Luis Duran | ABB Users Group, Anchorage | Feb. 24-25, 2016

System 800xA High Integrity SIL rated systems for BMS and Fire and Gas

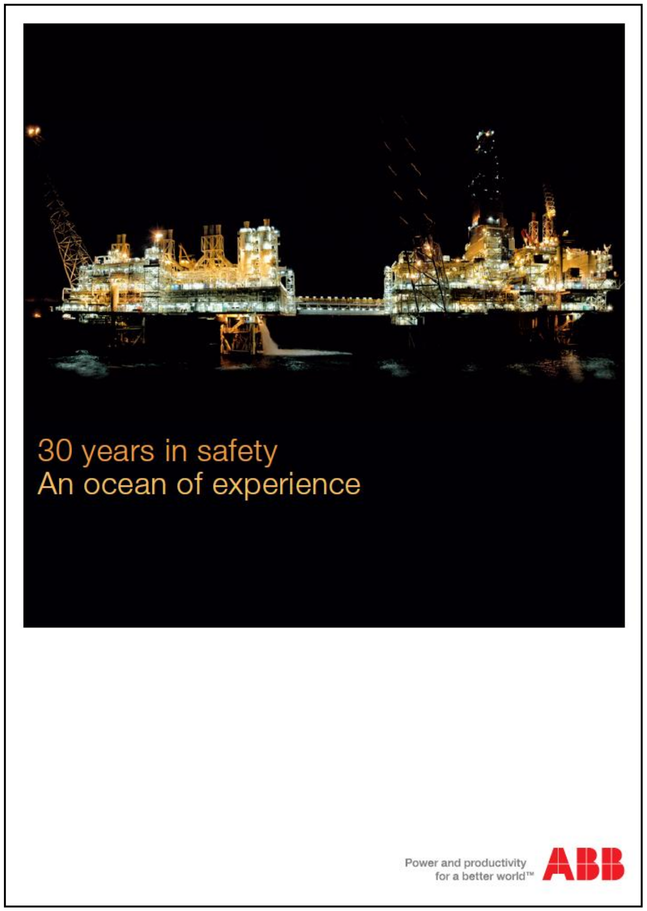
800xA High Integrity
Safety Update

- ABB in Safety
- Functional Safety Update
- High Integrity Overview
  - Integrated Control and Safety
  - Diversity and Systematic Capabilities
- Typical Applications
  - F&G Systems, Burner Management
- Burner Library
- Where to find additional information

Power and productivity
for a better world™ ABB

ABB in Safety for the Process Industries
35+ Years in Safety

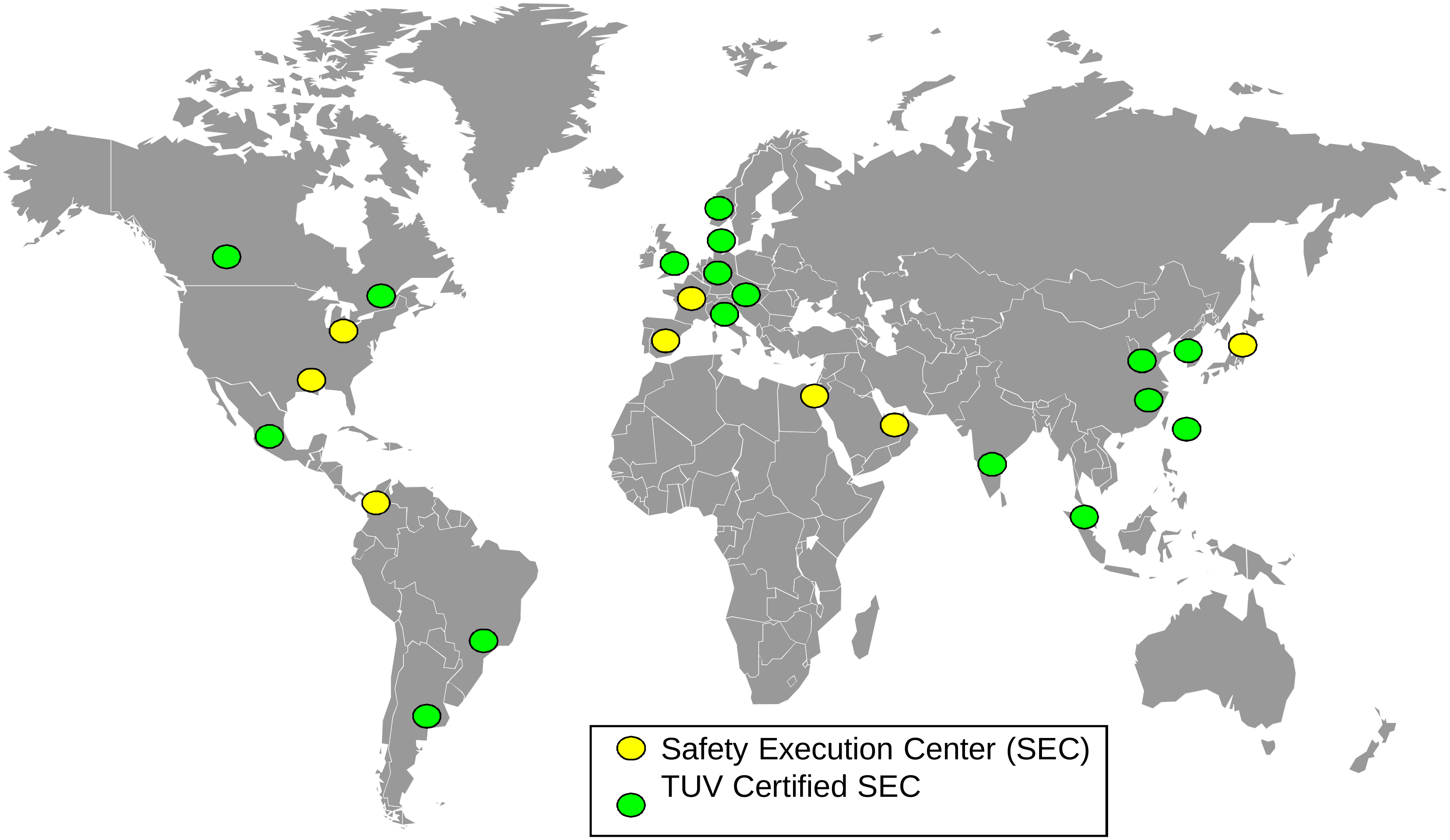
- 35+ years of experience in the specification, design, implementation and installation of process safety systems
- Over 3,600 System 800xA High Integrity safety systems installed globally since 2005
- Developed and installed the original “integrated” safety system with the Safeguard platform
- Global installations in over 55 countries including largest offshore installation on earth (Troll A)



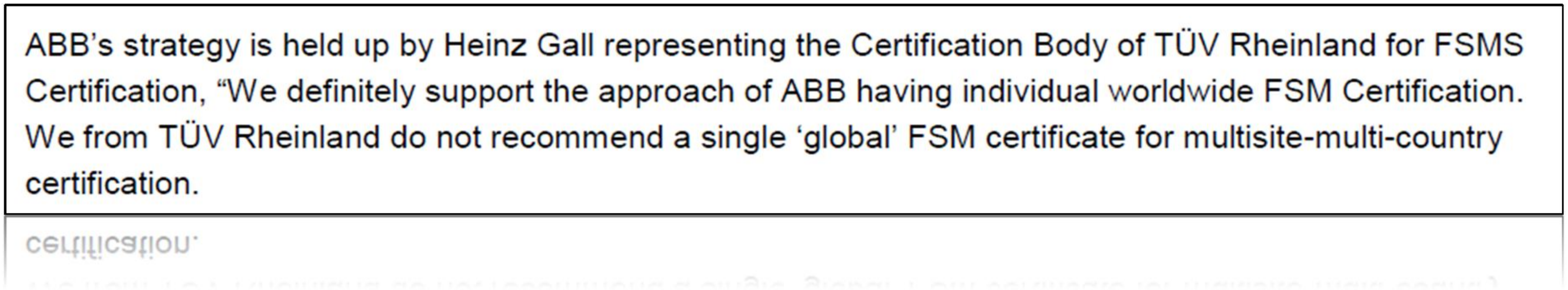
30 years in safety
An ocean of experience

Power and productivity
for a better world™ ABB

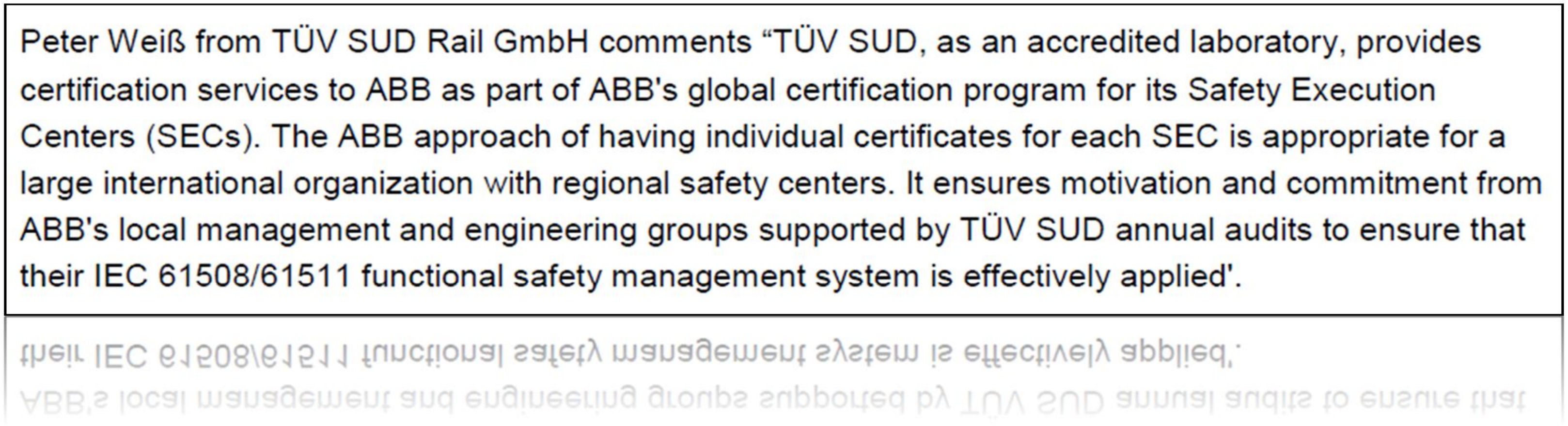
ABB Safety Execution Centers
35 Years Of Experience With Safety Systems



Where to find help?
TÜV endorsement of ABB SEC Approach



ABB’s strategy is held up by Heinz Gall representing the Certification Body of TÜV Rheinland for FSMS Certification, “We definitely support the approach of ABB having individual worldwide FSM Certification. We from TÜV Rheinland do not recommend a single ‘global’ FSM certificate for multisite-multi-country certification.



Peter Weiß from TÜV SUD Rail GmbH comments “TÜV SUD, as an accredited laboratory, provides certification services to ABB as part of ABB's global certification program for its Safety Execution Centers (SECs). The ABB approach of having individual certificates for each SEC is appropriate for a large international organization with regional safety centers. It ensures motivation and commitment from ABB's local management and engineering groups supported by TÜV SUD annual audits to ensure that their IEC 61508/61511 functional safety management system is effectively applied'.

