



ANCHORAGE USERS GROUP, FEB 15, 16 2017

800xA SIL capable systems

Lifecycle Updates

Luis Duran, Global Product Manager Safety and Security Industrial Automation Control Technologies



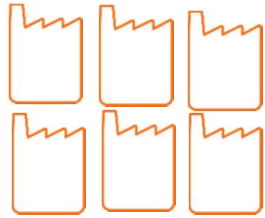
Agenda

ABB in Process Safety and Key Customers
SIL Capable Systems – Offering
Integrated Control and Safety: 800xA High Integrity
Independent High Integrity: Control Builder Safe
Burner Management Systems: Burner Library
High Integrity Overview: Differentiators and Benefits
Lifecycle Updates and Roadmap
Conclusions

ABB In Process Safety

Brief introduction

35+ years of experience in process safety systems



Over **4,000** System 800xA High Integrity
safety systems installed globally since **2005**



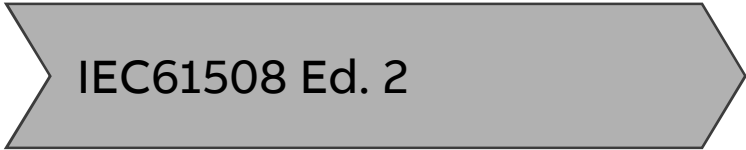
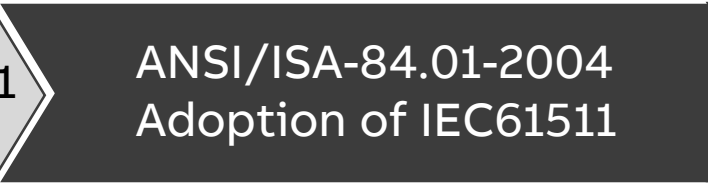
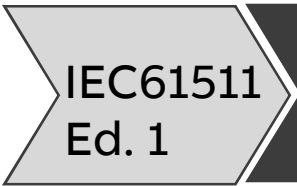
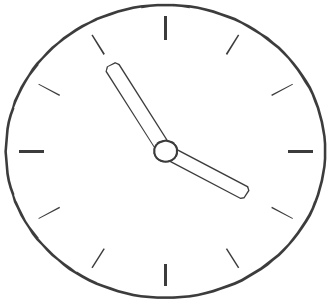
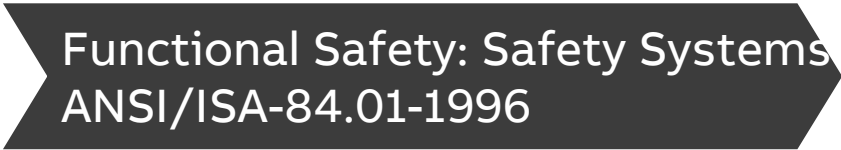
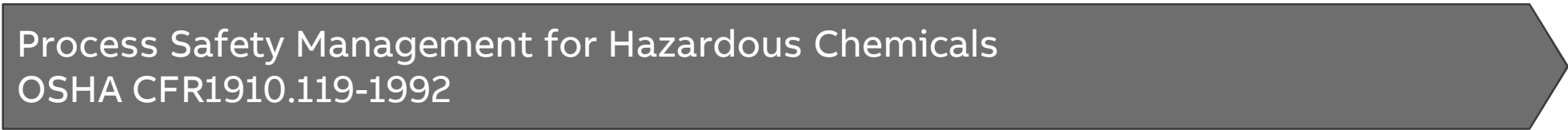
Installations in over 55 countries

26 Safety Execution Centers worldwide



Functional Safety

Evolution to Performance Based Standards



800xA High Integrity

References



SIL Capable Systems Offering



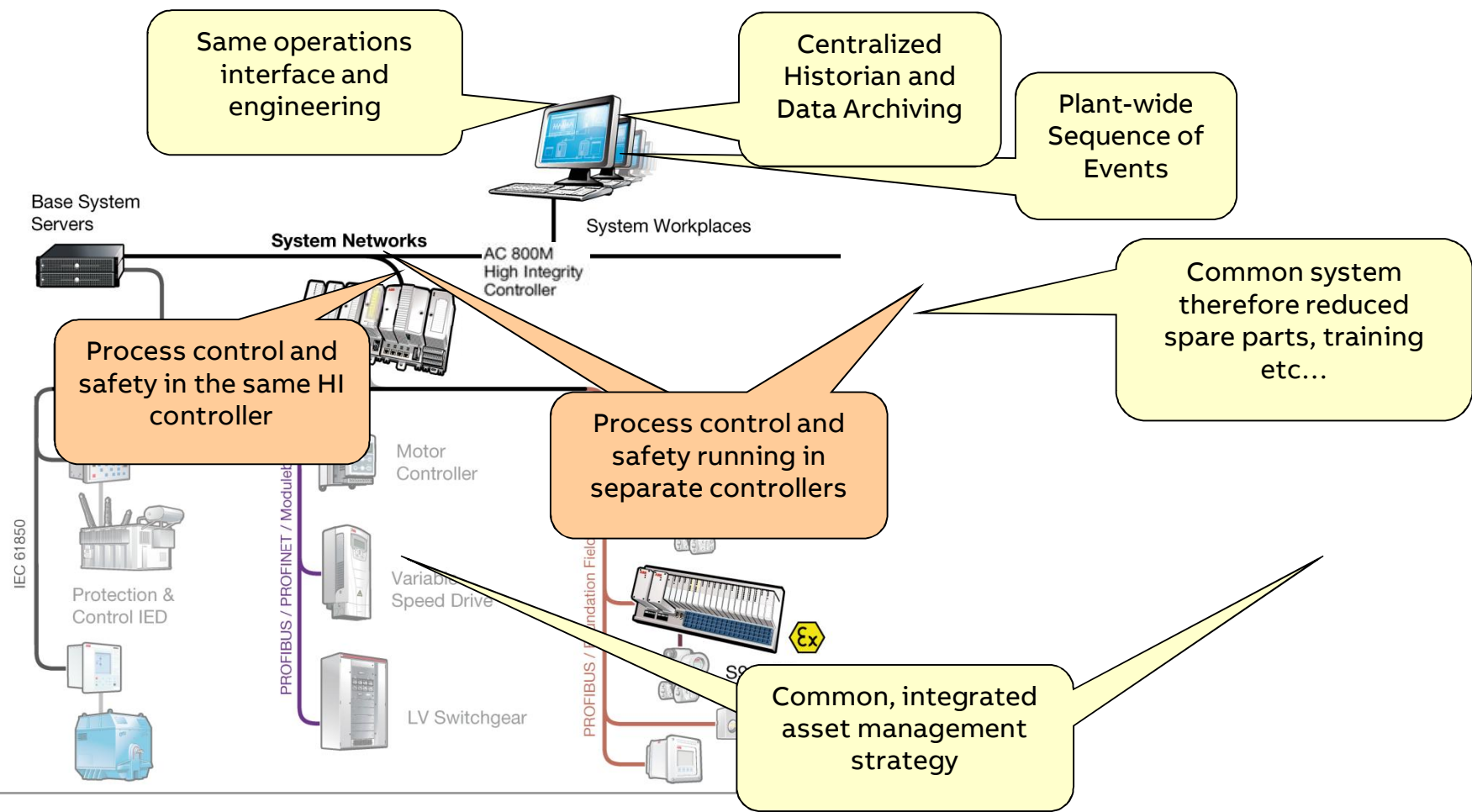
Integrated Control and Safety Systems



Functional Independence yet Integrated



Integrated Process Control and Safety



Operators can effectively react to abnormal events

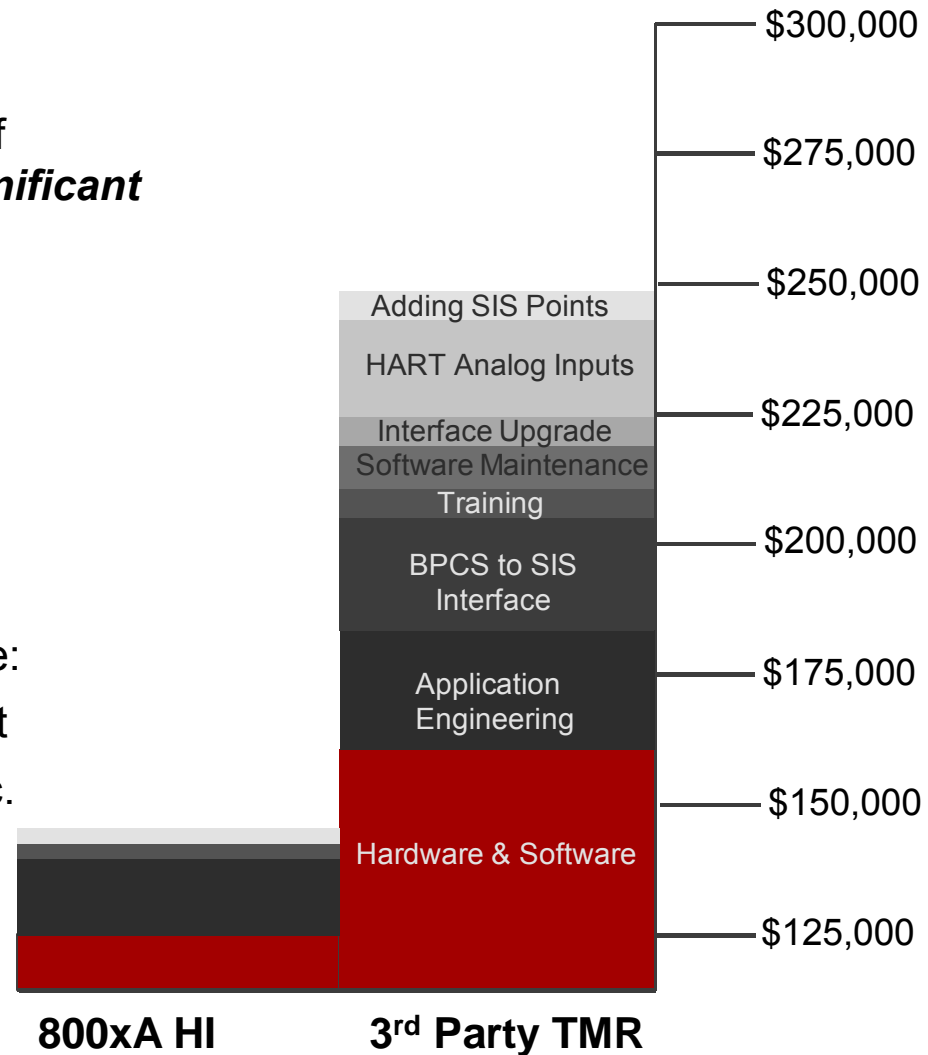


Lack of Integration increase project cost

The engineering effort and cost of interfacing a safety *could be significant*

...Over the system lifecycle

- Lifecycle costs add up
 - Extra hardware
 - Custom interface
 - HART analog inputs
- Additional “soft benefits” include:
 - Device / asset management
 - Common history, events etc.
 - Easier sensor validation



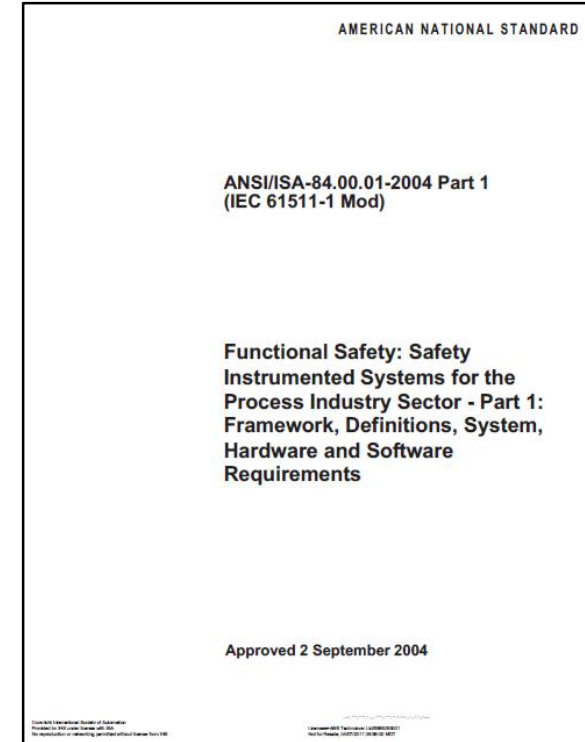
Independence and Functional Safety Standards

BPCS should be independent to the extent that the functional integrity of the SIS is not compromised.

