Process Safety

Allan Rentcome
Director Engineering
Process Safety Technologies

Rockwell Automation
Process Solutions User Group (PSUG)
November 14-15, 2011
Chicago, IL - McCormick Place West
Rockwell philosophy for Process Safety

• 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
Technology and Process Safety Milestones

1960’s – 1970’s
- Alarming and Annunciation
- Pneumatic and Relay based Safety

1970’s – 1980’s
- Solid State Logic Safety Systems
- Processor Based Safety (VME, BUS based)

1980’s - Now
- Product Based solutions (TMR, 1oo2D, PLC’s)

2000 - Now
- ICSS

Corporate Standards
- International Standards
- Safety Specific Standards (S84/IEC 61508)

Certification Authorities
- TUV
What is a Safety Instrumented System?

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.
Typical Process Safety Applications

• Process Safety = Maximize System & Process Availability
  – Fault-Tolerance option for continued operation.
  – No Single Point of Failure
  – Add I/O and make changes online
  – Software and Firmware Upgrades
  – Hot Swappable Modules

• High Availability & Critical Control
  – Safety Instrumented Systems (SIS)
  – Emergency Shutdown Systems (ESD)
  – Fire and Gas Detection (F&G)
  – Burner/Boiler Management (BMS)
  – High Integrity Pressure Protection System (HIPPS)
  – Integrated Control and Safety (ICSS)
  – Turbo Machinery Control (Turbine and Compressor)
ESD/SIS Emergency Shut-Down System

- Often Separate and independent system from the BPCS referred to as an SIS/Safety Instrumented System.
  - Separate unit with own sensors and actuators that brings the process to a safe state if it goes out of control
- Requirements:
  - Require Analog 4-20 ma
  - Safety response – Fail-Safe to Fault Tolerant/High Availability
- SIL ranges served:
  - SIL 1 or 2 ControlLogix Fail-Safe or Fault Tolerant
  - SIL 1-3, TMR AADvance (Fail-Safe or Fault Tolerant)
  - SIL 3 TMR Trusted (Fault Tolerant)
- Typical Solutions:
  - Refining and Petrochemical processing
  - Offshore oil production
  - LNG
  - Gas Separation
  - Utilities (Fossil Fuel, Co-Gen, Nuclear)
Safety

Freedom from **unacceptable risk** of physical injury or damage to the health of people, either directly, or indirectly as a result of damage to property, assets or to the environment.

Functional Safety

**is part of the overall safety** that depends on a system or equipment **operating correctly** in response to its inputs.

What is unacceptable or acceptable risk?

How to measure the performance of the safety system
What is an acceptable or tolerable level of risk? Should a plant be as safe as:

- Riding a rollercoaster?
- Driving in your car?
- Staying at home?
- Flying in an airplane?

One measure of risk is FAR (Fatal Accident Rate). It is expressed as the number of deaths per 100 million man-hours. In the U.S., the chemical industry has a risk less than that of driving a car (FAR of 4 vs. 40).
Selection of Technology Raises Many Questions

• Which system is “suitable”?

• What technology should be used?
  – Automation Controllers, PLC, TMR, Dual, Relays

• 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.?

• What standards to follow?
It Can Be Complex to Make the Right Decision

• Does using a logic solver certified for use in SIL 3 give you a SIL 3 system?
• What level of risk is tolerable?
• Which is safer; a dual 1oo2 system, or a triplicated 2oo3 system?
• Can a system that’s 10 times more reliable, be less safe?
• How often should a safety system be tested?
• Is mean time to repair (MTTR) the same as mean down time (MDT)?
• If there hasn’t been an accident in your plant for 15 years, does that mean you have a safe plant?
Accidents & Resulting Legislation

- **Flixborough (UK)**
  1974: 28 deaths, > 100 injuries

- **Seveso (Italy)**
  1976: Major dioxin release

- **Bhopal (India)**
  1984: > 3,000 deaths, 200,000 injuries

- **Pasadena (US)**
  1989: 23 deaths, > 130 injuries

- **Texas City (US)**
  2005: 15 deaths, 180 injuries
Control System Incidents

From ‘Out Of Control’
A compilation of incidents involving control and safety systems by the UK HSE
Control System Incidents

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

Identified need for better standards, implementation and technology
Evolving Standards