Success Stories
Kindly Tech Trading Co. Egyptian Potassium Sulfate

- **ABB Solution:**
- Freelance system and Independent HI safety system solution, including
  - 2 redundant AC 900F controllers,
  - 1 PM 865 HI,
  - 1 DCS Engineering stations,
  - 1 ESD Engineering Station,3 Operator stations
  - 1 set of Freelance 2013 and Control Builder Safe
  - 1500 I/O signals
  - Fieldbus: PRFOIBUS DP
- **Other ABB products:**
  - low-voltage switchgear, motor control center system, low-voltage drives and low-voltage motors.
- **Why ABB?**
  - Comprehensive solution and leading technology
- Operation: July, 2016

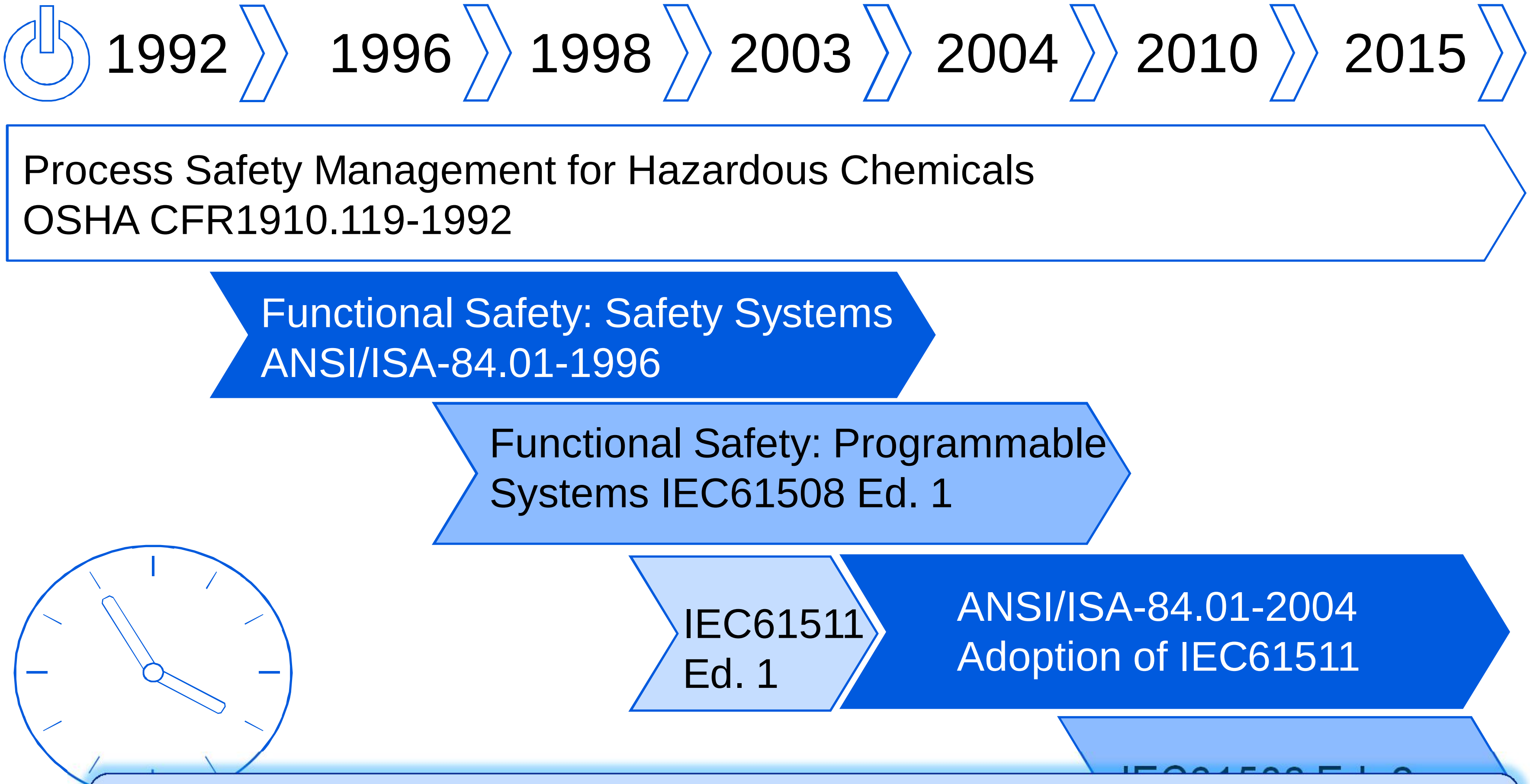
Success Story
Stand alone Safety Reference

- **Application:**
- Emergency shutdown system (ESD) designed for safe shutdown of the terminal operations during emergency situation
- **ABB solution**
- Integrated Process and Safety IO solution for 600 IOs. with one PM865 Controller , S800 I/Os and Control Builder Safe
- **Status:** Under commissioning
- **Why ABB:**
- Cost-effective solution
- 2 Standalone safety System, 2 PM865 with process and Safety IOs.

Functional Safety Update

Power and productivity
for a better world™

Functional Safety
Evolution to Performance Based Standards



1992 1996 1998 2003 2004 2010 2015

Process Safety Management for Hazardous Chemicals
OSHA CFR1910.119-1992

Functional Safety: Safety Systems
ANSI/ISA-84.01-1996

Functional Safety: Programmable
Systems IEC61508 Ed. 1

IEC61511
Ed. 1

ANSI/ISA-84.01-2004
Adoption of IEC61511

IEC61508 Ed. 2

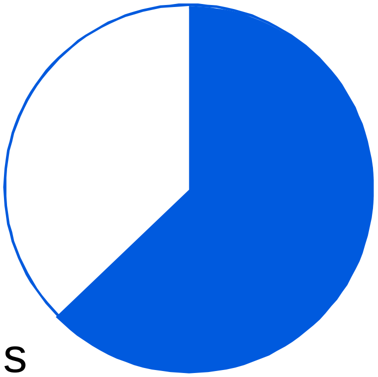
Acceptance and enforcement of safety standards fuel opportunities

Power and productivity
for a better world™

Business drivers
State of the Safety Systems installed base

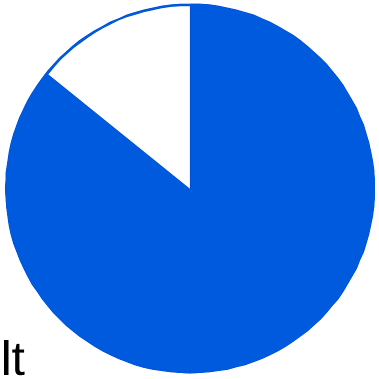
65%

Systems installed
before publication
of current standards



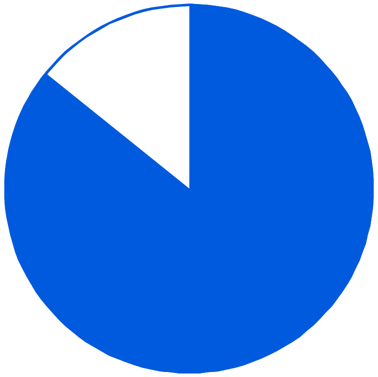
90%

Users perceived
compliance to new
standards are difficult



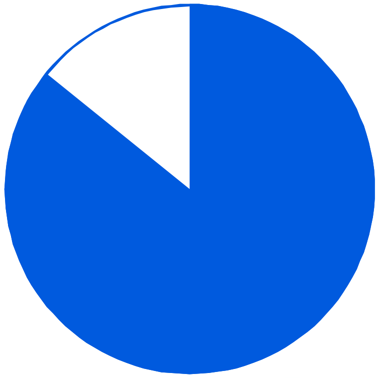
87%

Systems used today
are obsolete



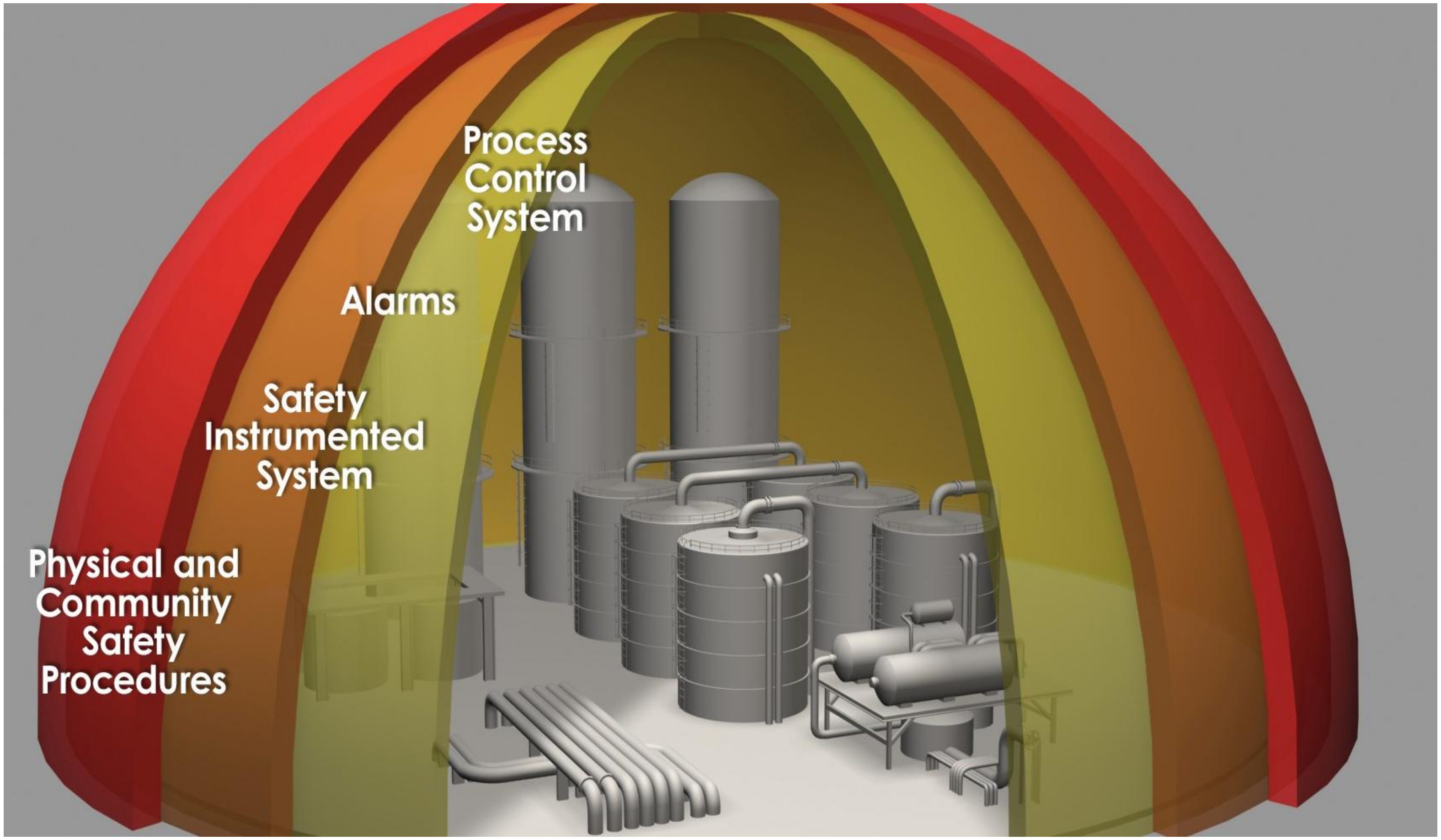
84%

Systems upgrades
are planned during
plant turnaround



Expansion & upgrade of existing plants drives safety systems retrofit

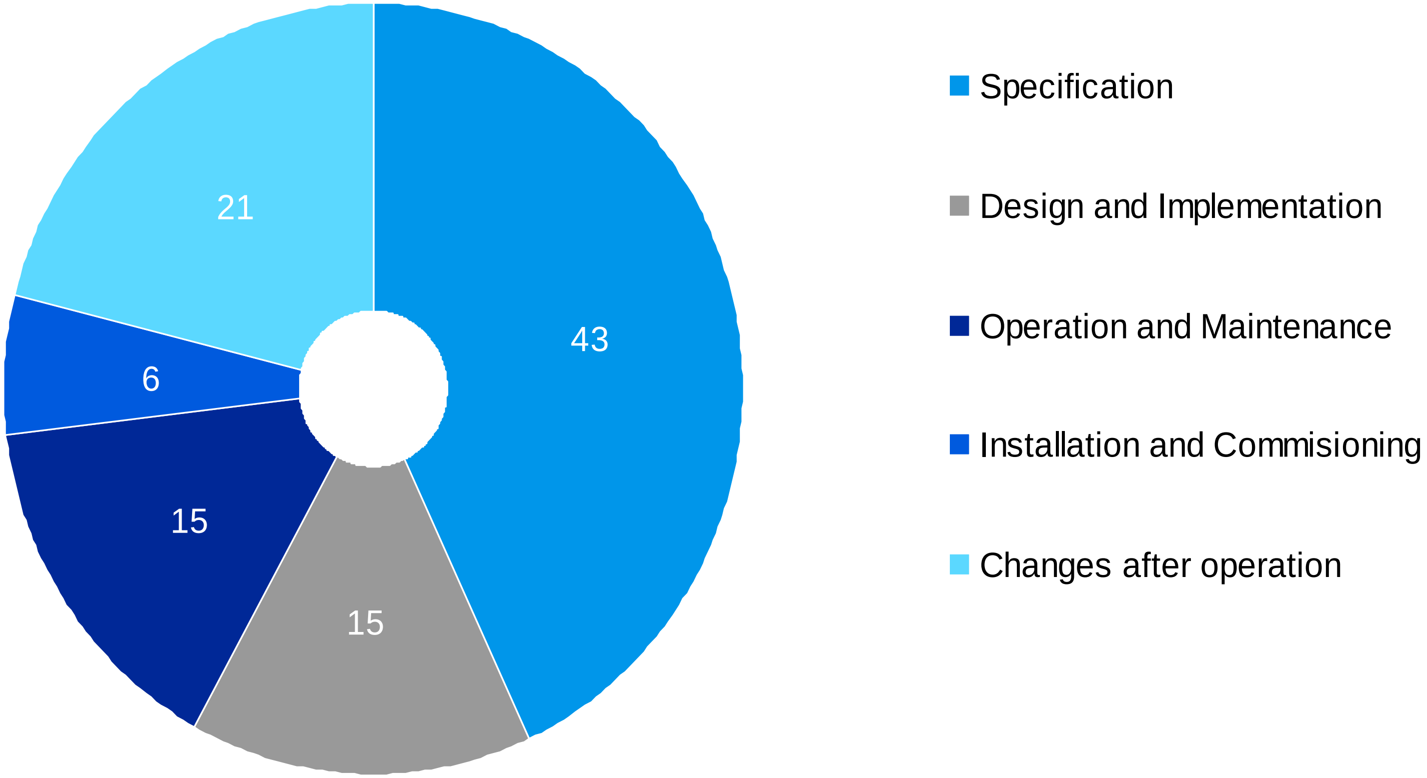
Independent Protection Layers


Process Control System
Alarms
Safety Instrumented System
Physical and Community Safety Procedures