Physical separation between BPCS and SIS may not be necessary

- independence is maintained,
- SIS operation is not be dangerously affected by:
 - Failures of the BPCS;
 - BPCS maintenance, operation or modification.

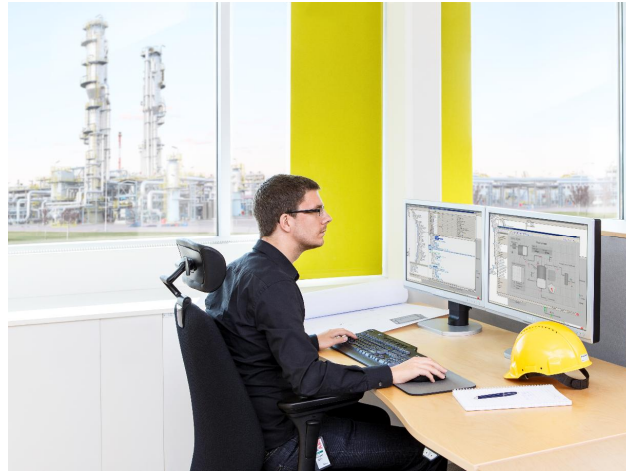
Need “effective” separation between BPCS & SIS.



- (1) IEC 61511-1 clause 11.2.4
- (2) ISA-84 .00.01-2004 Part 2 Clause 11.4.2

Integrated control and safety

Advantages



Potential common cause are analyzed and minimized during the design

Access control is a standard off-the shelf feature including write protection, bypassing and override mechanism

Integrated testing is performed during the design validation and verification test, including Network Security

Version control, compatibility and interoperability testing are all part of the release procedure

Independent High Integrity

Interfaced or Standalone Safety

- Independent High Integrity has the exact same certified components as the System 800xA High Integrity safety system
- Does not include functionality related specifically to process control (i.e. HMI or Operations)
- Control Builder Safe includes those items required for certified safe operations

Perfect solution for many industries:

Oil & Gas
Petrochemical
Chemical
Pulp & Paper
Power

Great for industrial applications:

Emergency Shutdown
Relay Interlock
Remote Terminal Units
Burner Management
High Integrity Pressure Protection



Independent High Integrity

Overview

Hardware

- TÜV certified SIL 3 controller (PM865/SM811)
- 24 VDC DC I/O and 4-20 ma Analog inputs

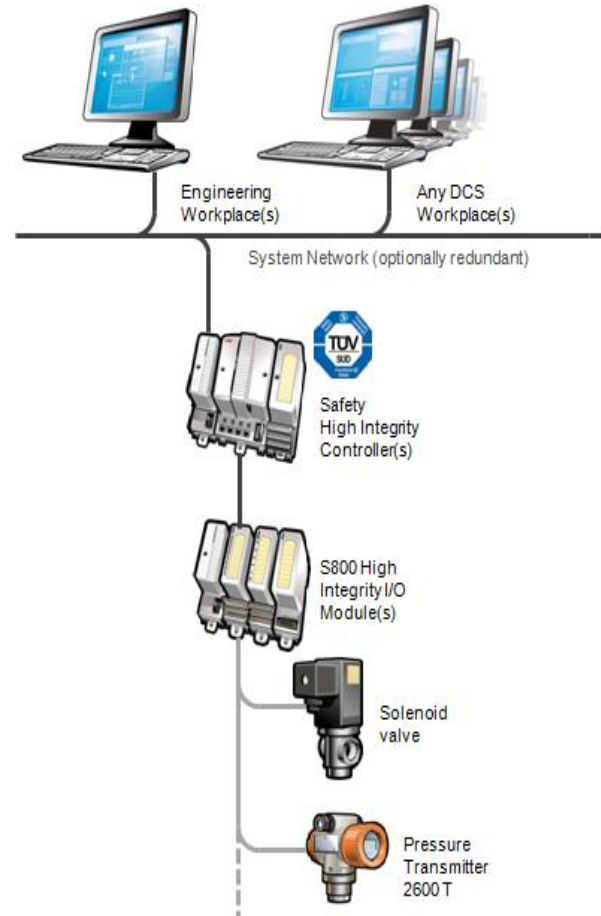
Control Builder Safe

- Engineering
- IEC1131 languages
- Access control and override control

Connectivity and Interfacing

- ABB Control systems
- 3rd party software and control systems

Diagnostics



Small Independent HI system with engineering and DCS

Burner Management System

BurnerLib

AC800M High Integrity Burner Management Library (BurnerLib) is fully integrated.

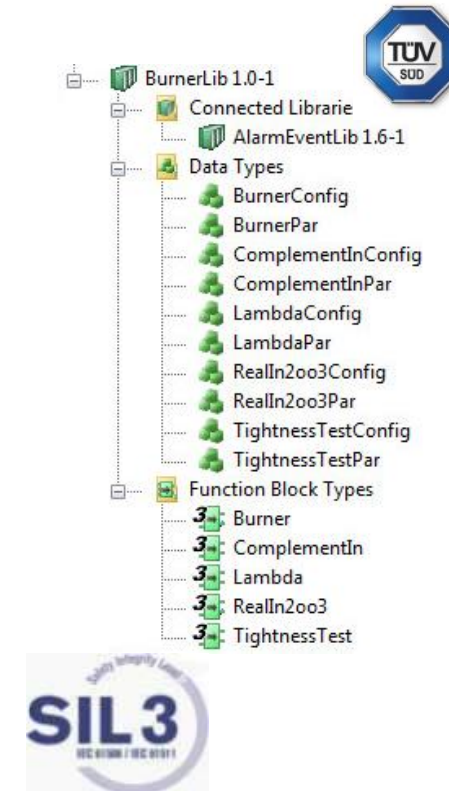
Contains five SIL 3 classified function block types to implement complete Burner Management applications.

- Includes complete control over startup and operation.

Has built in Alarm Handling, Faceplates and Display Elements.

Satisfies most relevant standards.

Allows complete visualization of the process
(No more “black box”).



800xA High Integrity Certification

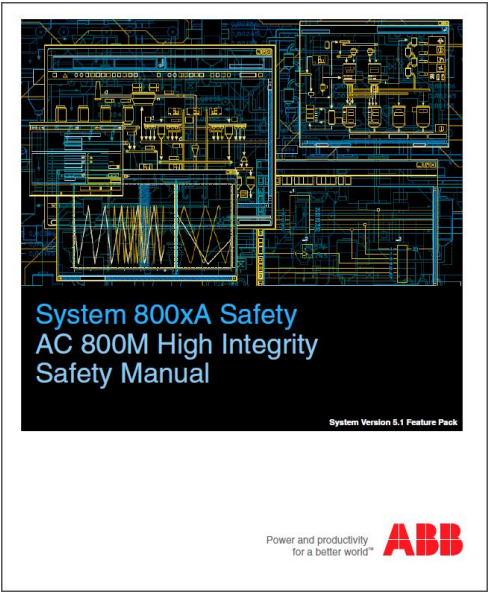
TÜV Certificates



Product Safety
Certificate



Development Department
Safety Certificate



Safety Manual

TÜV Product Service certified all product components in the High Integrity offering

800xA High Integrity Certification

Certified to Functional Safety Standards



Fully certified to IEC 61508, a generic standard providing guidance in the design of safety system products

In compliance with IEC 61511, a process industry specific standard providing guidance in the design of safety system projects

These standards specify procedures and routines for all activities required to manage safety throughout the entire lifecycle of the system

- Planning, design, implementation, documentation, training, operation and maintenance

Certificates

800xA High Integrity – Meets Industry Standards

Laws and Directives

| | |
|--------------------------|--|
| 2014/35/EU | Low Voltage Directive |
| 2014/30/EU | EMC Directive |
| 93/68/EC and amendments | CE marking Directive |
| 2006/42/EC | Safety of Machinery Directive ⁽¹⁾ |
| 94/9/EC – ATEX directive | Electrical and mechanical equipment and protective systems, which may be used in potentially explosive atmospheres |

(1) To fulfill the Safety of Machinery Directive, you need to make sure that the *System 800xA, Operations Basic Operations*, 2PAA111131* and *System 800xA, Operator Manual, Warnings*, 2PAA110888* are translated into the local official community language.

Please refer to Safety Manual 3BNP004865-601 for further information

Certificates

800xA High Integrity – Meets Industry Standards

General Safety Standards

| | | |
|----------------|------|--|
| IEC 61508 Ed2 | 2010 | Functional safety of electrical/electronic/programmable electronic safety-related systems |
| EN ISO 13849-1 | 2008 | Safety of machinery - Safety-related parts of control systems Part 1: General principles for design |
| EN ISO 13849-2 | 2008 | Safety of machinery - Safety-related parts of control systems Part 1: Validation |

Please refer to Safety Manual 3BNP004865-601 for further information

Certificates

800xA High Integrity – Meets Industry Standards

Additional Approvals for Safety Compliance

| | | |
|--------------------------------------|------|--|
| UL 508 | 2010 | Industrial Control Equipment |
| UL 1998 | 2010 | Standard for Software in Programmable Components |
| FM 7605 ⁽¹⁾ | 1999 | Programmable Logic Control based Burner Management Systems |
| CSA 22.2.NO.142-M1987 ⁽²⁾ | 2000 | Process Control Equipment |
| EN 50178 | 1997 | Electronic equipment for use in power installations |

(1) Only a selected number of AC 800M HI boards are certified according to FM7605
(2) The AC 800M HI is designed in accordance with this standard. The standard is not included in the certification.

Please refer to Safety Manual 3BNP004865-601 for further information

Certificates

800xA High Integrity – Meets Industry Standards

Application Standards (to the extent applicable)

| | | |
|---------------------------------------|------|---|
| IEC 61511 | 2003 | Functional safety - Safety Instrumented Systems for the process industry sector |
| ISA S84.01 | 2004 | Application of safety instrumented systems for the process industries |
| ISO 10418 (API RP 14c) ⁽¹⁾ | 1993 | Petroleum and natural gas industries – offshore production platforms – Analysis, design, installation and testing of basic surface safety systems |
| EN 50156-1 | 2004 | Electrical equipment for furnaces |
| EN 298 Ch 8,9,10 | 2003 | Automatic gas burner control systems for gas burners and gas burning appliances with or without fans |
| EN 54-2 and -4 | 1997 | Fire detection and fire alarm systems |
| NFPA 72 | 2007 | National Fire Alarm Code |
| NFPA 79 | 2007 | Electrical Standard for Industrial Machinery |
| NFPA 85 Ch 4.6.3 | 2007 | Boiler and Combustion Systems Hazards Code (compilation of 8501 – 8506) |
| prENV 1954 ⁽¹⁾ | 1995 | Internal and external fault behavior of safety-related electronic parts of gas appliances |

(1) The AC 800M HI is designed in accordance with this standard. The standard is not included in the certification.