- HSE, PES, 1987
- AIChE CCPS; Guidelines for Safe Automation of Chemical Processes, 1993
- ANSI/ISA 84; Application of Safety Instrumented Systems for the Process Industries, 1996 & 2004
- IEC 61508 (and 61511); Functional Safety - Safety Related Systems, 199
Process Safety Standards Today

- HSE, PES, 1987
- AIChE CCPS; Guidelines for Safe Automation of Chemical Processes, 1993
- ANSI/ISA 84; Application of Safety Instrumented Systems for the Process Industries, 1996 & 2004
- IEC 61508 (and 61511); Functional Safety - Safety Related Systems, 199
Key points to remember

• Key events in the last 30 years have become catalysts for legislation and evolution of standards.

• Early studies concluded many accidents as a result of poorly specified or implemented systems ( > 50% )

• Without standards some confusion within the industry on what are the correct technologies to use

• Vendors have some role but reviewing risk and hazards needs involvement of user

• IEC61511 / S84 key for Process Safety
Key Concepts Related to Standards

Key points to remember

- Standard covers safety life-cycle and includes analysis, realization and operation.
- Safety must be addressed from the beginning before detailed engineering.
- Zero risk cannot be reached.
- Non-tolerable risk must be reduced to as low as practically possible (ALARP).
- Standards are performance based.
- IEC61511 process industry specific.
- Process Safety technology selection is key.
Multiple Layers of Protection

- Community Emergency Response
- Plant Emergency Response
- Physical Protection (Dikes)
- Physical Protection (Relief Devices)
- Safety Instrumented System
- Alarms, Operator Intervention
- Basic Process Control

Process
Risk Reduction

- Residual Risk Level
- Tolerable Risk Level
- Risk inherent in the process

Other, Mech., SIS, Alarms, BPCS

Process
Risk Graph & SIL levels

Consequence
- Ca: Minor Injury
- Cb: Serious Injury, Single Death
- Cc: Several Deaths
- Cd: Many Deaths

Frequency & Exposure
- Fa: Rare to Frequent
- Fb: Frequent to Continuous

Possibility of Avoidance
- Pa: Sometimes Possible
- Pb: Almost Impossible

Probability of Occurrence
- W1: Very Slight
- W2: Slight
- W3: Relatively High

Safety Integrity Levels:
- a = No special safety requirements
- b = Single SIS not sufficient

Values:
- Ca
- Cb
- Cc
- Cd
- Fa
- Fb
- Pa
- Pb

Copyright © 2011 Rockwell Automation, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Probability of Failure on Demand (PFD)</th>
<th>Safety Availability (1-PFD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>≥ .00001 to &lt; .0001</td>
<td>&gt; 99.99 to ≤ 99.999</td>
</tr>
<tr>
<td>3</td>
<td>≥ .001 to &lt; .01</td>
<td>&gt; 99.9 to ≤ 99.99</td>
</tr>
<tr>
<td>2</td>
<td>≥ .01 to &lt; .1</td>
<td>&gt; 99 to ≤ 99.9</td>
</tr>
<tr>
<td>1</td>
<td>≥ .1 to &lt; 1</td>
<td>&gt; 90 to ≤ 99</td>
</tr>
<tr>
<td>0</td>
<td>Control (N/A)</td>
<td></td>
</tr>
</tbody>
</table>
## Safety Integrity Levels

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Risk Reduction Factor (1/PFD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>&gt; 10,000 to ≤ 100,000</td>
</tr>
<tr>
<td>3</td>
<td>&gt; 1,000 to ≤ 10,000</td>
</tr>
<tr>
<td>2</td>
<td>&gt; 100 to ≤ 1,000</td>
</tr>
<tr>
<td>1</td>
<td>&gt; 10 to ≤ 100</td>
</tr>
<tr>
<td>0</td>
<td>Control (N/A)</td>
</tr>
</tbody>
</table>
## 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; .0001</td>
<td>&gt; 10,000 to ≤ 100,000</td>
<td>&gt; 99.99 to ≤ 99.999</td>
</tr>
<tr>
<td>3</td>
<td>≥ .0001 to &lt; .001</td>
<td>&gt; 1,000 to ≤ 10,000</td>
<td>&gt; 99.9 to ≤ 99.99</td>
</tr>
<tr>
<td>2</td>
<td>≥ .001 to &lt; .01</td>
<td>&gt; 100 to ≤ 1,000</td>
<td>&gt; 99 to ≤ 99.9</td>
</tr>
<tr>
<td>1</td>
<td>≥ .01 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>
• Standards have evolved to be more performance than prescriptive
• S84 and 61508/61511 dominant
• Standards provide process and steps to follow for existing systems to determine SIL
• Functional Safety management needs competent, trained personnel, audits and assessments
• Hazard analysis and risk assessment key in determining SIL levels.
• Safety Layers within a process need consideration
Key Points...