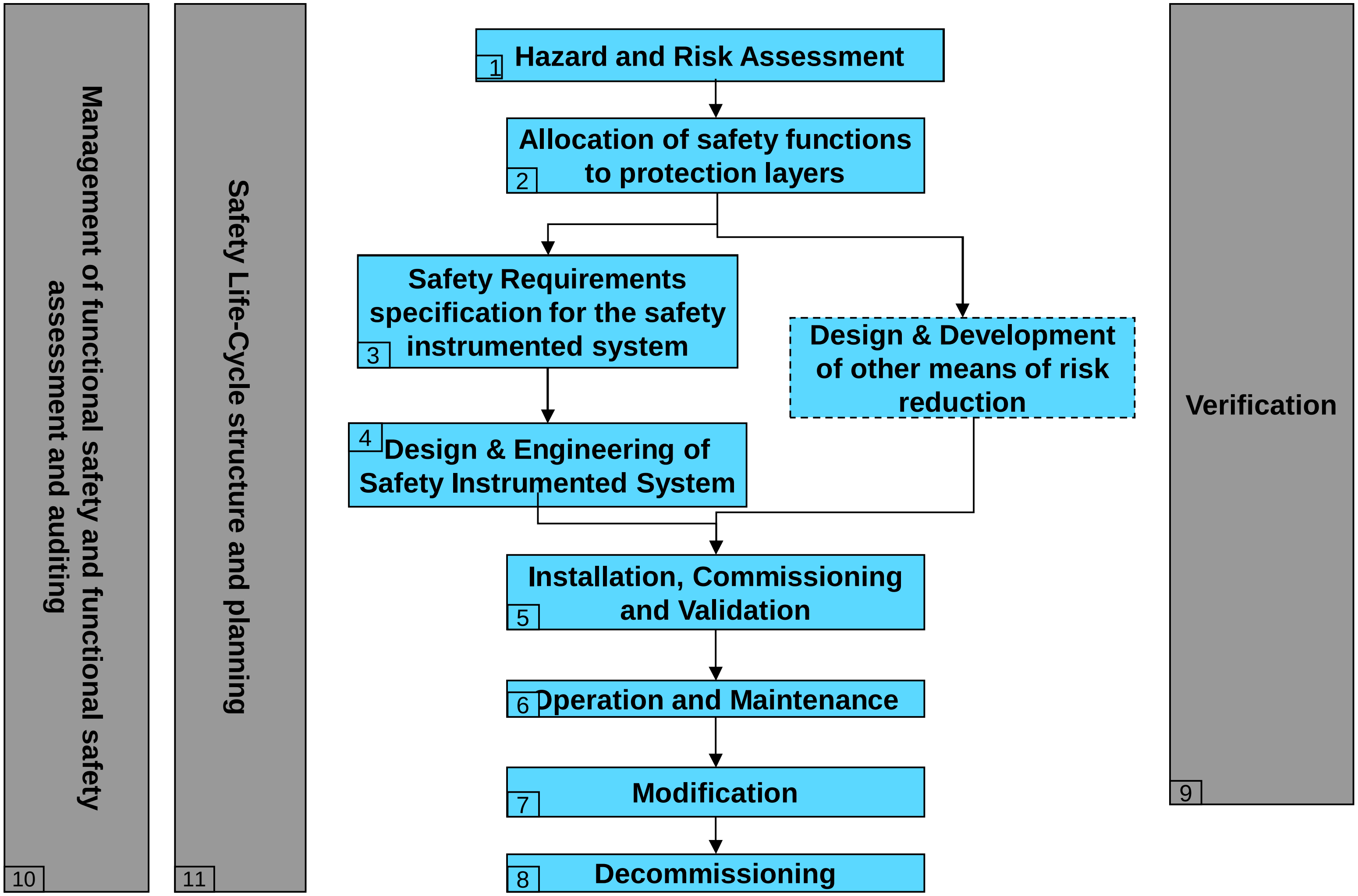
B

All Lifecycle Steps matter
Specification, Design and Implementation 58%!

Primary Cause of Control System Failure
Source: Out of control: Why control systems go wrong and how to prevent failure
HSE Books ISBN 0-7176-2192-8



Functional Safety Standard and Safety Lifecycle


1 Hazard and Risk Assessment
2 Allocation of safety functions to protection layers
3 Safety Requirements specification for the safety instrumented system
Design & Development of other means of risk reduction
4 Design & Engineering of Safety Instrumented System
5 Installation, Commissioning and Validation
6 Operation and Maintenance
7 Modification
8 Decommissioning
9 Verification
10 Management of functional safety and functional safety assessment and auditing
11 Safety Life-Cycle structure and planning

Safety Lifecycle from IEC 61511

SRS Requirements

- Definition of the safe state
- Process inputs and their trip points
- Process parameters normal operating range
- Process outputs and their actions
- Relationship between inputs and outputs
- Selection of energize-to-trip and reenergize-to-trip
- Response time requirement
- Operator interface requirement

NORME
INTERNATIONALE

INTERNATIONAL
STANDARD

CEI
IEC
61511-1

Première édition
First edition
2003-01

Sécurité fonctionnelle –
Systèmes instrumentés de sécurité pour
le secteur des industries de transformation –

Partie 1:
Cadre, définitions, exigences pour le système,
le matériel et le logiciel

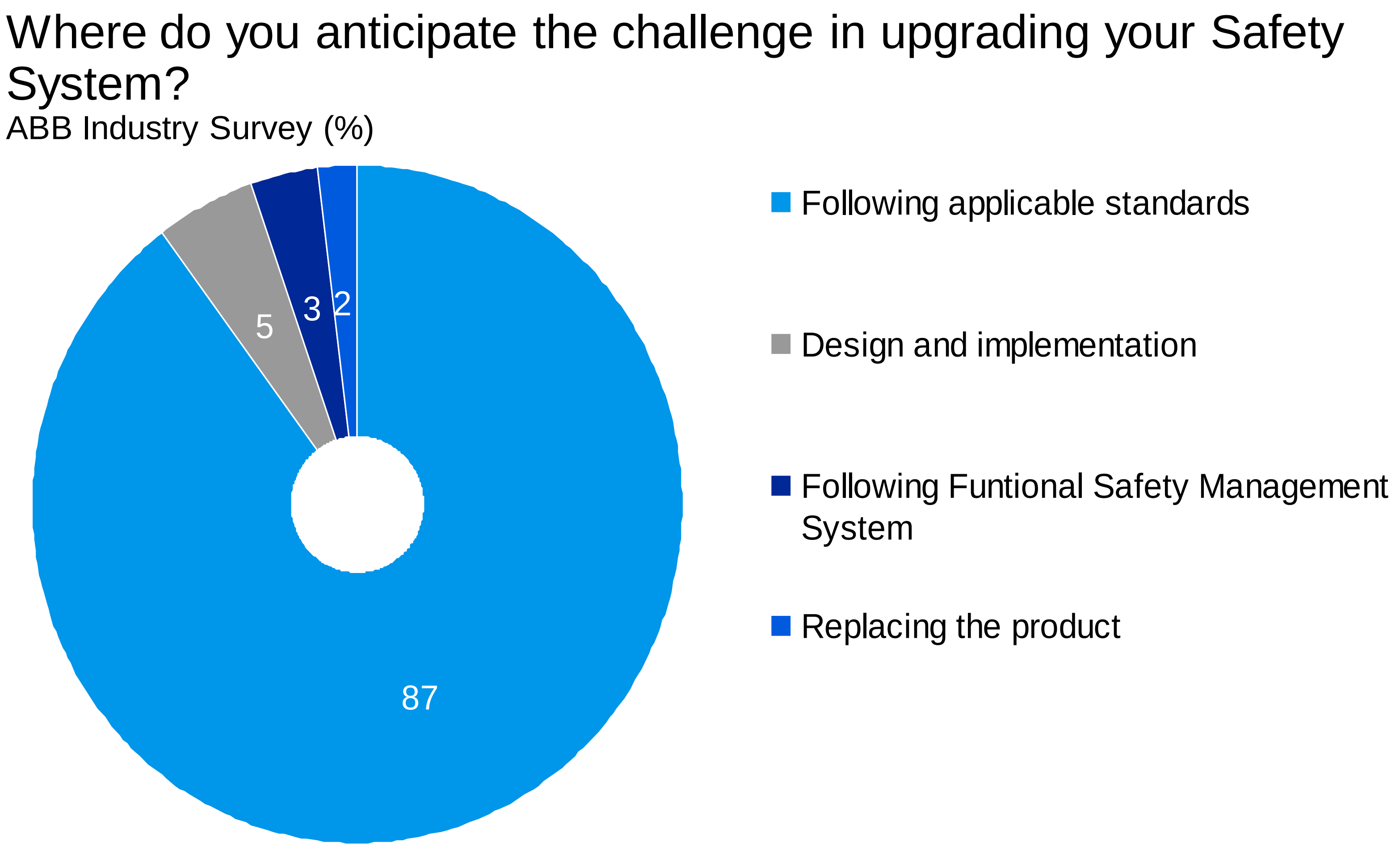
Functional safety –
Safety instrumented systems
for the process industry sector –