Please refer to Safety Manual 3BNP004865-601 for further information

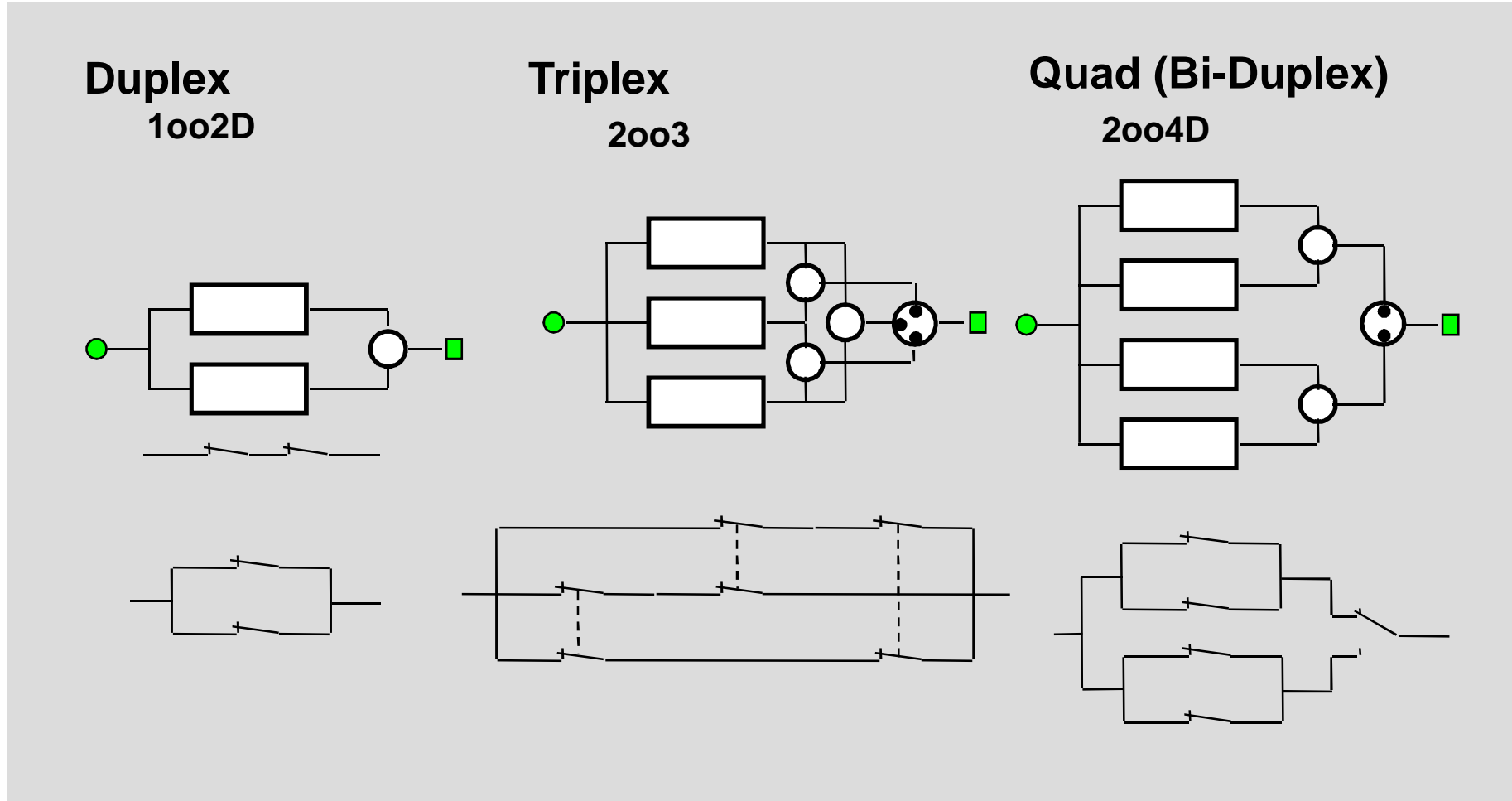
Why customers benefit from High Integrity?

| | |
|---------------------------|--|
| Use of Diverse Technology | Provides better protection against Common Cause Failures, leading to reduced PFD |
| Systematic Capabilities | Features as Difference Report, Compiler Restrictions, Access Control and Safe Online Write helps prevent systematic errors in programming the system |
| Live Code Evaluation | Difference Report and Load Evaluate Go (LEG) are unique to High Integrity |
| Tight integration | Integration to 800xA is the best SIS – BPCS integration in the market |
| Safe Online Write | Standard-off-the-shelf SOW allows for cost-effective, secure, pre-tested and certified approach to writing and bypassing the SIF and reduce the chances of systematic errors |

Benefit: Flexible and Cost effective solutions

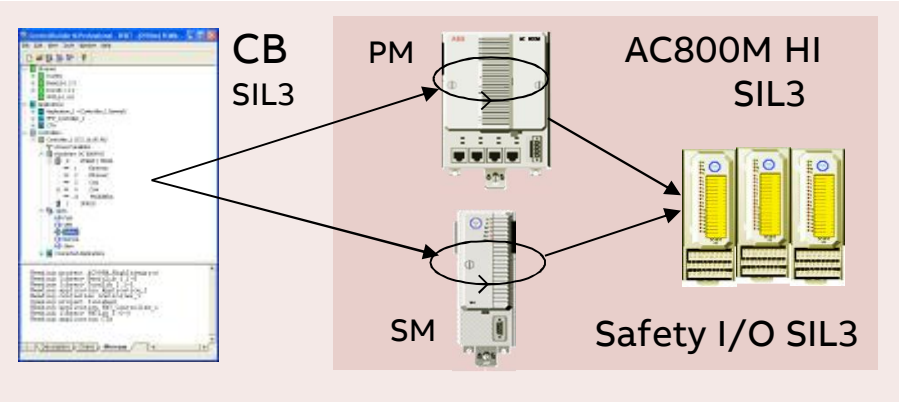
| | |
|--|---|
| Use of Diverse Technology | SIL 3 without redundancy Smaller footprint Flexible configuration |
| Systematic Capabilities | Reduce human error Ensure compliance to Safety Manual |
| Live Code Evaluation | Simplifies application troubleshooting Simplifies Management of Change and Audit Trail |
| Tight integration Safe Online Write | Eliminate extensive programming and testing |

1st Generation Logic Solver Architectures



800xA High Integrity

Diverse Architecture, Diverse Implementation



| | HFT | |
|---------|-------|-------|
| SFF (%) | 0 | 1 |
| < 60 | - | SIL 1 |
| 60 – 90 | SIL 1 | SIL2 |
| 90 – 99 | SIL2 | SIL 3 |
| > 99 | SIL 3 | SIL 4 |
| | | |

IEC61508-2 Table 3

The SIL 3 High Integrity controller has parallel processing paths based on diverse technology

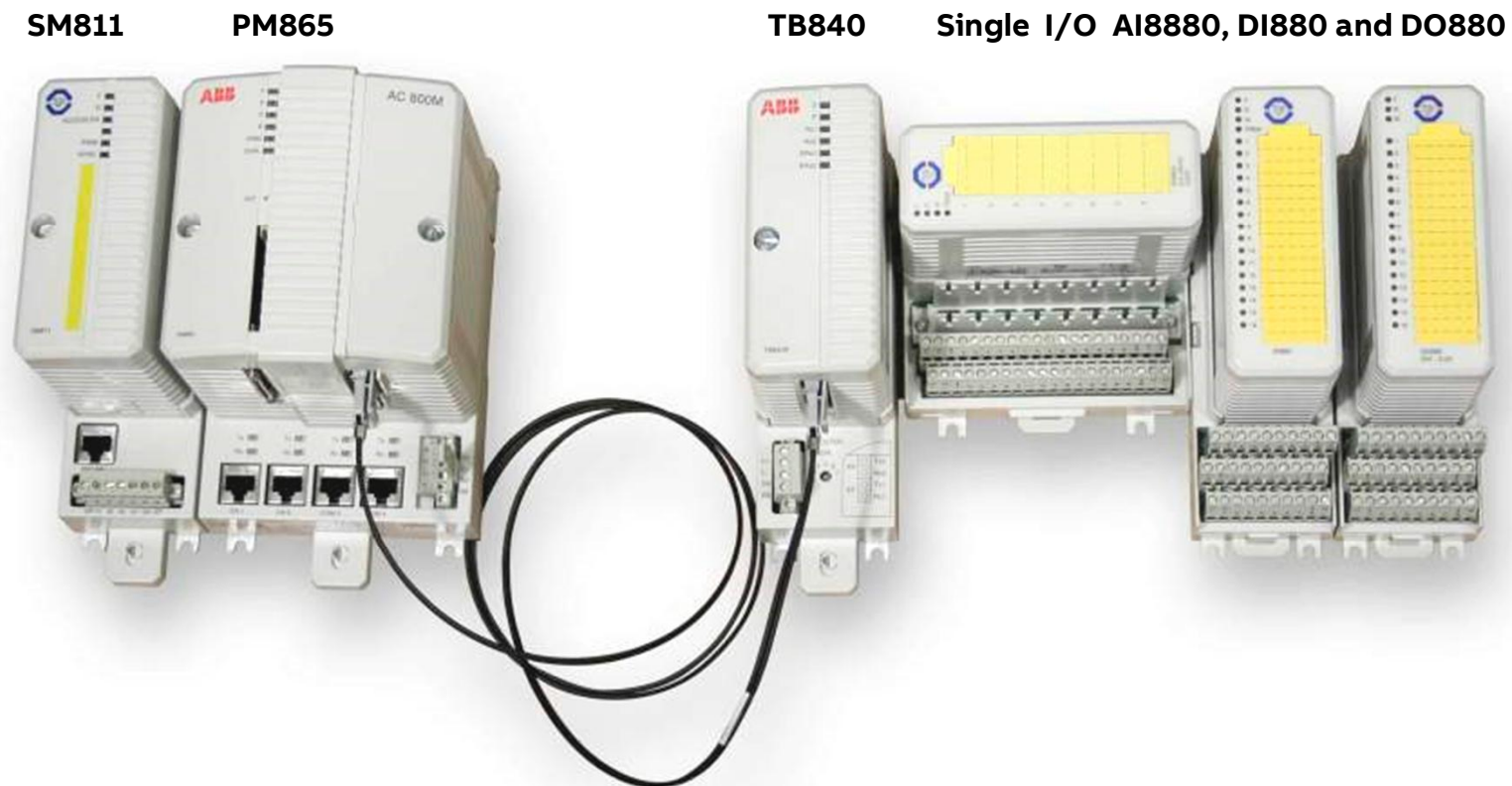
Integrity voting between paths compliments the built in active diagnostics

Controller (PM) and Safety Module (SM) developed by diverse (different and independent) teams and tested by a third team by people with different backgrounds in different locations

The two channel architecture meets SIL3 requirements for hardware fault detection and reaction

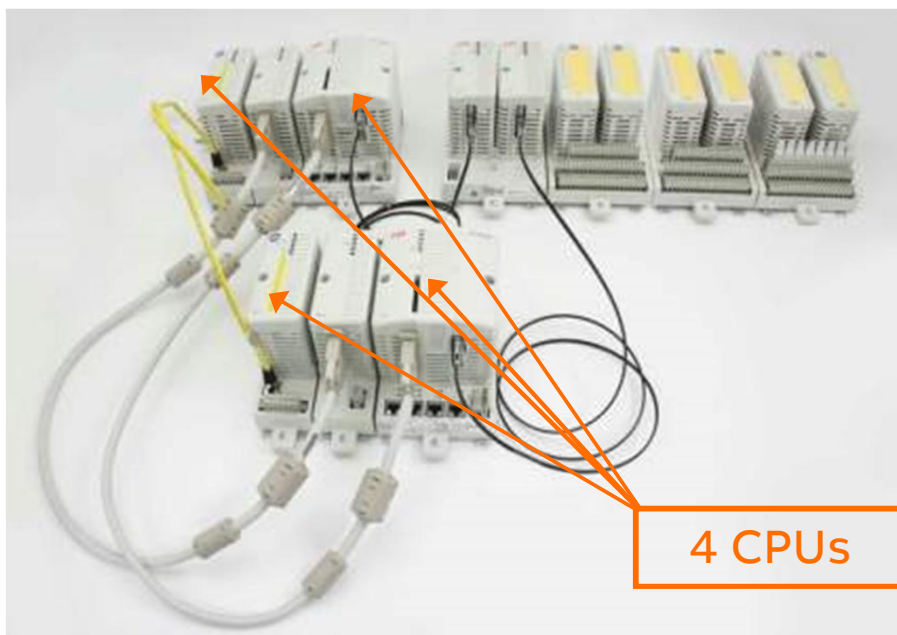
800xA High Integrity

Diverse Architecture: SIL 3 without Redundancy



800xA High Integrity

Diverse Architecture: Redundancy for Availability



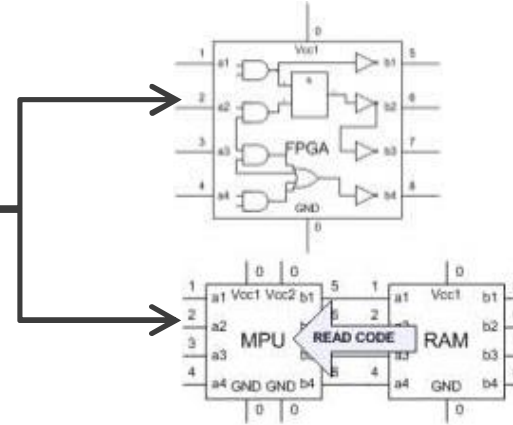
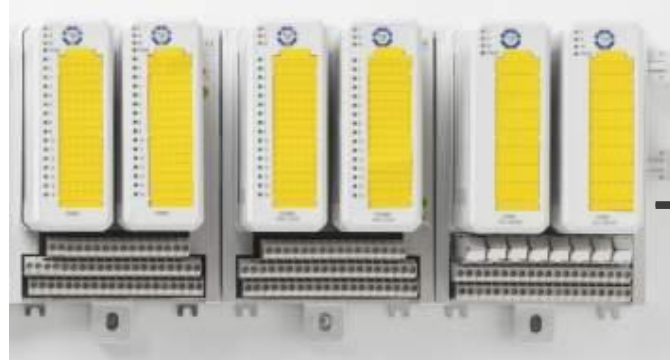
AC800M High Integrity offers availability figures comparable to or better than typical TMR systems