Key points to remember

- SIL Levels state numerical performance of a safety function. i.e. likelihood of failure
- Availability is expressed as a % (1-PFD)
- RRF more intuitive statement of performance
- Large software based systems difficult to model and often good qualitative practices considered most effective
- PFD Calculations consider fault tolerance, test interval and diagnostic coverage
Process Safety Architectures Key Technology Concepts
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

Demand and no availability
Analyzing Diagnostic Coverage

Conventional Input Circuit
Analyzing Diagnostic Coverage

Failure of opto coupler

Normally closed field sw

Diagram with components and labels:
- Input: Vin
- Capacitor: 0.18 μF
- Resistors: 1K, 200K, 10K, 10K
- Diodes: D1, D2
- Transistor: OC1
- Voltage: +5V, 5V ISO.
Failure Mode vs. Technology

Safe    Dangerous

Relays    Solid State

%
Two types of failure modes must be considered:
- Safe failures, Dangerous Failures
- Dangerous Failures:
  - Must be tested for. Systems must implement diagnostics
  - Potentially dangerous if not revealed
  - Inhibiting in nature.
- Safe failures:
  - Costly (cause plant downtime)
  - Spurious
  - Can be mitigated with fault tolerance
- More complex the systems the more testing needed
Simplex System Architecture

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple architecture easy to implement</td>
<td>Dangerous faults still need to be tested for and for safety need diagnostics</td>
</tr>
<tr>
<td>Fail safe characteristics</td>
<td></td>
</tr>
<tr>
<td>Low initial cost as a solution</td>
<td>Nuisance trips create costly downtime</td>
</tr>
<tr>
<td></td>
<td>Failing safe may not always be safest state for running process</td>
</tr>
</tbody>
</table>

Probabilities

<table>
<thead>
<tr>
<th>Safe</th>
<th>Dangerous</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.04</td>
<td>0.02</td>
</tr>
</tbody>
</table>
## Dual System Architecture

### Probabilities

<table>
<thead>
<tr>
<th>Safe</th>
<th>Dangerous</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1oo1)</td>
<td>0.04</td>
</tr>
<tr>
<td>1oo2</td>
<td>0.08</td>
</tr>
<tr>
<td>Vote</td>
<td></td>
</tr>
<tr>
<td>2oo2</td>
<td>0.0016</td>
</tr>
<tr>
<td>Vote</td>
<td></td>
</tr>
</tbody>
</table>

### Benefits vs. Considerations

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1oo2 more ‘safe’</td>
<td>More nuisance trips than simplex systems</td>
</tr>
<tr>
<td>2oo2 fewer nuisance trips –more uptime?</td>
<td>Less safe than simplex systems</td>
</tr>
<tr>
<td>Can provide fault tolerance</td>
<td>Diagnostics more complex</td>
</tr>
<tr>
<td>1oo2’d’ provides better diagnostics and fault tolerance</td>
<td>Solution can be more complex</td>
</tr>
</tbody>
</table>
(TMR) Triple System Architecture

Probabilities

<table>
<thead>
<tr>
<th>Safe</th>
<th>Dangerous</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1001)</td>
<td>0.04</td>
</tr>
<tr>
<td>(1002)</td>
<td>0.08</td>
</tr>
<tr>
<td>(2002)</td>
<td>0.0016</td>
</tr>
<tr>
<td>2003 Vote</td>
<td>0.0048</td>
</tr>
</tbody>
</table>

Benefits

| Provides high availability and safe architecture |
| Can be complex to design |
| Can have multiple faults and still operate |
| Perceived more cost |
| Excellent fault tolerance |
| More hardware than other solutions |
| System size increases |
Key Points....