Part 1:
Framework, definitions, system,
hardware and software requirements

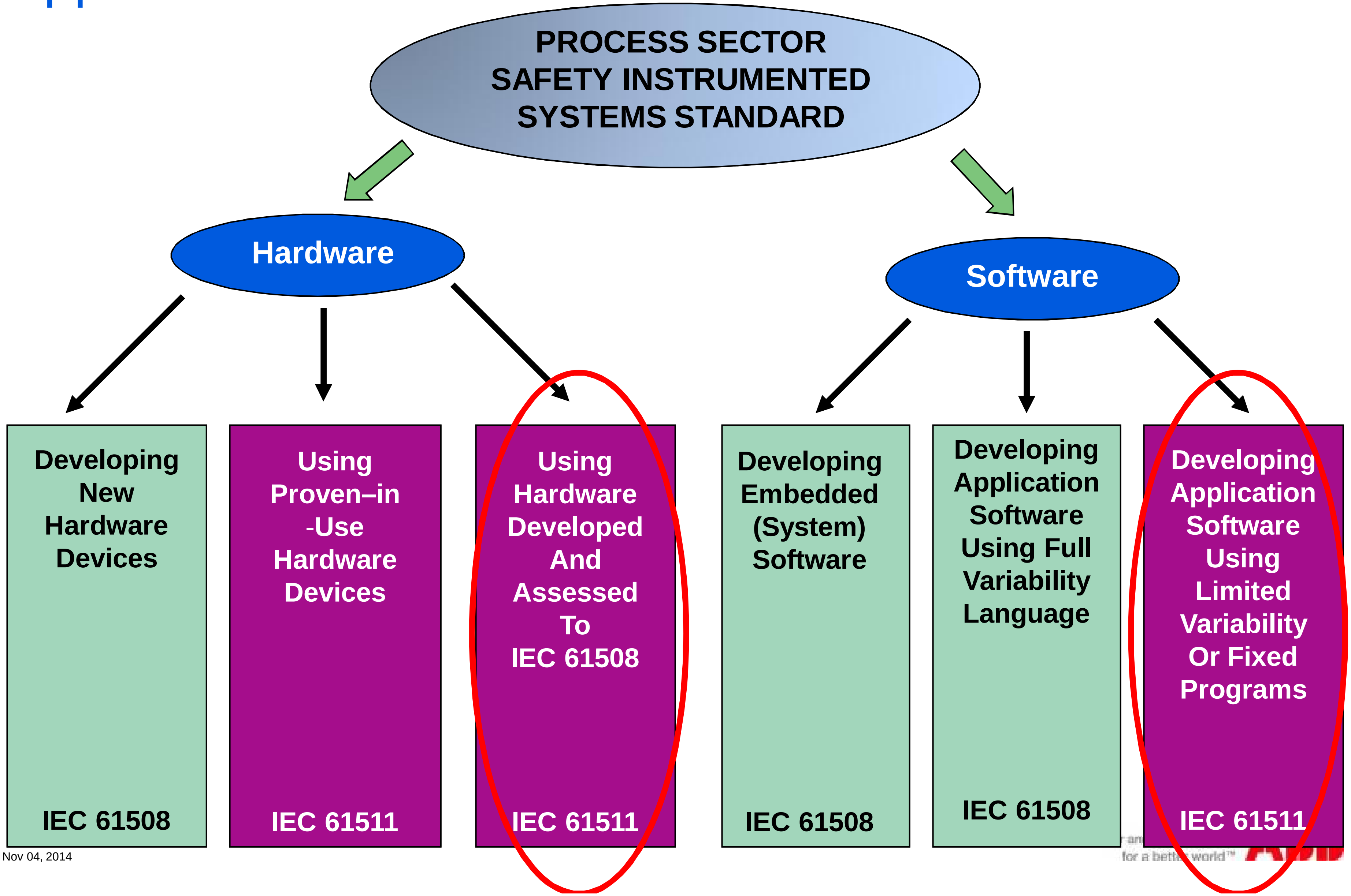
IEC

Numéro de référence
Reference number
CEI/IEC 61511-1:2003

Adopting Functional Safety Standards
Industry is challenged



Functional Safety Standards
Application of IEC 61508 and IEC 61511/ISA84



PROCESS SECTOR SAFETY INSTRUMENTED SYSTEMS STANDARD

Hardware

- Developing New Hardware Devices — IEC 61508
- Using Proven–in-Use Hardware Devices — IEC 61511
- Using Hardware Developed And Assessed To IEC 61508 — IEC 61511

Software

- Developing Embedded (System) Software — IEC 61508
- Developing Application Software Using Full Variability Language — IEC 61508
- Developing Application Software Using Limited Variability Or Fixed Programs — IEC 61511

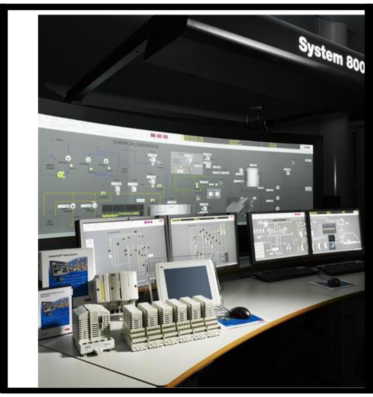
High Integrity:
One system Any Process Control

Power and productivity
for a better world™

High Integrity
One system for any Process Automation Interface

Compact

800xA

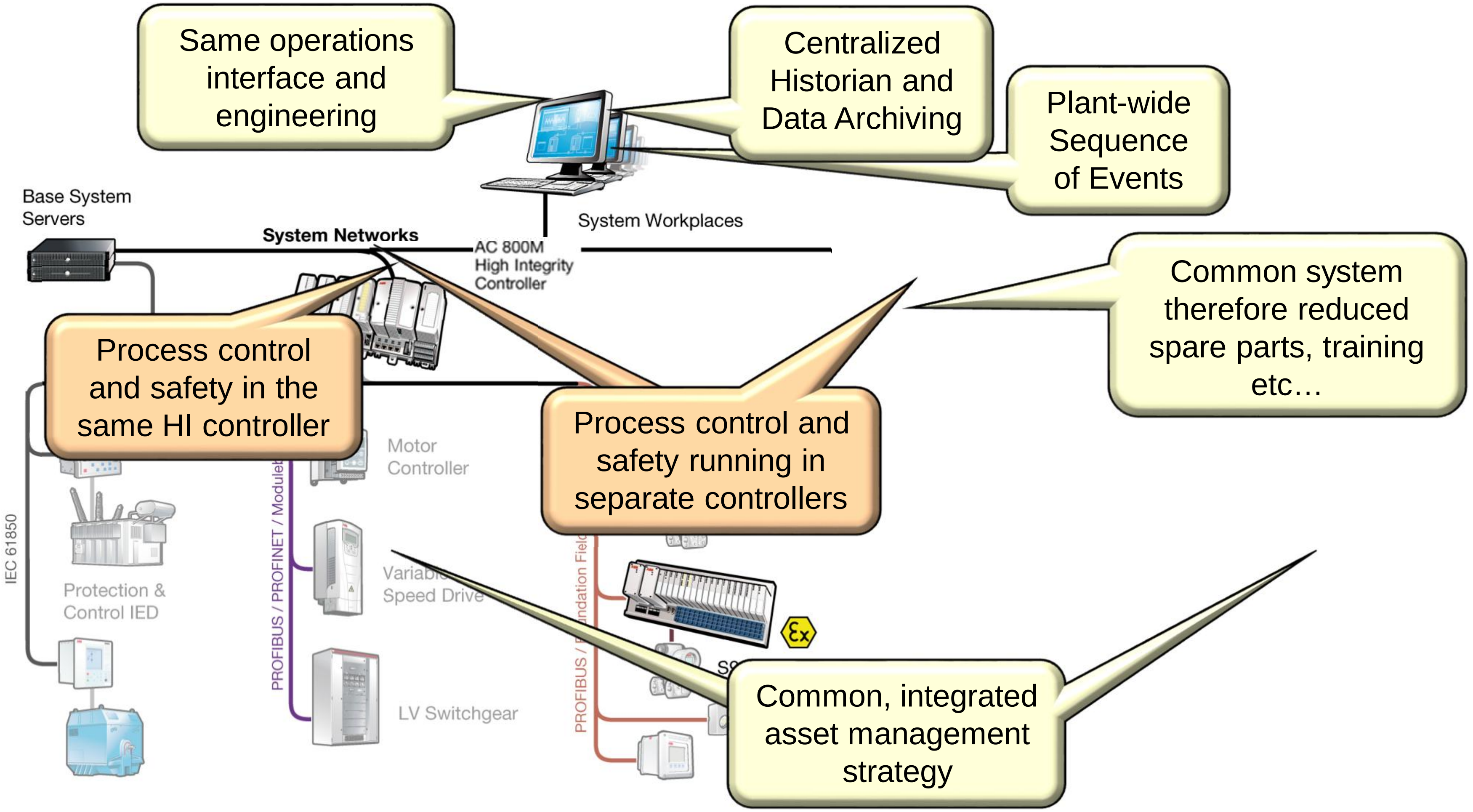


Freelance

Symphony Plus

- Safety is a top priority for most users in all industries
- Process Industries:
  - Oil & Gas, Chemical, Petrochemical, Pulp & Paper, Power Generation
- Multiple applications:
  - ESD/PSD, FGS, BMS, HIPPS, etc.

Integrated Process Control and Safety
System 800xA High Integrity



Same operations interface and engineering

Centralized Historian and Data Archiving

Plant-wide Sequence of Events

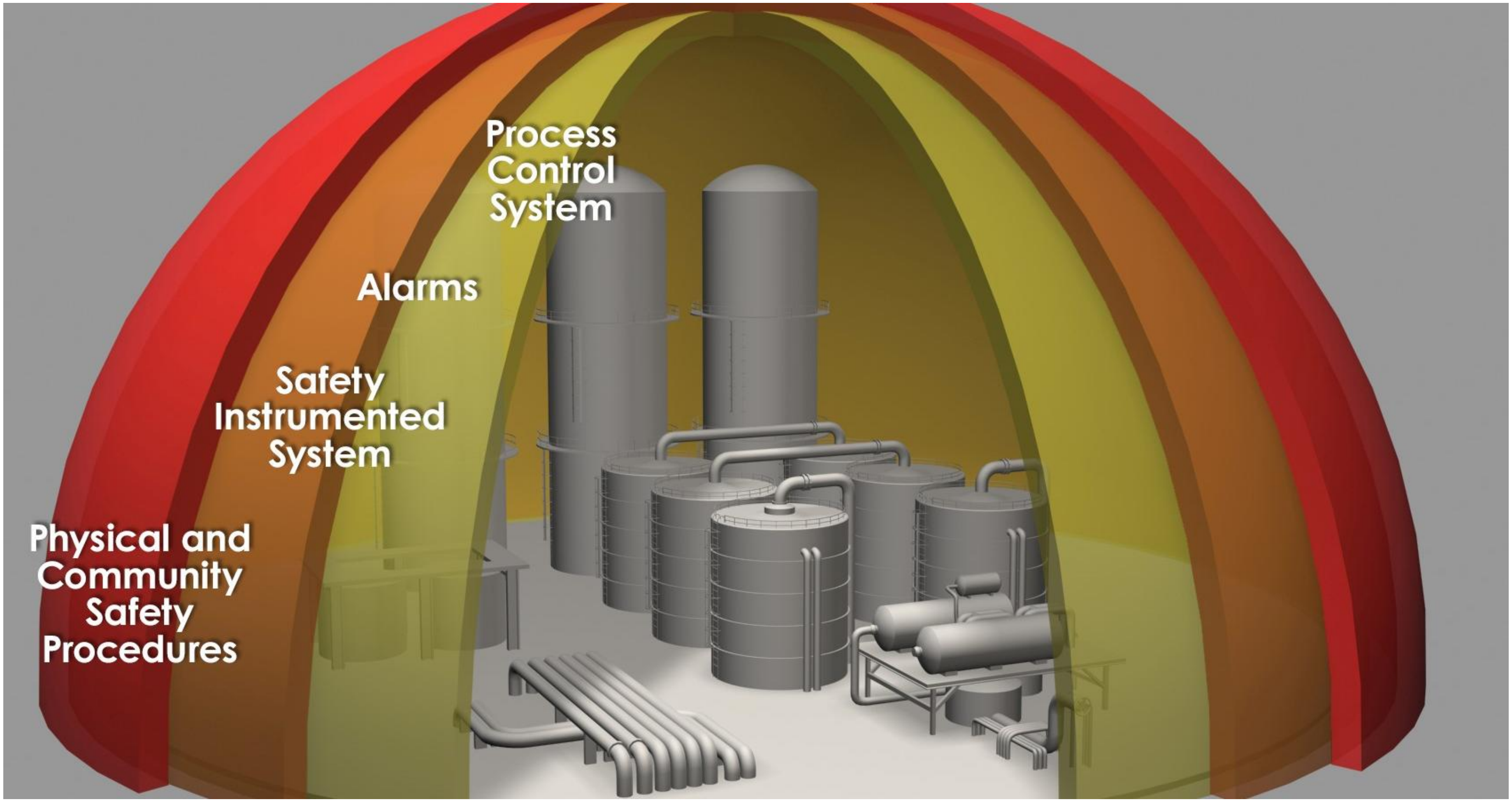
Common system therefore reduced spare parts, training etc…

Process control and safety in the same HI controller

Process control and safety running in separate controllers

Common, integrated asset management strategy

Protection Layers must be Independent
Not uncoordinated


Process Control System
Alarms
Safety Instrumented System
Physical and Community Safety Procedures

Power and productivity for a better world™ ABB

What are the benefits of ICSS to Operations?
Better response to abnormal conditions

- Integrated Control and Safety System (ICSS) implementations enable end-users to fully leverage the capabilities on the BPCS
  - Information Management
  - Reporting
  - Alarm Management
  - Sequence Of Events
  - Asset Optimization
  - Engineering
  - Etc