- Availability up to 99.9999%

Redundancy and switch-over to stand-by unit allow continuous operation without time restriction upon failure of one of the redundant modules

800xA High Integrity

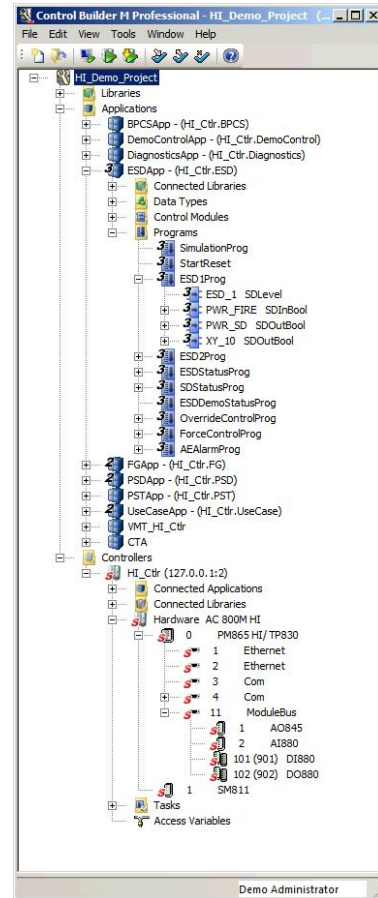
S880 I/O Functionality



- Single and Redundant configuration
- Hot Insertion and Hot Swap in redundant configuration
- G3 Coating
- EX certified – Zone 2, Class 1 according to US standard
- Embedded Diversity
 - Two diverse execution paths based on different hardware technology
 - Both MCU and FPGA
 - Each individual single IO module has an internal 1oo2 architecture

Engineering

Application Development Environment



The engineering tool, the Control Builder M, will automatically limit user configuration choices to ensure integrity

Safety functions protect and control download to the process and runtime environment

- Download is prevented unless all SIL requirements are met

Embedded firewall mechanisms include

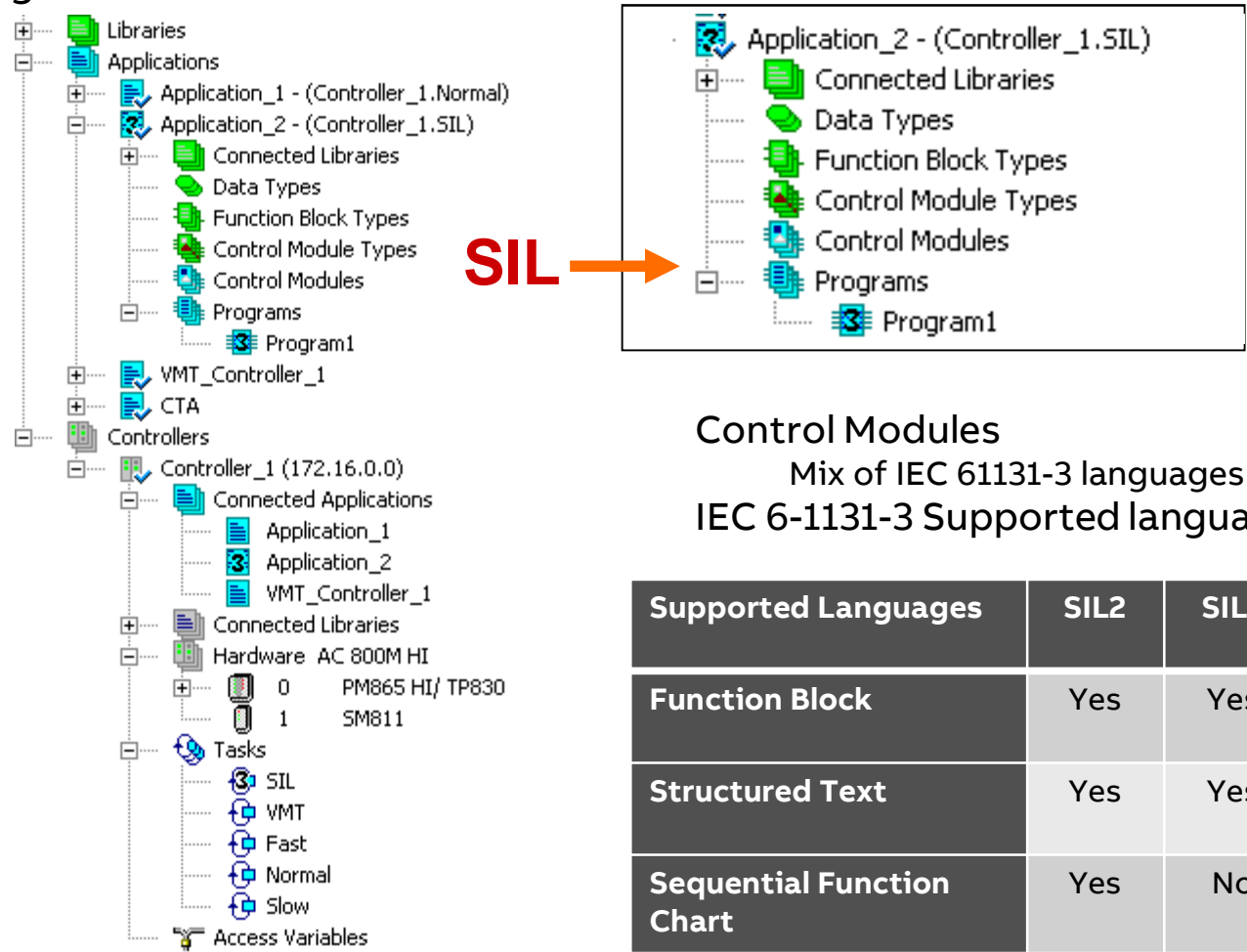
- CRC protection on different levels

- Double code generation with comparison

- Compiler with revalidation

Engineering:

IEC 6-1131-3 Supported languages



Engineering

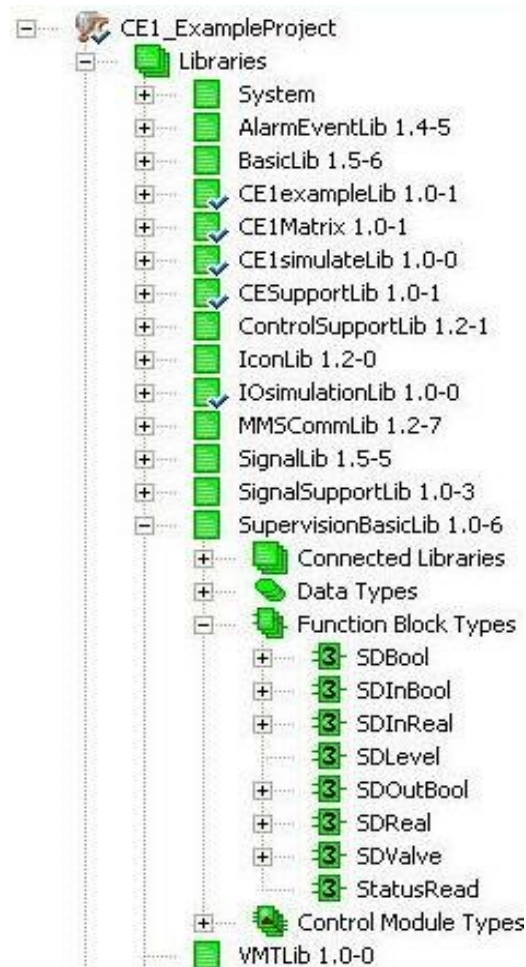
Safety Application Libraries



SIL3 Mark



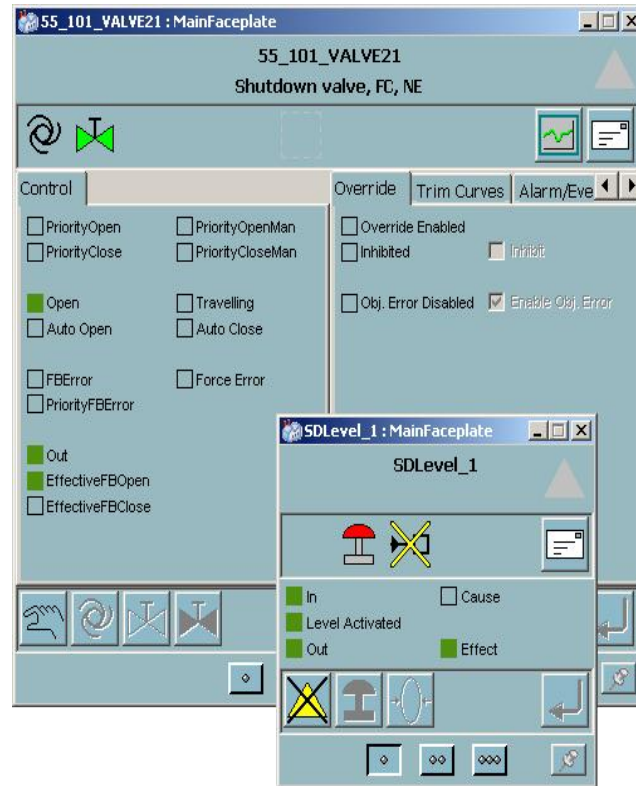
SIL 2 Mark



System
BasicLib
MMSCCommLib
AlarmEventLib
ProcessObjLib
SupervisionLib
SupervisionBasicLib
FireGasLib
SignalLib

Engineering

SIL Certified Libraries



Support for IEC61131-3 Functions and FB types

New SIL3 FB Types

Input/Output handling
(Boolean, Real)

Support for Shutdown applications (ESD, PSD)