Key points to remember

• 1oo2, 2oo2, 1oo2d, 2oo3 all provide degrees of fault tolerance and should ultimately be transparent to the user/solution
• Process Safety systems can be fail-safe only
• Diagnostics and level of diagnostic coverage needs to be considered, rarely 100%
• SIL levels used to determine level of safety performance
Agenda

Rockwell Automation Process Safety
PlantPAx High Availability and Process Safety
Integrated Control and Safety System

PlantPAx
Process Automation System

Operator Interface
FactoryTalk View HMI Data Server

CIP Network (EtherNet/IP)

Process Control

SIS
PlantPAX Process Safety Today

Increasing Safety Integrity Level

Process Control

SIL 0
Process Control

SIL 1
Fail Safe

SIL 2
Fail Safe

SIL 2
Fault Tolerance

SIL 3
Fail Safe

SIL 3
Fault Tolerance

Process Safety

PlantPAx (Logix)

EtherNet/IP communication between AADvance™, Trusted™, and PlantPAx™

AADvance Scalable Safety

Trusted TMR

The most scalable process control and safety offering in the industry
Logix For Safety

Logix SIL 2

- SIL 2 Certified By
  - Safety AOIs
  - Peer-Peer Communications
  - I/O on EtherNet/IP
  - Up-to-date with Logix releases
  - Supports fail safe and fault tolerant configurations
Process Safety - GuardLogix

- Targeted for applications that do not require High Availability
  - Burner Management (BMS)
  - Thermoprocessing Equipment (Thermoforming)
  - Turbo Machinery

- Ideal for customers who prefer a single architecture

- Key Advantages/Features:
  - High performance
  - Supports PointGuard Discrete and Analog I/O
    - SIL2 inputs (single channel), SIL3 dual channel
    - Common Network for Safe & Standard Communications
  - Easiest to use safety environment in the market
    - Extensive suite of safety certified instructions
    - Supports safety Add-On instructions
  - Rated for Integrated standard and safety control
    - Diagnostics and control in standard tasks
    - Safety related functions in the safety task
Extensive 2oo3 (2 out of 3) voting
Extensive diagnostics and triplication provides high safety, fault-tolerance & high availability
High density 40 channel TMR IO modules
CIP connectivity to PlantPAx system
Supports 1000’s of IO with a single TMR processor
3-2-1 degradation modes supports high availability
Partial Stroke testing part of standard product offering
Rockwell Trusted TMR Technology

- Triple Modular Redundant (TMR) architecture
- Multiple True fault tolerance for minimum plant downtime (No limit on fault repair time)
- Comprehensive diagnostics and self test
- Open Communications (OPC, Modbus)
- Hot swap of modules, 1mS SOE
- Online firmware upgrade of all modules
- All five IEC 61131 languages
- Online software modification and Offline software simulation
- 5000 I/O per Controller,-High Density I/O (40 ch.)
- Companion or Smart Slot -Smallest Footprint
- Upload programs from controller
- Partial Stroke Valve Testing Module
- TUV, SIL3, IEC61508, ANSI/UL 508, NFPA 72,85,86
AADvance Scalable Safety

- Single, dual or triple configurations
- 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
- Simplex, 1oo2D or TMR processor and I/O architectures
Rockwell Automation Solutions: Sub-Sea Control and Safety

- **Rockwell Sub-Sea Technology**
  - Designed for Eurocard Rack Mount
  - Custom Module Centers, 3HP (0.6”) min
  - Hypertac Connector Technology
  - All connections are by custom wired harness or custom backplane
  - Validated against ISO13628-6 “Subsea Production Control Systems”
• Standards today are performance based and end users should determine levels of safety performance through risk review, analysis, HAZOP’s etc to determine appropriate SIF and SIL levels

• Process Safety products are a part of the process safety solution

• Process Safety solutions are one of the layers of protection in a process

• Process Safety products need to support deterministic failure modes

• Process Safety products need to support ability to be fault tolerant when needed

• Process Safety products need to minimize common cause failures

• Process Safety products are increasingly part of the control system and need to support well defined levels of integration without compromising safety
Thank You!

Rockwell Automation
Process Solutions User Group (PSUG)
November 14-15, 2011
Chicago, IL - McCormick Place West