Process Safety & Critical Control
Rockwell Automation Process Safety Platforms

Name – Allan Rentcome
Title – Director Engineering – Process Safety
Agenda

An Introduction to Process Safety

Rockwell Automation Process Safety Philosophy

Rockwell Automation Process Safety Capability
Introduction to Process Safety
Terminology - BPCS and SIS

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.

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.

I/P
Basic Process Control System (BPCS)

PT 1A
PT 1B

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?

Mitigate

Prevent

Containment Passive protection layer

Plant and Emergency Response

Passive protection layer

Relief valve, Rupture disk Active protection layer

Safety Instrumented System Safety layer

Emergency response layer

Emergency Shut Down Pressure Relief

Trip point

Process Shutdown Process control layer

Operator Intervention Normal behaviour

Process Control Process control layer

Basic Process Control System

Process Setpoint

Process alarm
Confusion in the Industry with SIL

- What level of risk is tolerable?
- Which system is “suitable” (not best)?
- What technology should be used?
  - Relay, solid state, PLC or TMR?
- What level of redundancy is appropriate?
  - Single, dual or triple?
- How often should systems be tested?
  - Quarterly, yearly or per shutdown?
- What about field devices?
  - Technology, level of redundancy, etc.?
SIL is a way to Quantify Risk

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

RISK reduction

How Bad? - Consequences
How Likely? - Chances
How Often? - Frequency
Failure Modes

With a safety system, the concern shouldn’t so much be with how the system operates, but rather how the system fails. Safety systems can fail in two ways:

Safe failures
- initiating
- overt
- spurious
- costly downtime

Dangerous failures
- inhibiting
- covert
- potentially dangerous
- must find by testing

\[ D \times U = \]

SIL is a measure of dangerous failures only
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, HRSG’s, 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
An Introduction to Process Safety

Rockwell’s Process Safety philosophy

Rockwell’s Process Safety Capability
Process Safety Philosophy
Products and Solutions philosophy

- **Dedicated portfolio of products for process safety with architectures that support:**
  - Fault tolerance for system components
  - Scalable portfolio of technologies including fail-safe, fault tolerant and Triple Modular Redundant (TMR) options
  - SIL rated and certified up to SIL3 for use in Process Safety Solutions
  - Offers integrated and separated platform choices
  - Technology offering high level of diagnostics

- **Dedicated resources for design of complete Process Safety Solutions**
  - Global Solutions offers expertise to design, implement and deploy process safety solutions using functional certified safety engineers
  - Follows best engineering practices against IEC61511
An Introduction to Process Safety

Rockwell’s Process Safety philosophy

Rockwell’s Process Safety Capability
Which Platform
Portfolio Positioning

<table>
<thead>
<tr>
<th>Process Control</th>
<th>Process Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 0 Process</td>
<td>SIL 3 Fault Tolerance</td>
</tr>
<tr>
<td>SIL 1 Fail Safe</td>
<td>SIL 3 Fail Safe</td>
</tr>
<tr>
<td>SIL 2 Fail Safe</td>
<td>SIL 2 Fault Tolerance</td>
</tr>
<tr>
<td>SIL 2 Fault Tolerance</td>
<td>SIL 1 Fail Safe</td>
</tr>
<tr>
<td>SIL 3 Fail Safe</td>
<td>SIL 0 Process</td>
</tr>
</tbody>
</table>

Ethernet/IP communication: AADvance™ & PlantPAx™

PlantPAx (Logix) -> Trusted™

AADvance™ Scalable Safety

O&G / Petro-Chem applications favor AADvance™ & Trusted™
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)
Which Platform
ControlLogix®

Targeted for applications where customers who prefer a single architecture

Key Features:

- Safety AOIs
- 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
Which Platform
GuardLogix®

Targeted for applications that do not require High Availability

Key Features:
• Supports PointGuard Discrete and Analog I/O
• SIL2 inputs (single channel), SIL3 dual channel
• Common Network for Safe & Standard Communications
• Extensive suite of safety certified instructions
• Supports safety Add-On instructions
• Diagnostics and control in standard tasks
• Safety related functions in the safety task

Integrated, Fail Safe, SIL 3
1715 SIL 2

SIL 2 (CLX/1715)
SIL 3 (AADvance™)
High Availability
Interchangeable I/O
Infrastructure Support
Scalability

SIL 2

HART

SIL 3
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
- All 5 IEC 61131-3 programming languages
- Comprehensive diagnostics and self test
- Scalable fault-tolerance and safety at module level
- Fully fault-tolerant Ethernet networks for safety
- HART Support for Field Device Diagnostics & Maintenance (HART Passthru).

Interfaced, Fault Tolerant/Fail Safe, SIL 2 & 3
Portal & Network
Scalability & Connectivity

Ethernet based Safety Network

Workstation  Workstation  portal  NAS
Scalable Redundancy
Simplex (SIL 2)

1oo1D Fail Safe – Certified for use in SIL2 applications
AADvance™ Controller
Simplex

CPU Base with one CPU populated

I/O Base with one input and one output fail safe
Scalable Redundancy
Simplex (SIL3)

1oo1D/1oo2D Fail Safe – Certified for use in SIL3 applications
AADvance™ Controller
Simplex IO, FT CPU

Redundant CPUs
Scalable Redundancy
Redundant (SIL3)

1oo2D/2oo3 Fault Tolerant – Certified for use in SIL3 applications
AADvance™ Controller
Redundant CPUs
Redundant Terminations
Redundant inputs
Redundant outputs
AADvance™ Controller
Triplicated

- Triplicated CPUs
- Triplicated Terminations
- Triplicated inputs
- Fault Tolerant outputs
Targeted for applications that require a High Availability TMR architecture or have very high IO counts.

Key Features:
- Extensive 2oo3 (2 out of 3) voting throughout architecture
- Extensive diagnostics and triplication provides high safety, fault-tolerance & high availability
- High density 40 channel TMR IO modules
- CIP connectivity to PlantPAx
- Supports 1000’s of IO with a single TMR processor
- Partial Stroke testing part of standard product offering
- All 5 IEC 61131-3 programming languages
- Fully fault-tolerant Ethernet networks for safety

Interfaced, Fault Tolerant, SIL 3
Process Safety Philosophy
Solutions Capabilities

Process Development Phase
- Formulate concept and design of the process
- Identify Process Hazards (HAZOP etc)
- Identify non SIS layers of protection
- Determine if any, need for further risk reduction

SIS Design process
- Determine target SIL level
- Develop Safety Requirements Specification (SRS)
- Develop SIS design to meet SRS
- Select, build, test, deploy

Post deployment
- Install, commission and test prior to start-up
- Develop and implement maintenance and operational procedures
- Assess and manage modifications to SIS
- Decommission

Rockwell Automation provides a wide range of Expertise and Services throughout the project lifecycle
Questions?