Integration must be designed to avoid Common Cause Failures

800xA High Integrity
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

TUV Certificate

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

Optimize Factory Acceptance Test and Lifecycle Support

System 800xA High Integrity
The Value of Adding Safety to 800xA

The cost of ad
safety system
significantly c
system that nee

Adding SIS points means updating that custom interface

Interface updates require more

Ex
sof

Extra hardware and software is needed to implement HART

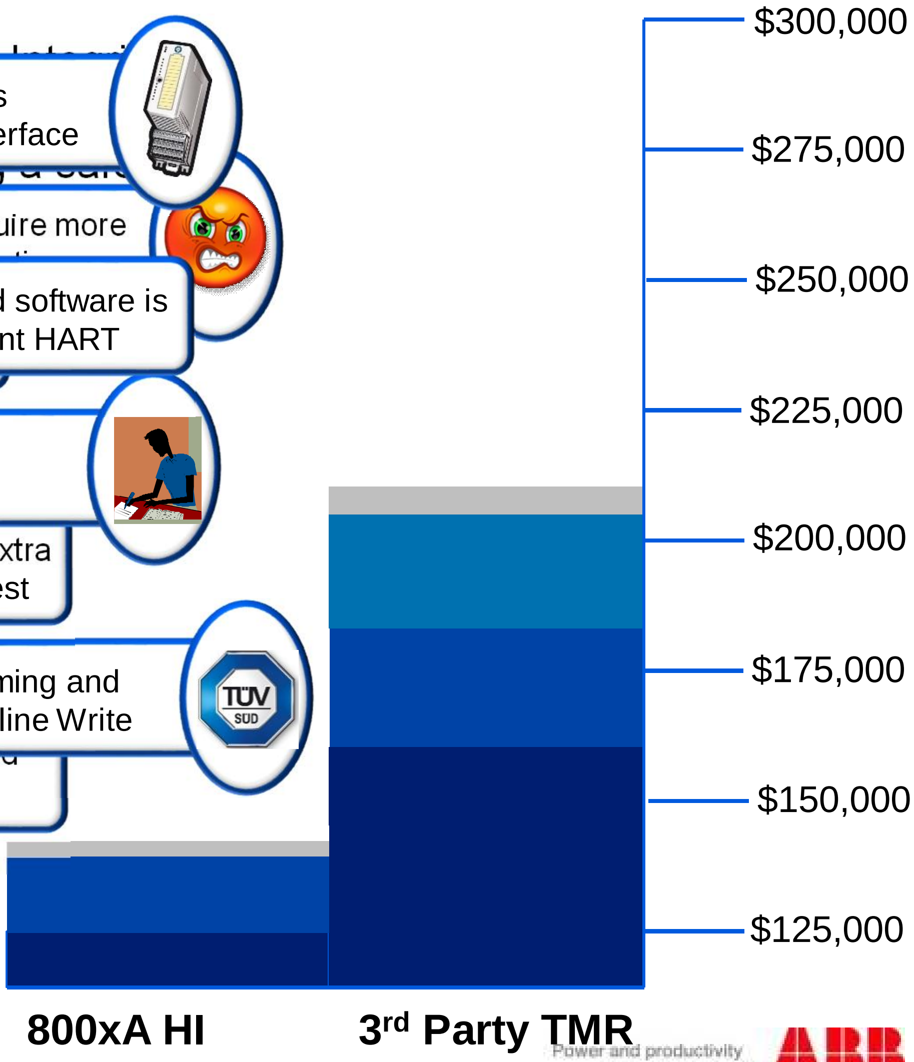
Separate engineering tool means more training

Custom interface requires extra design, programming and test

Additional programming and testing for Safe On-line Write

Extra lic
ethernet module required

- Adding SIS
- HAR
- Inter
- Software Mainter
- Trai
- BPC
- Application Engineering
- Hardware and Software

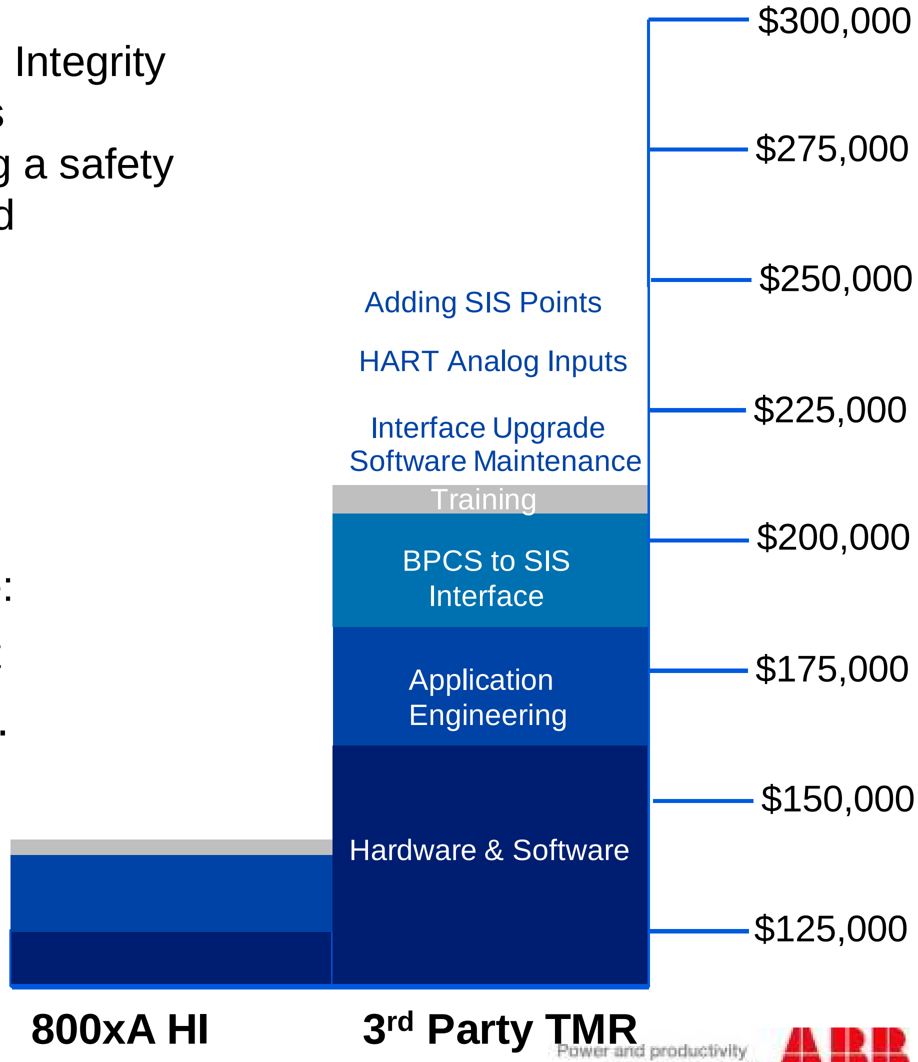


Power and productivity
for a better world™

System 800xA High Integrity
The Value of Adding Safety to 800xA

The cost of adding an 800xA High Integrity safety system to an 800xA DCS is ***significantly*** cheaper than adding a safety system that needs to be interfaced

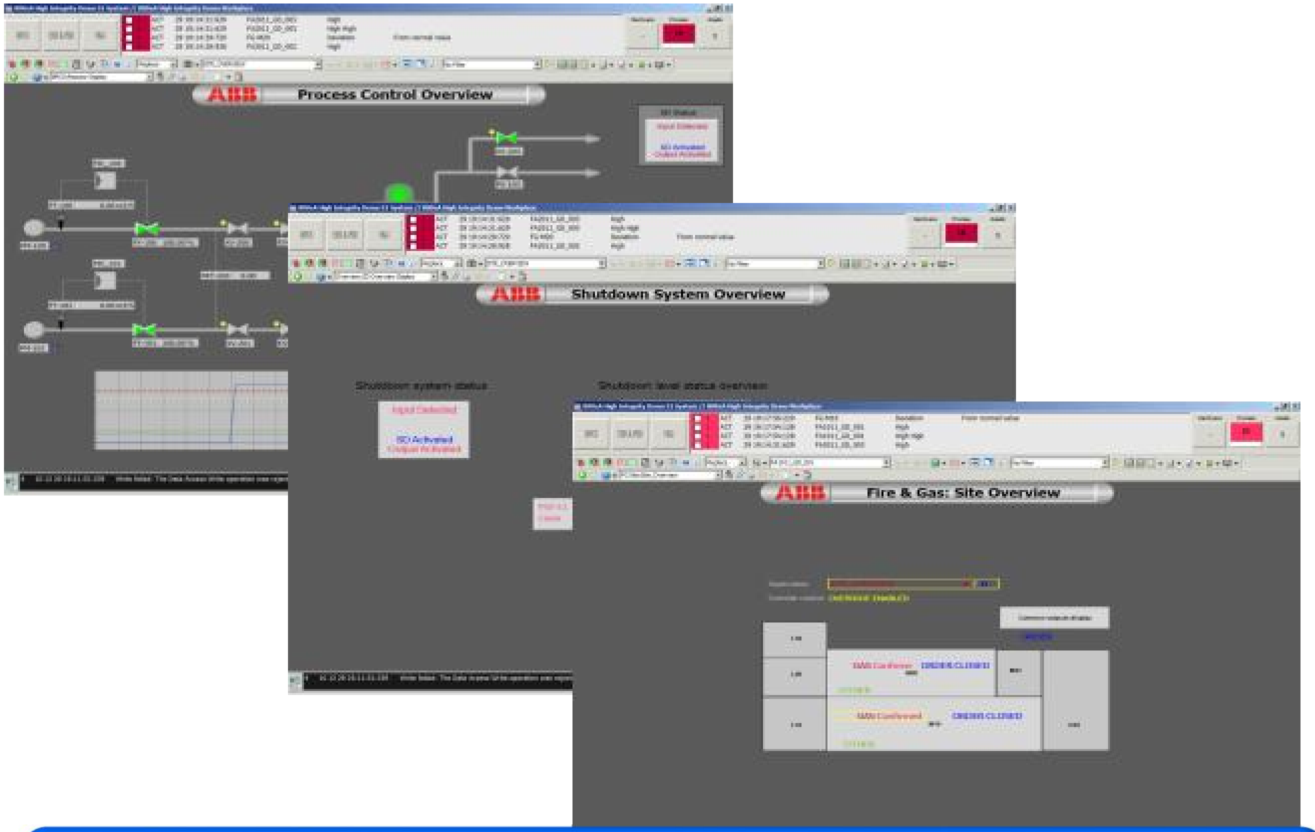
- Lifecycle costs add up
  - Extra hardware
  - Custom interface
  - HART analog inputs
- Additional “soft benefits” include:
  - Device / asset management
  - Common history, events etc.
  - Easier sensor validation



Operators can effectively react to abnormal events

Power and productivity
for a better world™

Thanks to a Common Operation Environment…
…Operator can take timely action



Monitor the Process and respond to Abnormal Conditions

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:

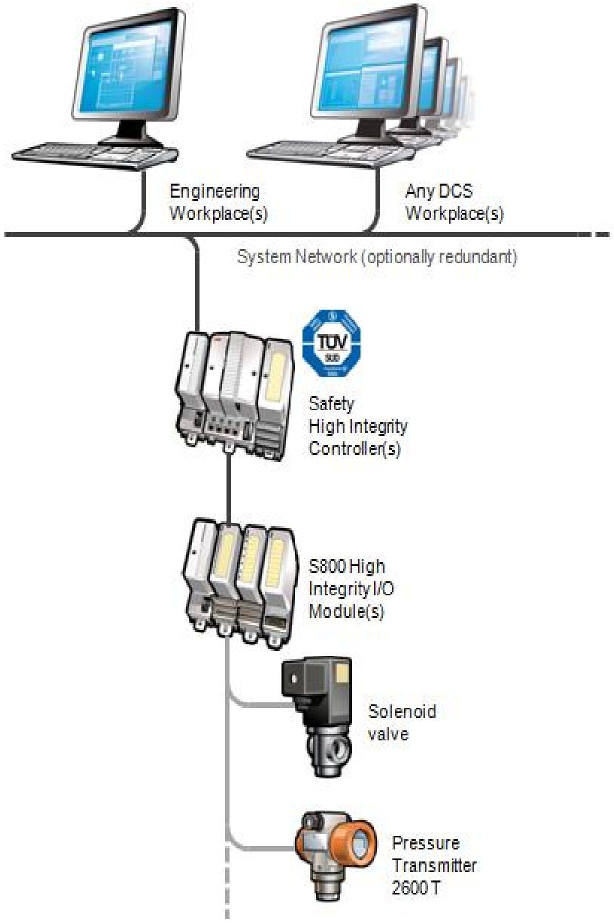
- Oil & Gas
- Petrochemical
- Chemical
- Pulp & Paper
- Power