Valve

Shutdown level

MMS Control Modules for Safe peer-to-peer communication

MMSDefHI and MMSReadHI

Data type check added in both

Engineering

Re-Use Instead Of Re-Inventing

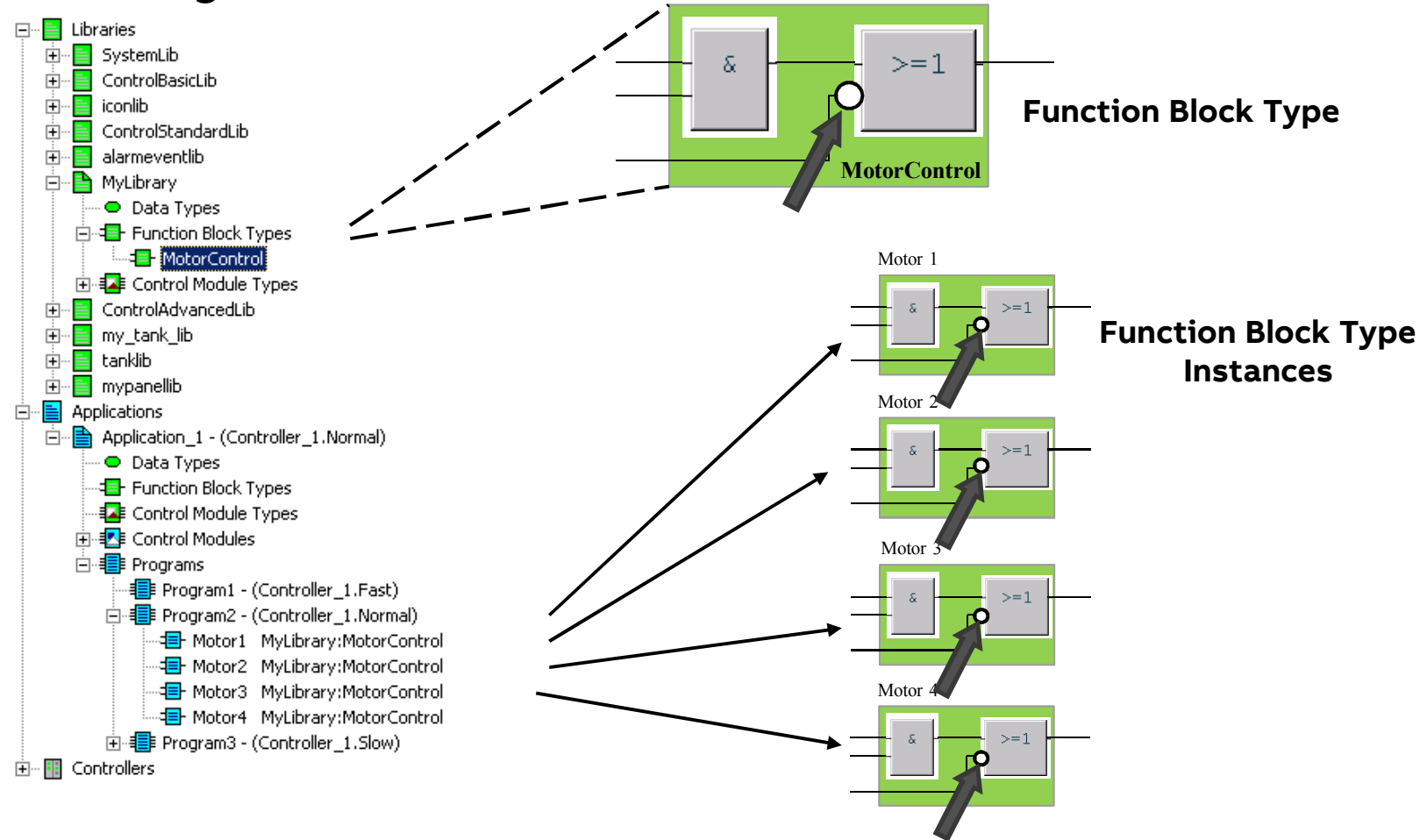
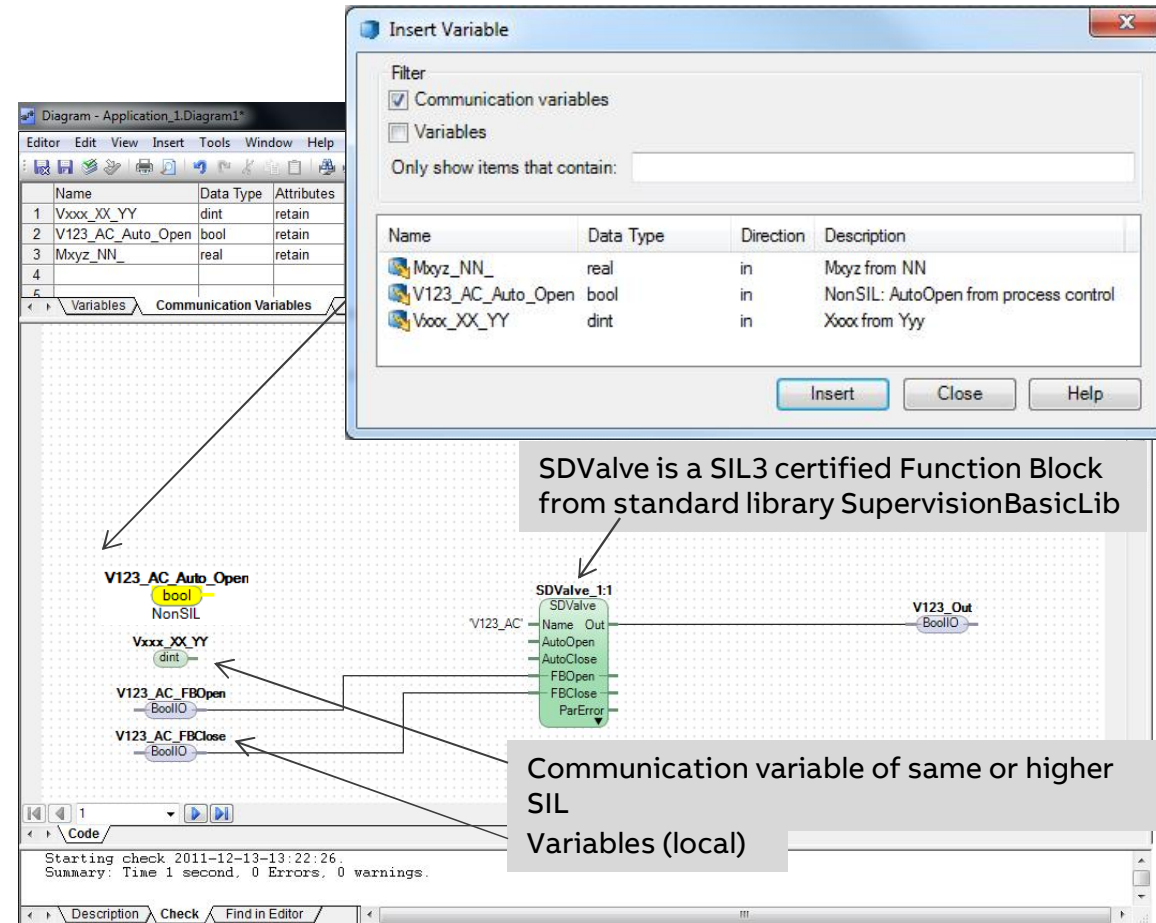


Diagram Editor for SIL Applications

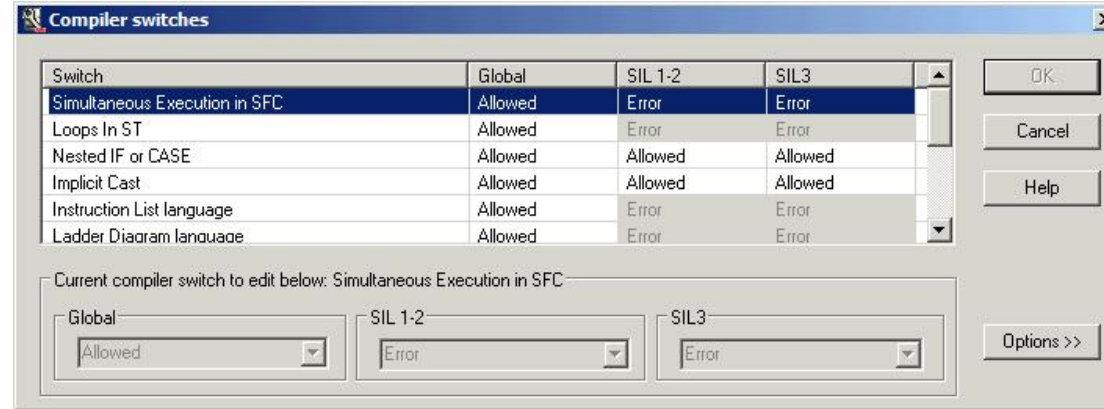
- TÜV certified engineering environment for safety applications
- Easy SIF configuration
- Supports Low to High SIL Communications
- A "Lower SIL" communication variable is indicated by different color and "Expected SIL".

V123_AC_Auto_Open
bool
NonSIL



Engineering

Compiler Restrictions



The compiler warns and / or prevents the engineer from designing dangerous code

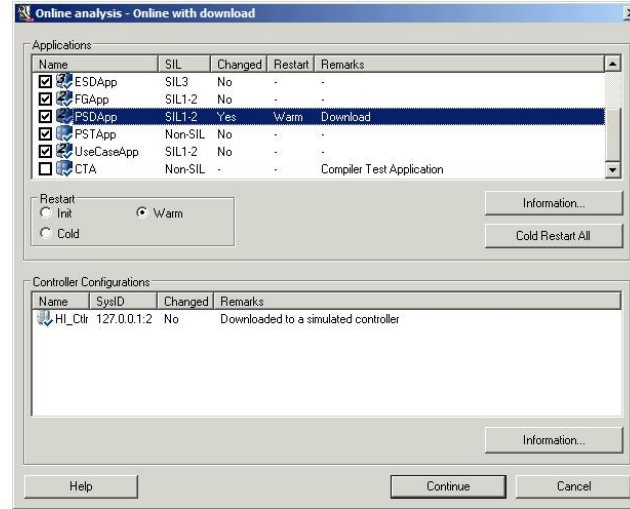
- For example complex code structures, loops etc

The compiler checks that all restrictions and rules necessary to achieve the intended SIL of the application are adhered to

An error is reported when a rule is violated and the attempted download to the controller is blocked

Engineering

On-line changes



Online changes can be downloaded to the controller without interfering with the running process

FB/CM parameters (e.g. trip limit)

Hardware settings (e.g. ISP value)

Logic

Downloads are protected by the

“Access enable” function

Re-authentication can be configured to

ensure that the user is authorized

This is also recorded in the audit trail

Engineering

Difference Report

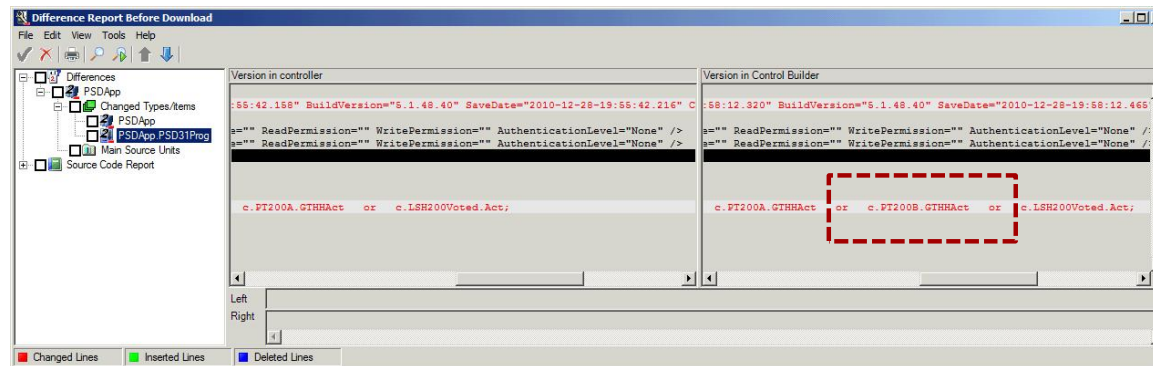
Reports the differences between the project running in the controller and the project in the Control Builder M

Presented before download to the controller

Changes may be rejected (in which case the download is cancelled)

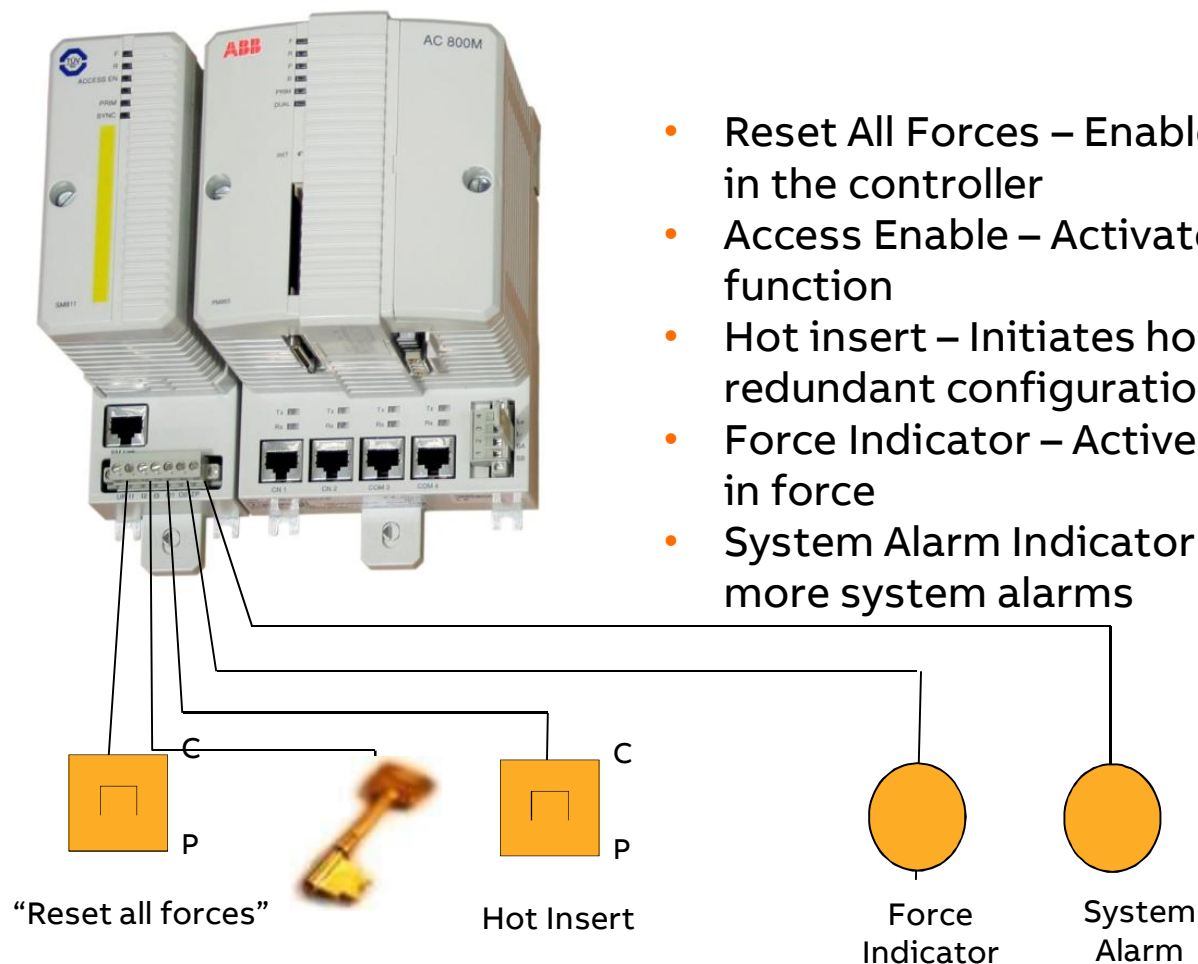
Each difference report is saved and stored automatically and can be reviewed at any time

