fault tolerant configurations

Common, Fault Tolerant/Fail Safe, SIL 2
Targeted for applications that require a flexible architecture, distributed safety and mixed SIL Levels

Key Features:

- Simplex (1oo1D), Dual (1oo2D) or TMR (2oo3) processor and I/O architectures
- Stand alone or part of a large distributed network
- Supports CIP connectivity to PlantPAx®
- Structured Text, FBD, and Ladder Diagram for Safety
- Comprehensive diagnostics and self-test
- Compiler Verification Tool
- Integrated Version Source Control
- HART Support for Field Device Diagnostics & Maintenance (HART pass through).

Modular, Distributed, Fault Tolerant/Fail Safe, SIL 2 & 3
Targeted for applications that require a Packaged and Configurable SIS

Key Benefits and Features:

- Based on AADvance modules
- Shorter lead-times, rapid deployment
- Quick installation, easy upgrades
- Minimized risk, lower installed costs
- Configurable (no programming required)
- Ready-to-install TUV-certified HW and validated SW
- Connectivity to smart field devices and asset management systems
- Meets SIL 3 requirements

Configurable, Fault Tolerant/Fail Safe, SIL 2 & 3
Targeted for applications that require a High Availability TMR architecture or have very high I/O counts.

Key Features:

- Extensive 2oo3 (2 out of 3) voting throughout architecture
- High density 40 channel TMR I/O modules
- CIP connectivity to PlantPAx
- Supports 1000’s of I/O with a single TMR processor
- Partial Stroke testing part of standard product offering
- Supports 24-120V DC or 120V I/O modules
- Supports performance levels required for Turbo Machinery Control
- Wide range of modules meeting SIL3
Agenda

- Introduction To Process Safety
- Process Safety and Machine Safety
- Things to Consider When Choosing
- Rockwell Automation and Critical Control

Questions
Thank You!