Great for industrial applications:

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

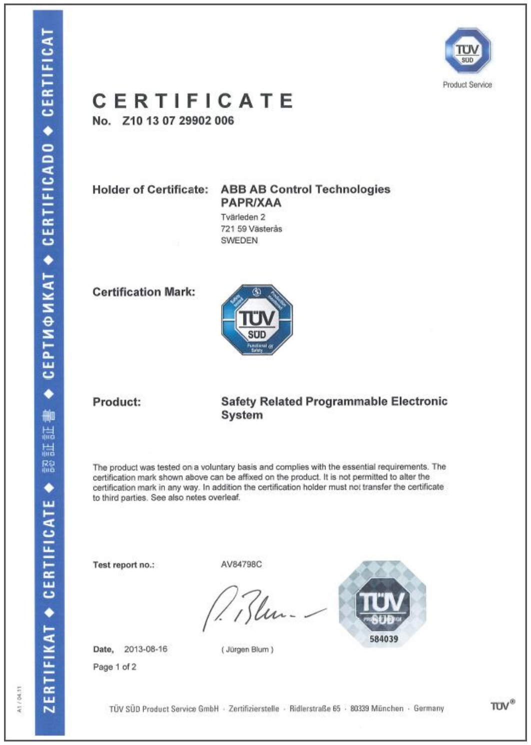
Independent High Integrity
Overview

- 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
  - Certified Libraries
- Connectivity and Interfacing
  - ABB Control systems
  - 3rd party software and control systems
- Diagnostics


Engineering Workplace(s)
Any DCS Workplace(s)
System Network (optionally redundant)
TÜV SÜD
Safety High Integrity Controller(s)
S800 High Integrity I/O Module(s)
Solenoid valve
Pressure Transmitter 2600T

Small Independent HI system with engineering and DCS

TÜV Certificates
ABB High Integrity Safety Certificates



ZERTIFIKAT ◆ CERTIFICATE ◆ 認証証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE
No. Z10 13 07 29902 006

Holder of Certificate: **ABB AB Control Technologies PAPR/XAA**
Tvärleden 2
721 59 Västerås
SWEDEN

Certification Mark:

Product: **Safety Related Programmable Electronic System**

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: AV84798C

P. Blum

Date, 2013-08-16 (Jürgen Blum)

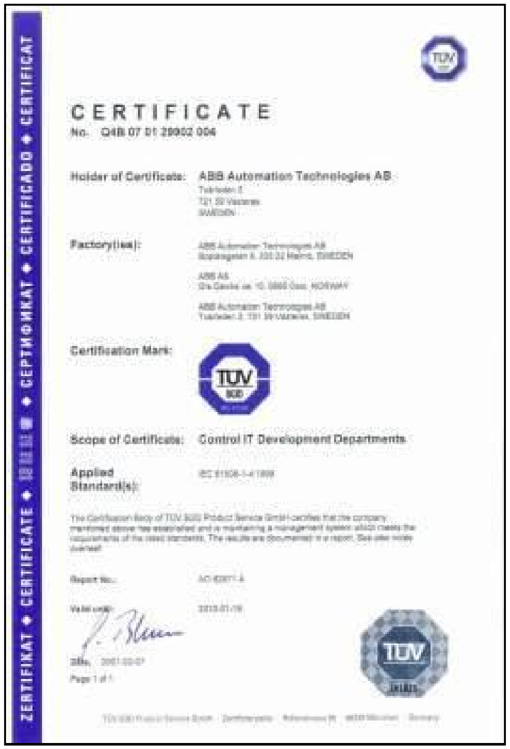
Page 1 of 2

584039

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

A1 / 04.11

Product Safety Certificate



ZERTIFIKAT ◆ CERTIFICATE ◆ [illegible] ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE
No. Q4B 07 01 29902 004

Holder of Certificate: ABB Automation Technologies AB
[illegible]
SWEDEN

Factory(ies): ABB Automation Technologies AB
[illegible] SWEDEN

ABB AS
[illegible] NORWAY

ABB Automation Technologies AB
[illegible] SWEDEN

Certification Mark:

Scope of Certificate: Control IT Development Departments

Applied Standard(s): IEC 61508-1-4:1998

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: [illegible]

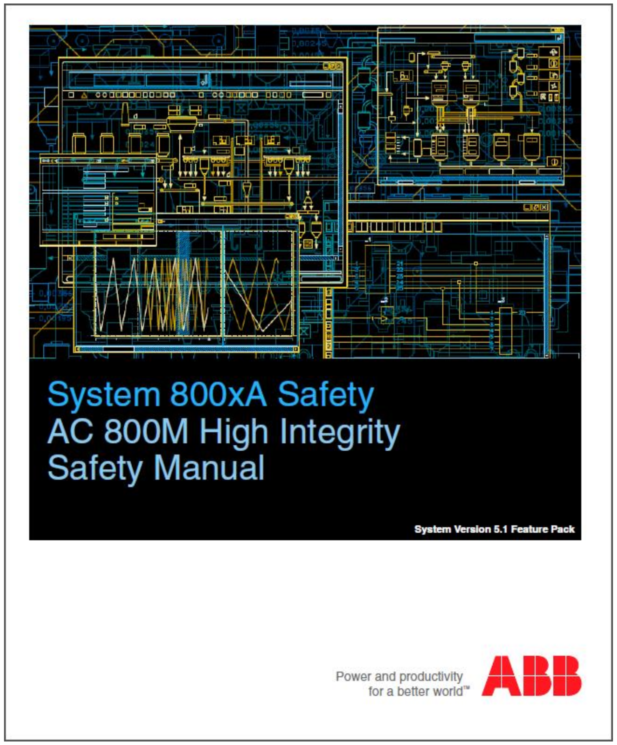
Valid until: [illegible]

Date, [illegible]

Page 1 of 1

[illegible]

Development Department Safety Certificate



System 800xA Safety
AC 800M High Integrity
Safety Manual

System Version 5.1 Feature Pack

Power and productivity
for a better world™

Safety Manual

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

Certificates
Industry Standards

- Functional Safety
  - IEC 61508
  - IEC 61511/ISA 84
  - UL1998
- Basic Safety
  - IEC61131
  - EN50178
  - UL508

- Application Standards
  - NFPA72/EN54
  - NFPA85/FM 7605
  - IEC62061
  - NFPA79

Why customers benefit from High Integrity?
High Integrity is different and better…

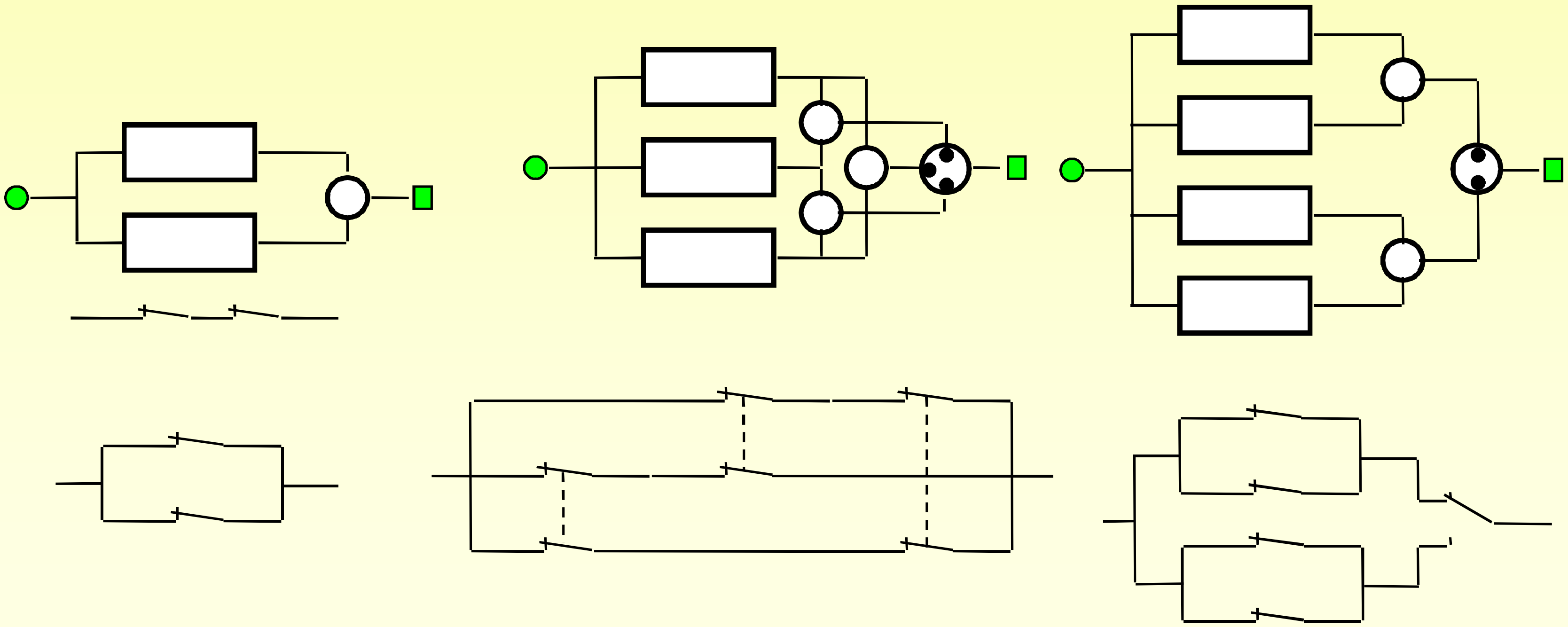
- Use of Diverse Technology
  - Provides better protection against Common Cause Failures, leading to reduced PFD
- Systematic Capabilities
  - Features as Difference Report, Compiler Restrictions, Access Control and Safe Online Write helps prevent systematic errors in programming the system
- Live Code 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

What does it mean for you?
Cost effective and Flexible solutions

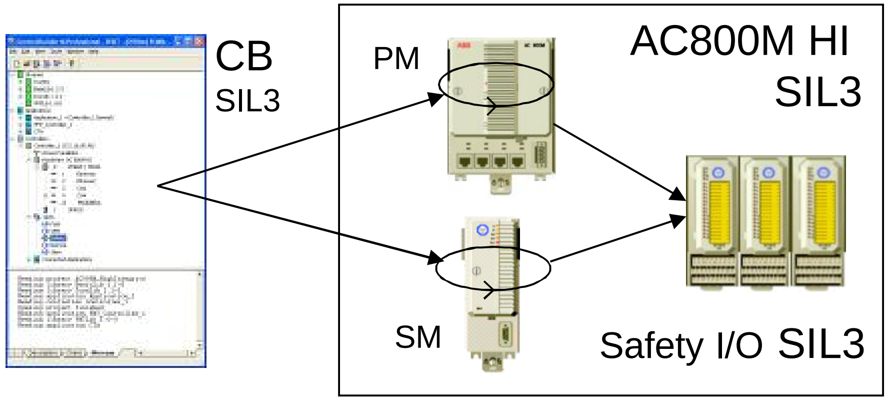
▪ Use of Diverse Technology	▪ SIL 3 without redundancy ▪ Smaller footprint ▪ Flexible configuration
▪ Systematic Capabilities	▪ Reduce human error ▪ Ensure compliance to Safety Manual
▪ Live Code Evaluation	▪ Simplifies application troubleshooting ▪ Simplifies Management of Change and Audit Trail
▪ Tight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

1st Generation Logic Solver Architectures
Traditional redundant systems

- **Duplex**
  - **1oo2D**
- **Triplex**
  - **2oo3**
- **Quad (Bi-Duplex)**
  - **2oo4D**



Diverse Architecture, Diverse Implementation
SIL 3? Yes, Redundancy? Not required