This, together with audit trail functionality and more, provides a well documented and traceable history



Security

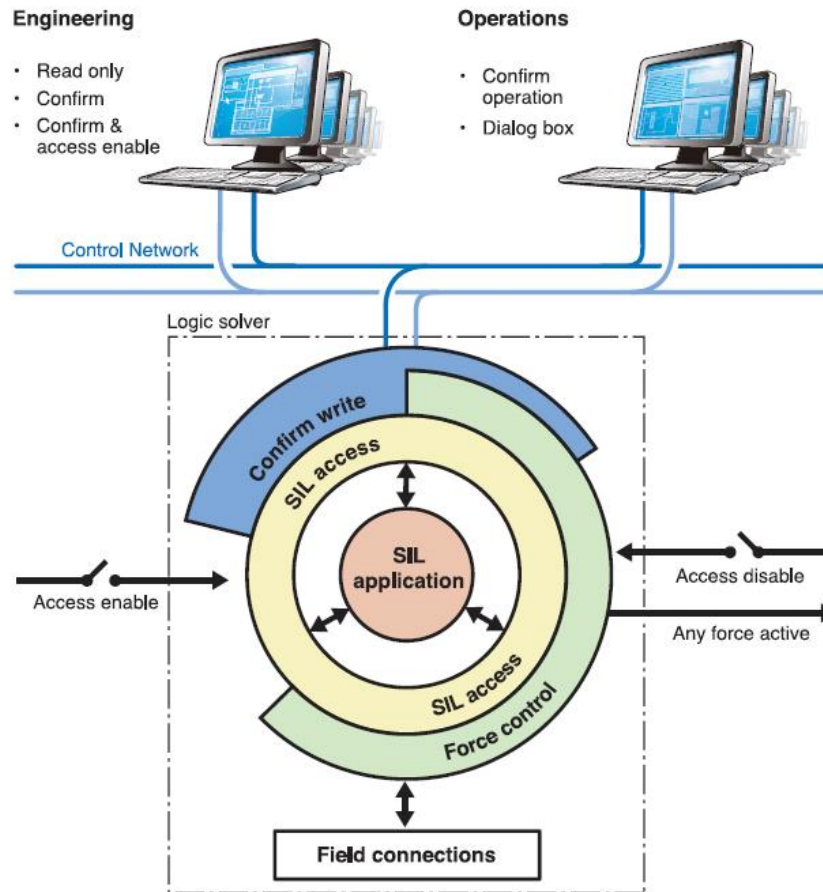
Safety Module Security



- Reset All Forces – Enable a quick reset of all forces in the controller
- Access Enable – Activates the access enable function
- Hot insert – Initiates hot insertion of SM811 (in redundant configuration)
- Force Indicator – Active if one or more signals are in force
- System Alarm Indicator – Active if there are one or more system alarms

Security

System Security And Embedded Firewalls



Provides functions for protection of SIL classified applications in AC800M HI Controllers

- SIL Access Control and Authorization
- Force Control / Override Control / Bypass Management
- Confirmed Online Write / Confirmed Operation

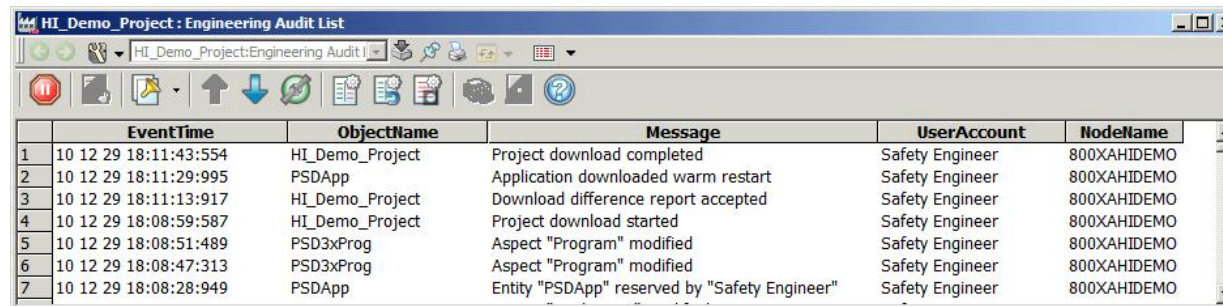
Embedded firewalls and confirmation procedures protect the SIL application from inadvertent / accidental control actions

Security: Audit Trail

- Enables audit of all operator and engineering actions
- Audit actions examples
 - Configuration changed
 - Signal forced
 - Download
 - Reserved/Released

Audit log contains:

- Date and time for the operation
- Node from which the operation was performed
- User name of those performing the operation
- Type of operation
- Object, property or aspect affected by the operation



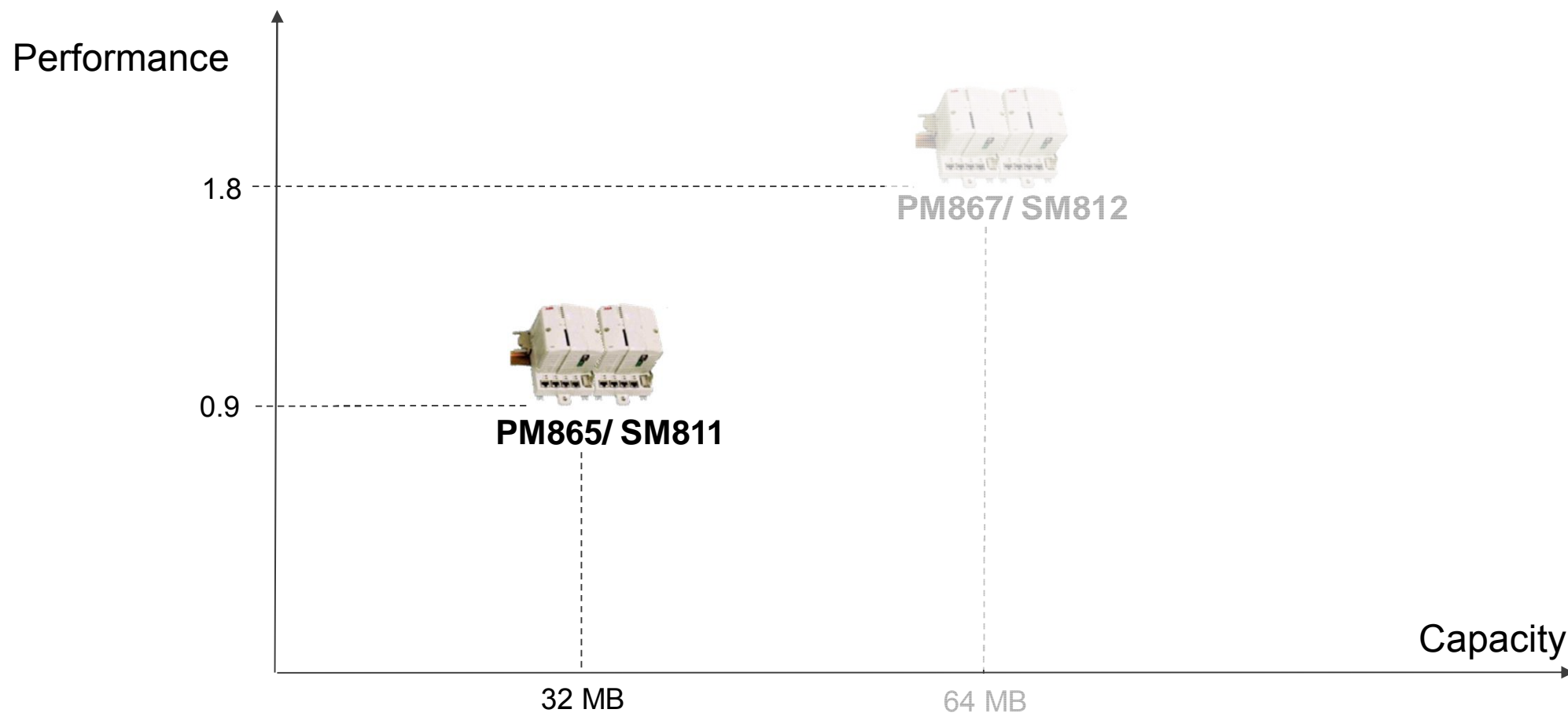
| | EventTime | ObjectName | Message | UserAccount | NodeName |
|---|-----------------------|-----------------|---|-----------------|-------------|
| 1 | 10 12 29 18:11:43:554 | HI_Demo_Project | Project download completed | Safety Engineer | 800XAHIDEMO |
| 2 | 10 12 29 18:11:29:995 | PSDApp | Application downloaded warm restart | Safety Engineer | 800XAHIDEMO |
| 3 | 10 12 29 18:11:13:917 | HI_Demo_Project | Download difference report accepted | Safety Engineer | 800XAHIDEMO |
| 4 | 10 12 29 18:08:59:587 | HI_Demo_Project | Project download started | Safety Engineer | 800XAHIDEMO |
| 5 | 10 12 29 18:08:51:489 | PSD3xProg | Aspect "Program" modified | Safety Engineer | 800XAHIDEMO |
| 6 | 10 12 29 18:08:47:313 | PSD3xProg | Aspect "Program" modified | Safety Engineer | 800XAHIDEMO |
| 7 | 10 12 29 18:08:28:949 | PSDApp | Entity "PSDApp" reserved by "Safety Engineer" | Safety Engineer | 800XAHIDEMO |



Lifecycle Updates

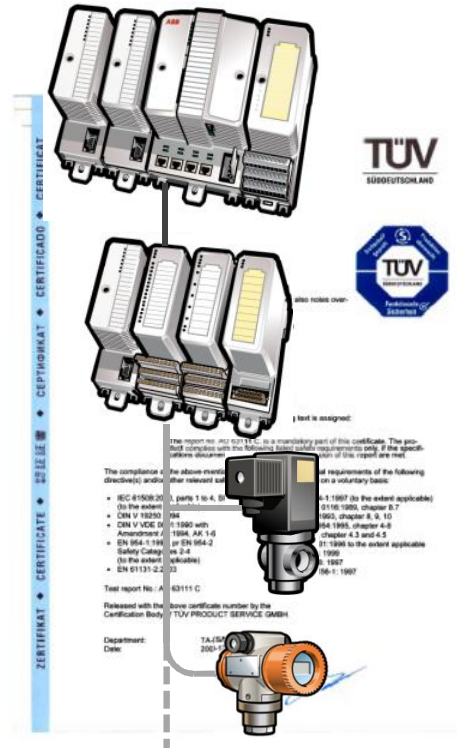
AC 800M High Integrity

Product Offering



New Safety controller

PM867/SM812 – More power for critical applications



- Expected to handle full Module bus capacity (around 450 I/O)
- Fast response times (faster than 250ms)
- About 2x more powerful than PM865/SM811
- Double memory compared to PM865 (64Mb)
- Enables future technologies
- PM867/SM812: more power, same size

New Safety controller

PM867/SM812: a new family member



PM867/SM812 is a new member to the family of controllers

PM865/SM811 is still Active and available

Supported on 800xA 6.0.2 and forward

SIL 3 Capable and Certified (TUV SUD)



Other Safety related features



Burner Management Library

- Now available in v6.0.2
- Reduces engineering effort through powerful building blocks
- Includes complete control over startup and operation.