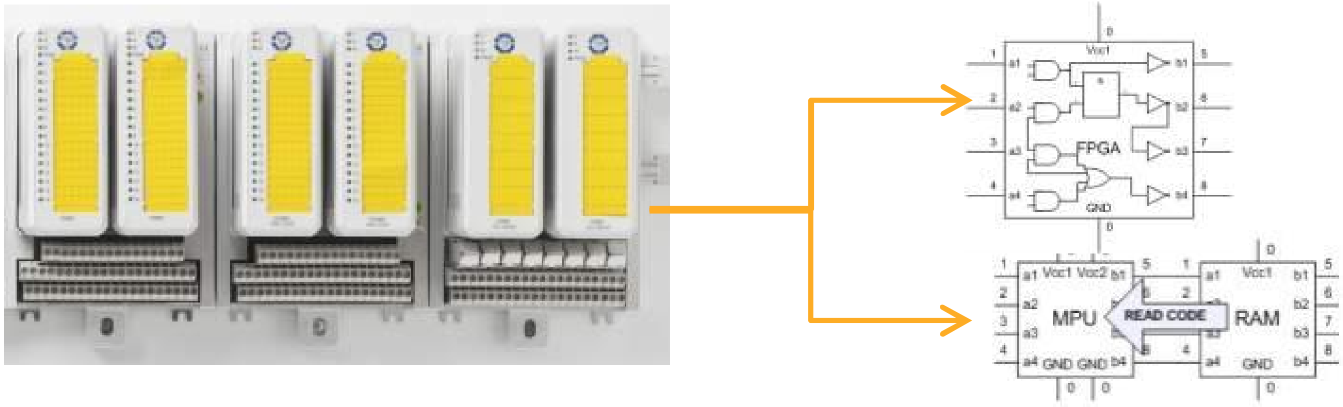


	HFT	
SFF (%)	0	1
< 60	—	SIL 1
60 - 90	SIL 1	SIL 2
90 - 99	SIL 2	SIL 3
> 99	SIL 3	SIL 4
	 1oo1D	 1oo2D

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) teams (Vasteras and Malmo, Sweden) and tested by a third independent team by people with different backgrounds
- The two channel architecture meets SIL3 requirements for hardware fault detection and reaction

Diverse Architecture, Diverse Implementation
S880 High Integrity I/O



Single and Redundant configuration

Hot Insertion and Hot Swap in redundant configuration

G3 Coating

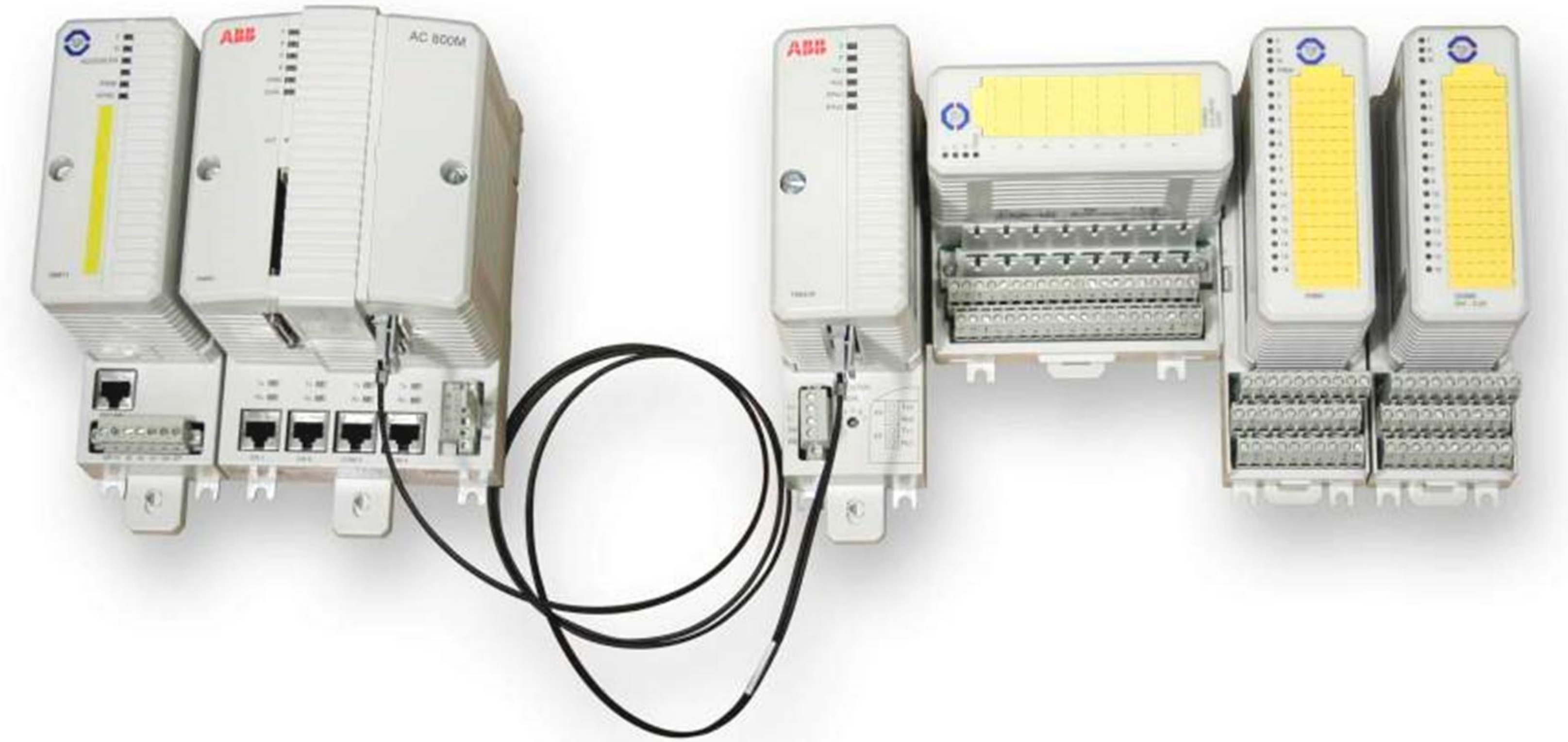
EX certified – Zone 2, Class 1 according to US standard

Embedded Diversity

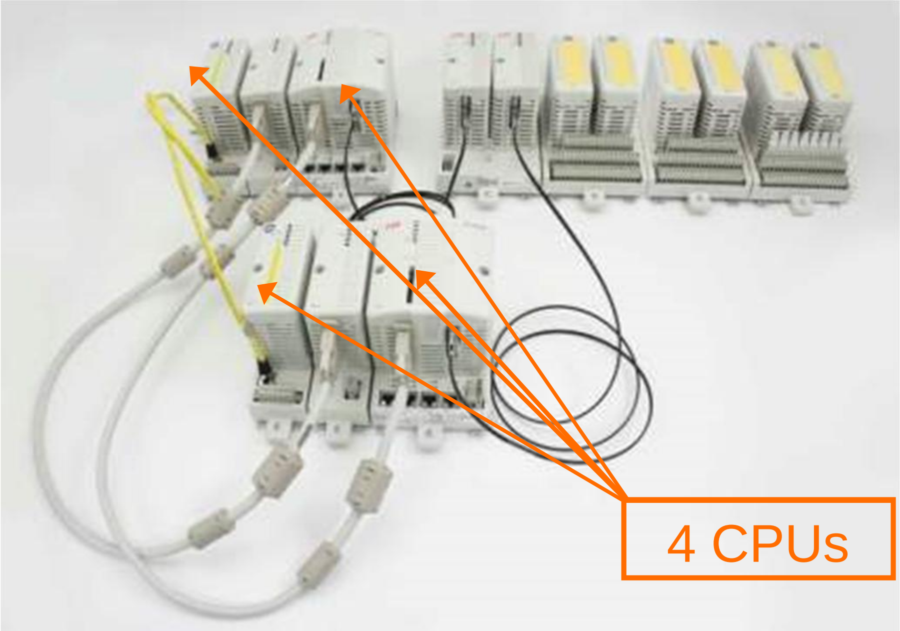
- Two diverse execution paths based on different hardware technology
- Both MCU and FPGA
- Each individual single IO module has an internal 1oo2 architecture

SIL 3 Criteria without Redundancy
Single Configuration

SM811 PM865 TB840 Single I/O AI8880, DI880 and DO880

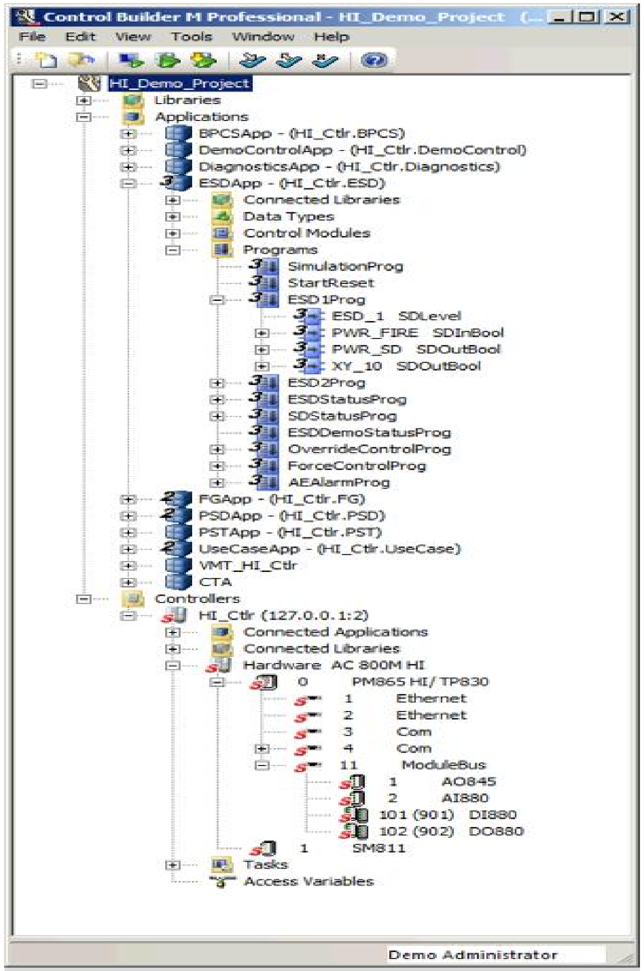


Reliability and Availability
Flexible redundancy options



- 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

Systematic Capabilities: Engineering
SIL Compliant Application Environment



```
HI_Demo_Project
    Libraries
    Applications
        BPCSApp - (HI_Ctlr.BPCS)
        DemoControlApp - (HI_Ctlr.DemoControl)
        DiagnosticsApp - (HI_Ctlr.Diagnostics)
        ESDApp - (HI_Ctlr.ESD)
            Connected Libraries
            Data Types
            Control Modules
            Programs
                SimulationProg
                StartReset
                ESD1Prog
                    ESD_1   SDLevel
                    PWR_FIRE   SDInBool
                    PWR_SD   SDOutBool
                    XY_10   SDOutBool
                ESD2Prog
                ESDStatusProg
                SDStatusProg
                ESDDemoStatusProg
                OverrideControlProg
                ForceControlProg
                AEAlarmProg
        FGApp - (HI_Ctlr.FG)
        PSDApp - (HI_Ctlr.PSD)
        PSTApp - (HI_Ctlr.PST)
        UseCaseApp - (HI_Ctlr.UseCase)
        VMT_HI_Ctlr
        CTA
    Controllers
        HI_Ctlr (127.0.0.1:2)
            Connected Applications
            Connected Libraries
            Hardware  AC 800M HI
                0        PM865 HI/ TP830
                    1        Ethernet
                    2        Ethernet
                    3        Com
                    4        Com
                    11        ModuleBus
                        1        AO845
                        2        AI880
                        101 (901)   DI880
                        102 (902)   DO880
                1        SM811
            Tasks
            Access Variables

Demo Administrator
```

Engineering tool automatically limits user configuration choices to ensure integrity