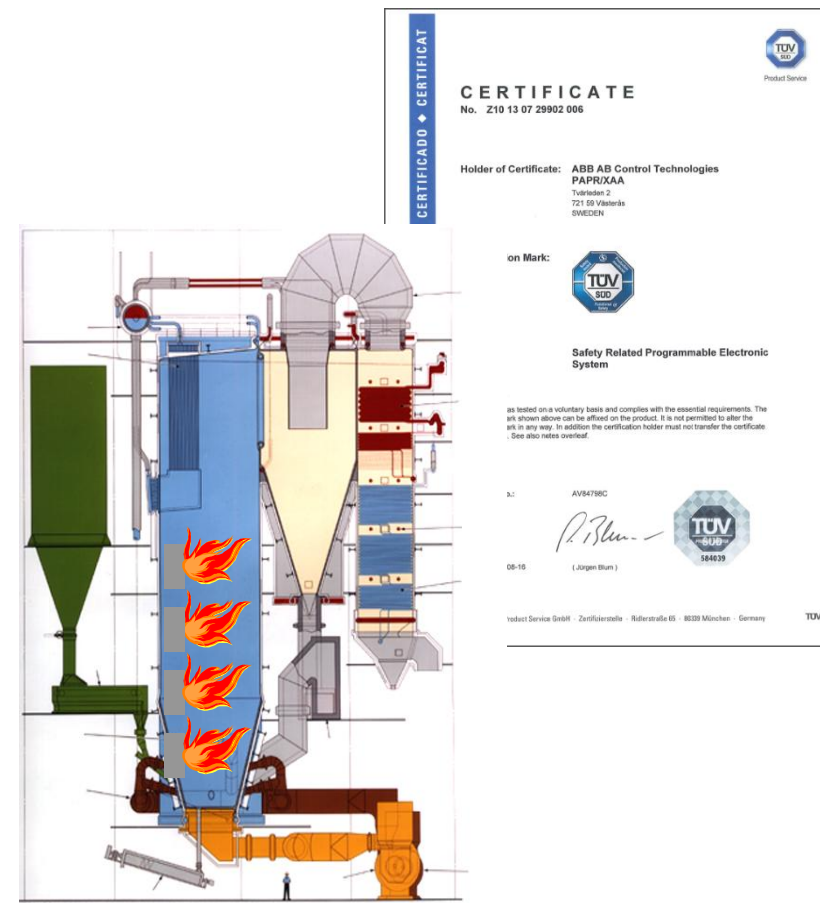
Difference report viewer updated

- Updated with offline support for viewing reports

System Diagnostics update

- NonSIL System Diagnostics no longer requires a combined High Integrity and Process Control license.

Improved failover for redundant controllers



Control Builder Safe 2.0

Stand Alone Safety

Safety – Reduced Footprint and Enhanced Capacity

– PM867 & SM812 (~1.5-2x capacity) - Single & Redundant



Life Cycle Management

– Windows 10 Workstation Support (Windows 10 Enterprise



Changes to Burner Management Library

Version 1.1-2 (with 800xA 6.0.2, release April 2016)

Some parameters in Burner object lose their current value at warm download. The out parameters of the object did not have the attribute Retain set. (#58223)

Erroneous Order to Open PilotValve is Set during Application Reconfiguration. If BurnerLib burner is Active an Erroneous Order to Open PilotValve was Set during Application Reconfiguration. 800xA CON-CN-5112-001 (#56144)

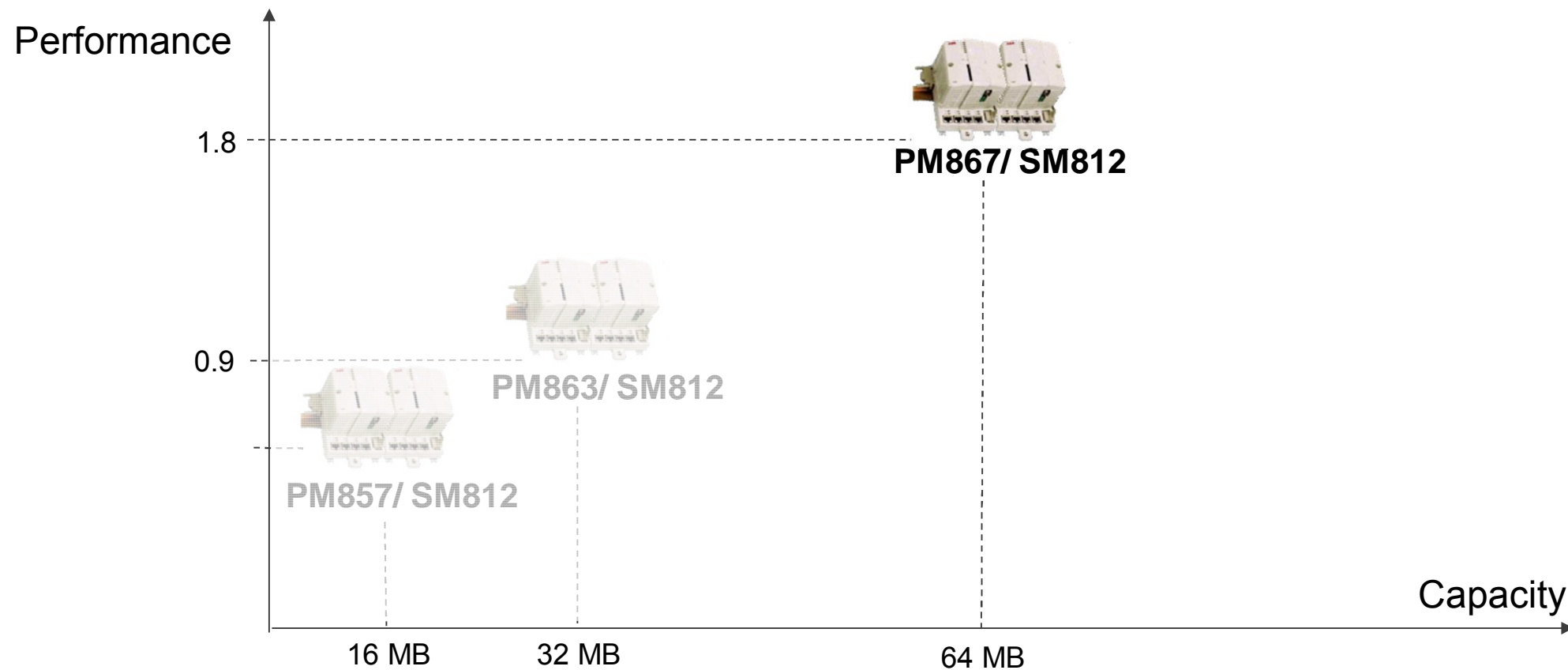
Realln2oo3 does not show the Error alarm if Fault1oo3 alarm has been set before. (#55688)

New indication in FB Tightness Test. (#55749)

Improved alarm messages in Realln2oo3. (#56281)

AC 800M High Integrity

Product Offering



Conclusions

ABB has relevant and proven experience in Functional Safety for Process applications

Top player worldwide and in key industries with over 4000 installations worldwide

Integrated to 800xA, Independent or Interfaced to S+ or other DCS, HMI or SCADA

Diverse Redundancy and Logical Separation are ways to avoid Common Cause Failures and maintain Independent Protection Layers

Product functionality enables cost effective and flexible solutions

Follows design practices as described on the IEC/ISA Safety Lifecycle to built robustness to the integration and achieve Independent Protection Layers

Security and Access Control are crucial for the successful implementation of the integration

Reduce engineering effort and ensures compliance to relevant Safety and Application standards



ABB



ANCHORAGE USERS GROUP, FEB 15, 16 2017

800xA SIL capable systems

Fire & Gas Applications Update

Luis Duran, Global Product Manager Safety and Security Industrial Automation Control Technologies



Independent Protection Layers

Is a Fire & Gas System a Layer of Protection?



Fire and Gas Systems (FGS)

Subset of industrial automation and control systems

Employed in the process industries for the purpose of:

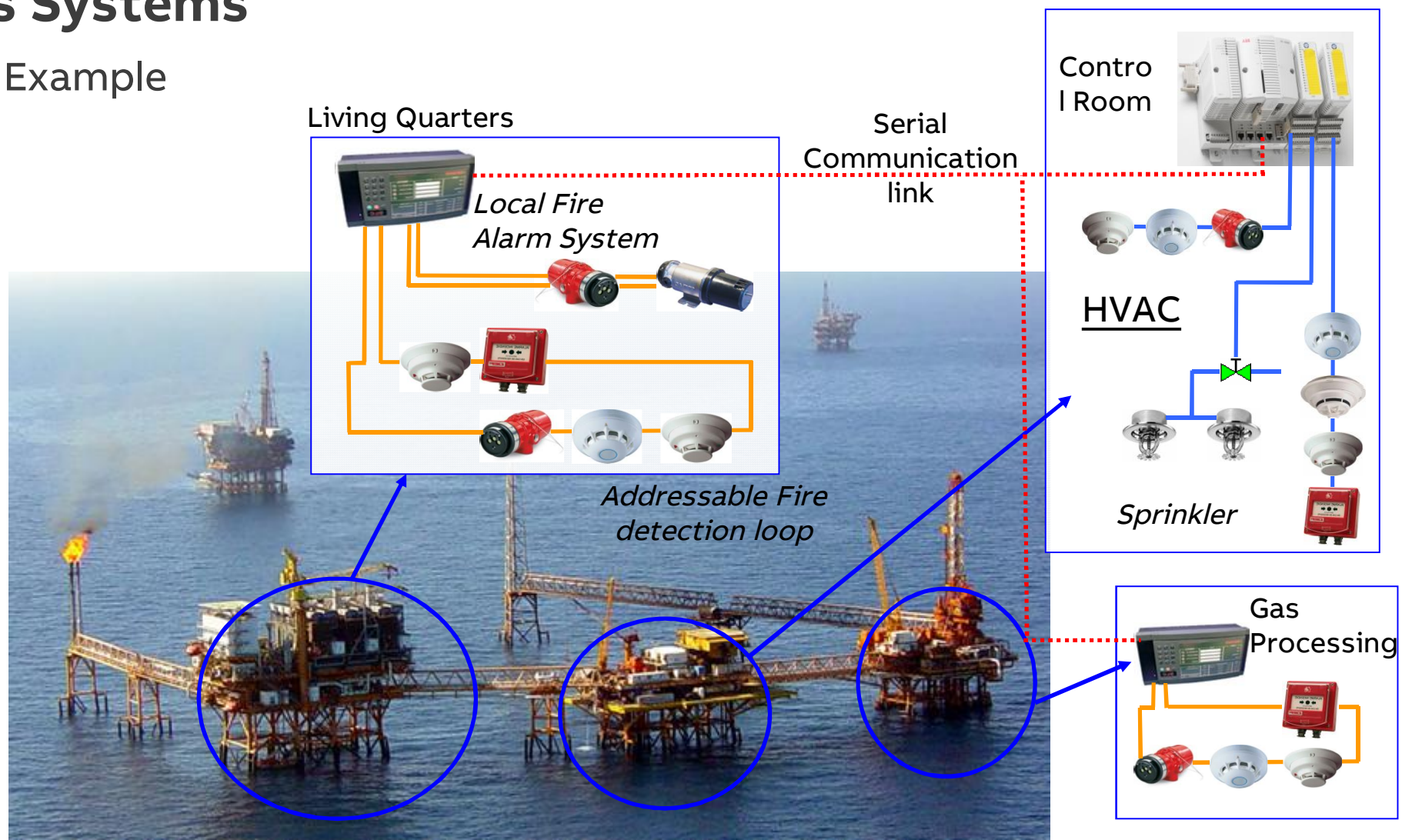
- Detecting loss of containment of hazardous materials
- And initiating response to mitigate the impact

Typically the design intent is not to prevent a hazardous condition

But rather to reduce (or mitigate) the consequences to a lower level

Fire & Gas Systems

F&G System Example



NFPA 72

Scope and Certification

NFPA extends beyond the control unit and covers:

- Application, installation, performance, inspection, testing and maintenance of fire alarm systems, supervising systems public emergency alarm reporting system, fire warning equipment and emergency communication systems and their components

Automation Systems are tested and certified to comply with the requirements of a Fire Alarm Control Unit,

- Primary and secondary power sources
- Receives signals from initiating devices or other fire alarm control units
- And processes signals to determine part or all of the required fire alarm system output functions.

Nationally Recognized Testing Lab (NRTL)



TÜV SÜD Product Services GmbH (TUVPSG)

- 49-89-5008-4335
- Ridlerstrasse 65, D-80339
- Munich, Germany

List includes:

- CSA International
- FM Approvals LLC (FM)
(formerly Factory Mutual Research Corporation)
- Underwriters Laboratories Inc. (UL)

For additional information please visit

- <http://www.osha.gov/dts/otpca/nrtl/nrtllist.html>

S800 High Integrity I/O

AI880 Features

8 channels, 4-20mA and 0-20mA

Certified for 4-20mA

10mS time resolution

0 – 1240mS configurable filtering time

Communication with Hart enabled transmitters (router)

Replaceable shunt per channel

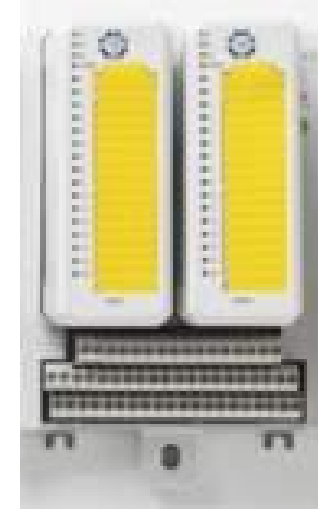
Supervision of shunt

Current limited field power supply per channel

Supervision of power supply per channel, also in a redundant configuration

Individual supervision and reporting of 4 configurable alarm limits per channel
(Device Malfunction Low, Low, High, Device Malfunction High)

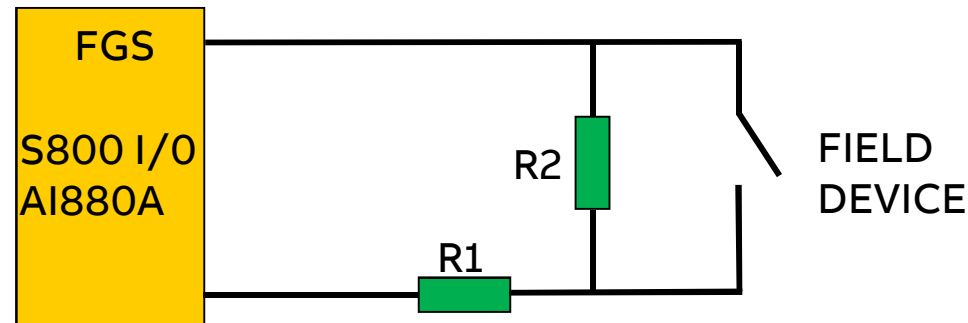
Simple configuration for alarm limits according to Namur standard NE 43



Analog Inputs

AI880A as DI - Loop Supervised Digital Input Module is used with an external field loop resistor network, this resistor network shall be configured in accordance with the guidance in the user manual Doc No. 3BSE020924

Automatic fire detectors selected for select process modules include UL listed / FM approved standard photoelectric smoke detectors and rate compensated heat detectors. Manual fire detection includes UL listed fire alarm call points. Each of these field devices interface with the Safety Instrumented System (SIS) via the high integrity input module (AI880A). The input module is configured for loop supervision and digital input. The resistor network is an end-of-line / in-line assembly placed in the circuit near the field device for open circuit and short circuit supervision.



S800 High Integrity I/O

DO880 Features

16 channels, 19-30 V

Certified for "normally energized" (NE) (high demand), "normally de-energized" (ND) (low demand)

Output diagnostics is performed without pulsing of outputs

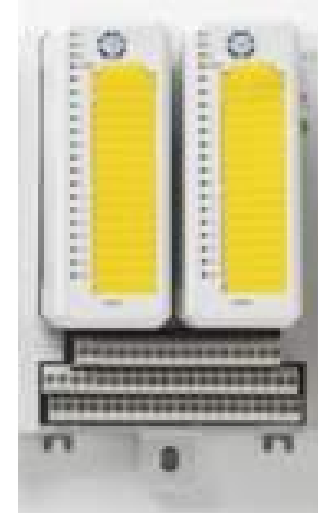
Outputs are supervised for overload and short & over current protected

Load is monitored in energized and de-energized state (per channel)

Configurable limits for overload

Upon channel errors, relevant outputs are set to safe state (de-energized)

Upon module errors, all outputs are set to safe state (de-energized)



Digital Outputs

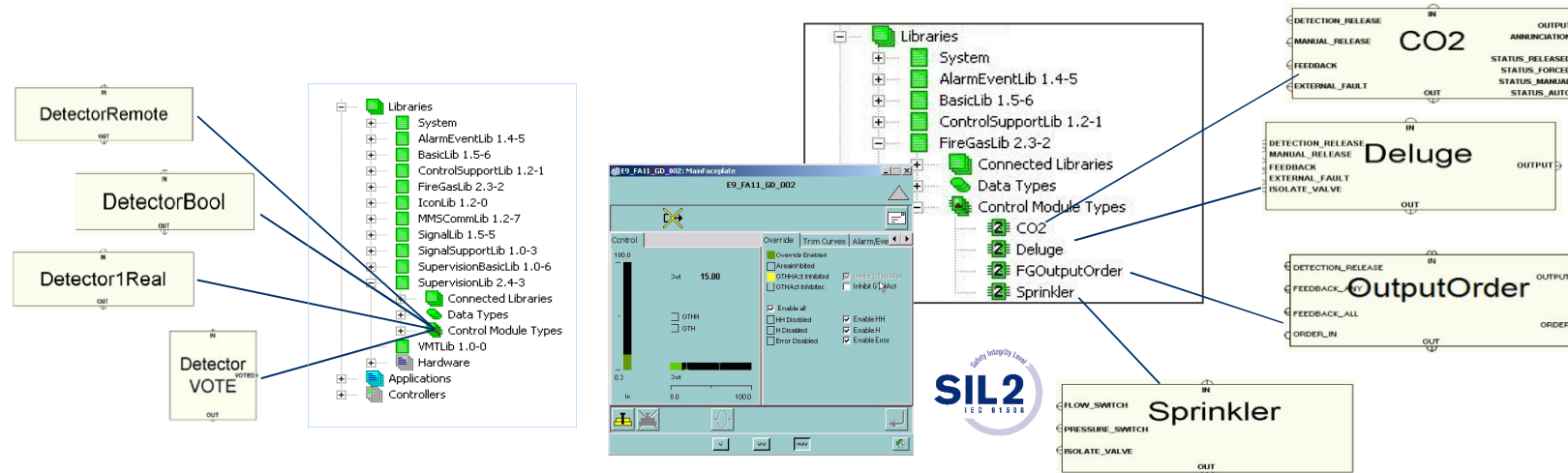
Normally De-energized DO880 channels can only be used in High Demand applications provided the demand rate of the process exceed 10 minutes.

Normally De-energized DO880 channels used in loops where a false trip directly cause a hazardous event (e.g. fire extinguishing with CO2) are restricted to SIL2 if the field device has a response time that is shorter than 10ms.

Normally De-energized DO880 channels are meant to be used with latched field devices where no continuous energized safe state is required.

Fire & Gas System

Safety Certified Libraries



Supervision Library

Detector input

System control and monitoring

Output handling

Overview presentation

Libraries enable significant savings during engineering

Fire & Gas Library

Modules for monitoring and control of protection systems

CO2

Deluge

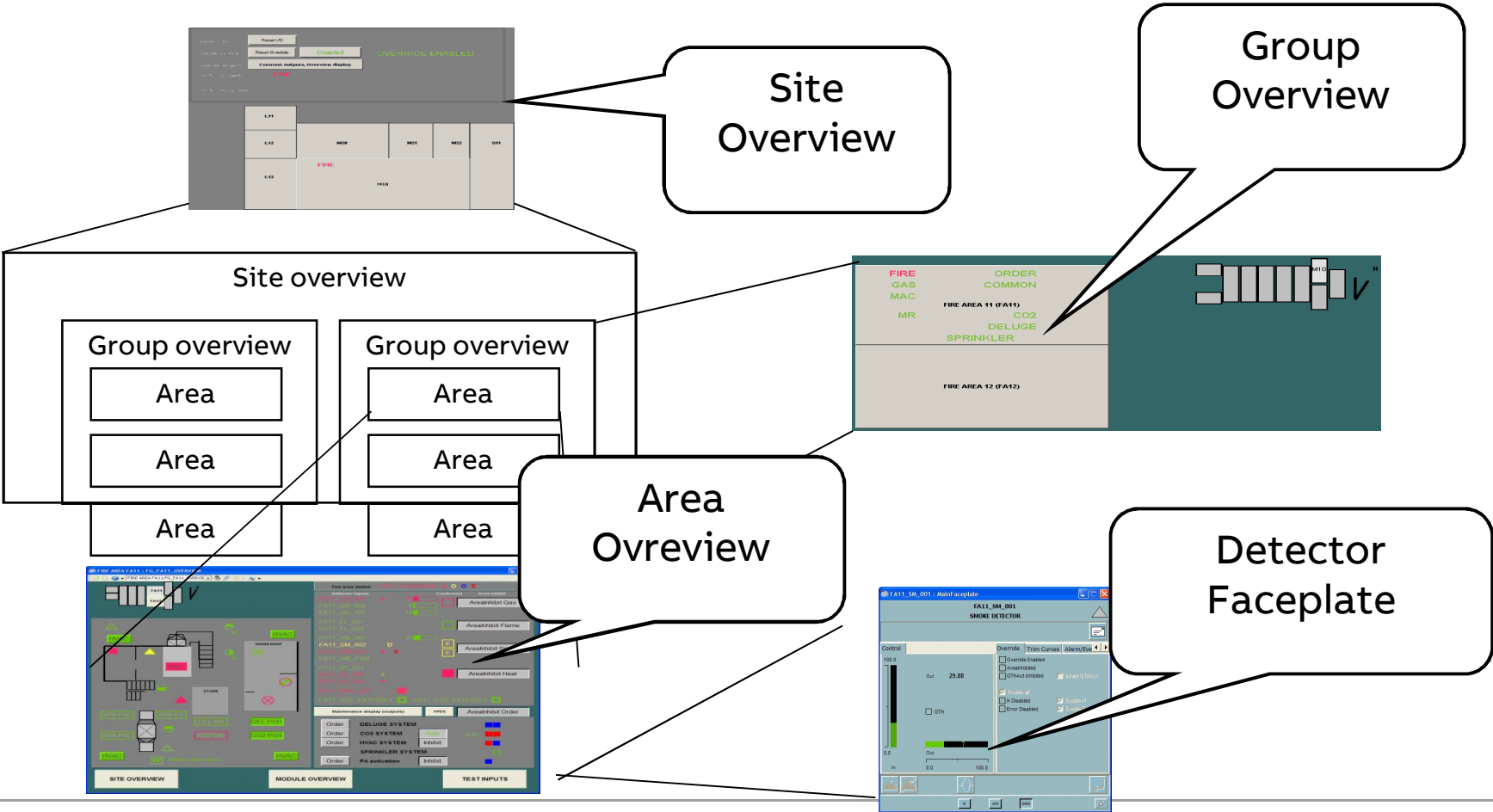
Sprinkler

Override functionality built into the modules to supervise the use of Force, Inhibit, Disable, and Manual Mode



Fire & Gas System – F&G

800xA HI – Display Structure



Conclusion

NFPA 72 covers system or application design aspects that are outside of the product(s) certification.

AC800M High Integrity satisfies the requirements of NFPA 72, EN 54 and IEC 61508/61511 as certified by TÜV.



ABB