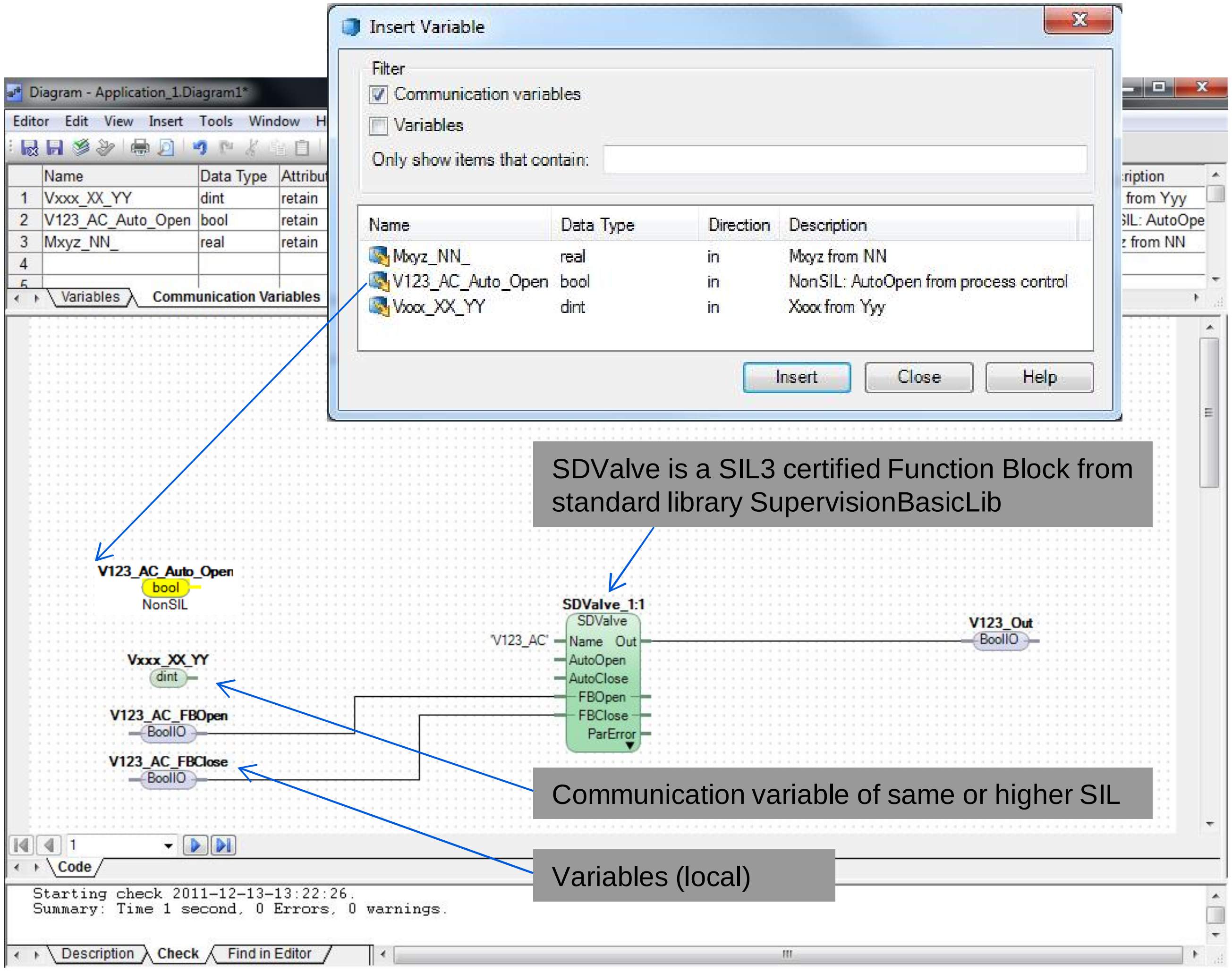
Safety functions protect and control download to the process and runtime environment

- 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

Systematic Capabilities: Engineering
Diagram Editor for SIL Applications



	Name	Data Type	Attribut
1	Vxxx_XX_YY	dint	retain
2	V123_AC_Auto_Open	bool	retain
3	Mxyz_NN_	real	retain
4			
5			

Filter

☑ Communication variables

☐ Variables

Only show items that contain:

Name	Data Type	Direction	Description
Mxyz_NN_	real	in	Mxyz from NN
V123_AC_Auto_Open	bool	in	NonSIL: AutoOpen from process control
Vxxx_XX_YY	dint	in	Xxxx from Yyy

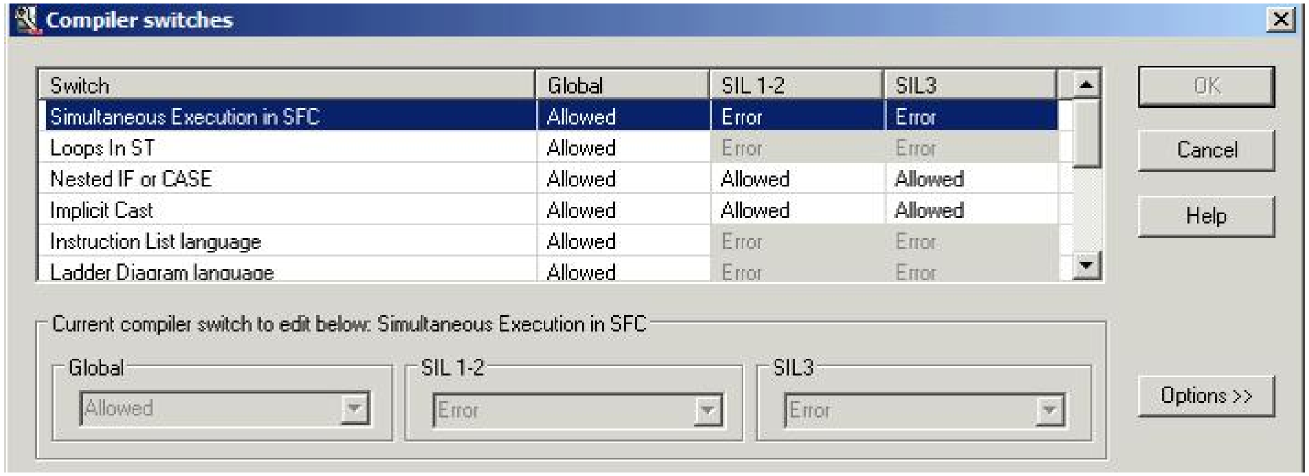
```
Starting check 2011-12-13-13:22:26.
Summary: Time 1 second, 0 Errors, 0 warnings.
```

SDValve is a SIL3 certified Function Block from standard library SupervisionBasicLib

Communication variable of same or higher SIL

Variables (local)

Systematic Capabilities: Engineering
Compiler Restrictions



Switch	Global	SIL 1-2	SIL3
Simultaneous Execution in SFC	Allowed	Error	Error
Loops In ST	Allowed	Error	Error
Nested IF or CASE	Allowed	Allowed	Allowed
Implicit Cast	Allowed	Allowed	Allowed
Instruction List language	Allowed	Error	Error
Ladder Diagram language	Allowed	Error	Error

Current compiler switch to edit below: Simultaneous Execution in SFC

Global: Allowed

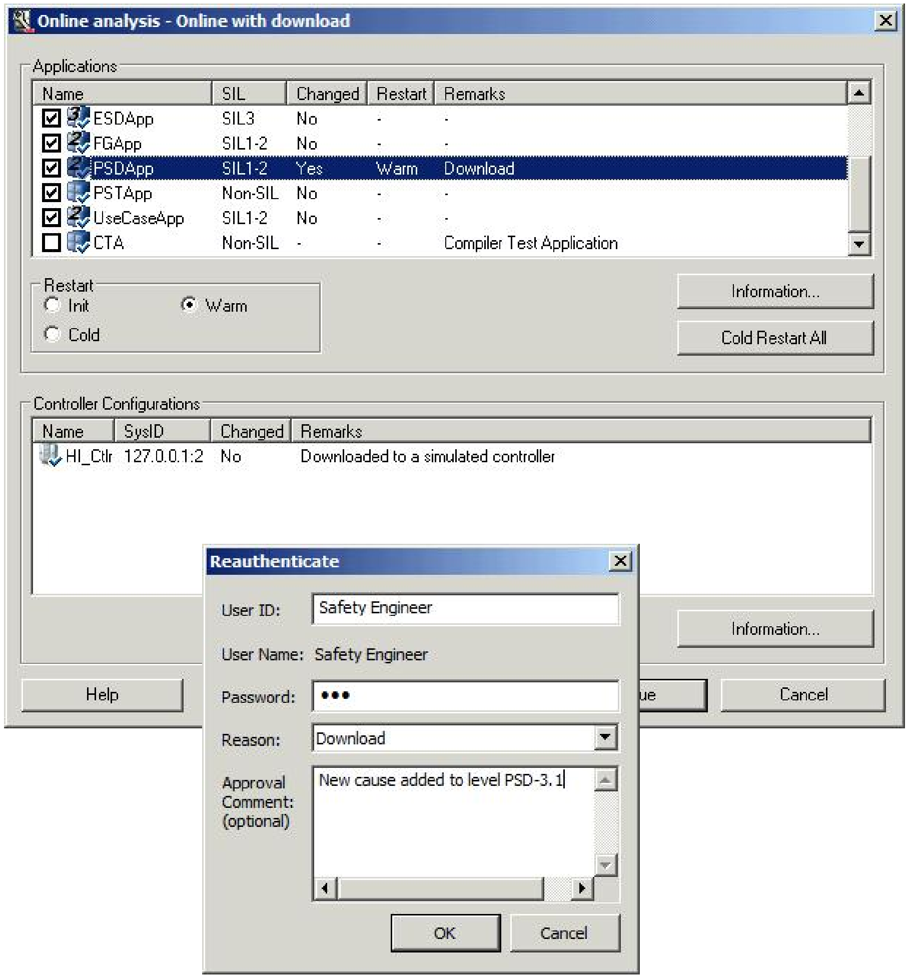
SIL 1-2: Error

SIL3: Error

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

Systematic Capabilties: Engineering
On-line changes

- Online changes can be downloaded to the controller without interfering with the running process
  - Trip limit change
  - Hardware settings
  - Logic
- Downloads are protected by “Access enable” function
- Re-authentication can be configured to ensure that the user is authorized
  - This is also recorded in the audit trail



Online analysis - Online with download

Applications

	Name	SIL	Changed	Restart	Remarks
☑	ESDApp	SIL3	No	-	-
☑	FGApp	SIL1-2	No	-	-
☑	PSDApp	SIL1-2	Yes	Warm	Download
☑	PSTApp	Non-SIL	No	-	-
☑	UseCaseApp	SIL1-2	No	-	-
☐	CTA	Non-SIL	-	-	Compiler Test Application

Restart: ○ Init ● Warm ○ Cold

Controller Configurations

Name	SysID	Changed	Remarks
HI_Ctlr	127.0.0.1:2	No	Downloaded to a simulated controller

Reauthenticate

User ID: Safety Engineer

User Name: Safety Engineer

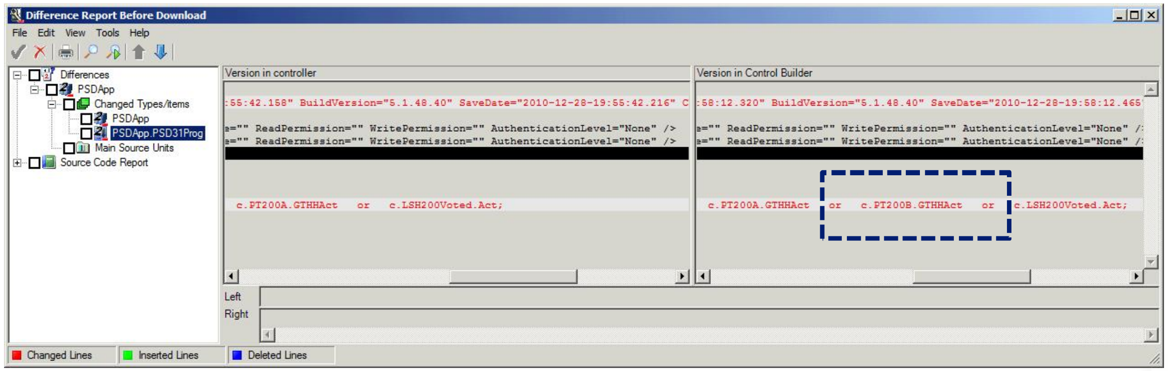
Password: •••

Reason: Download

Approval Comment: (optional) New cause added to level PSD-3.1

Live Code Evaluation: 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



Version in controller

```
:55:42.158" BuildVersion="5.1.48.40" SaveDate="2010-12-28-19:55:42.216" C

="" ReadPermission="" WritePermission="" AuthenticationLevel="None" />
="" ReadPermission="" WritePermission="" AuthenticationLevel="None" />
[redacted]


 c.PT200A.GTHHAct   or   c.LSH200Voted.Act;
```

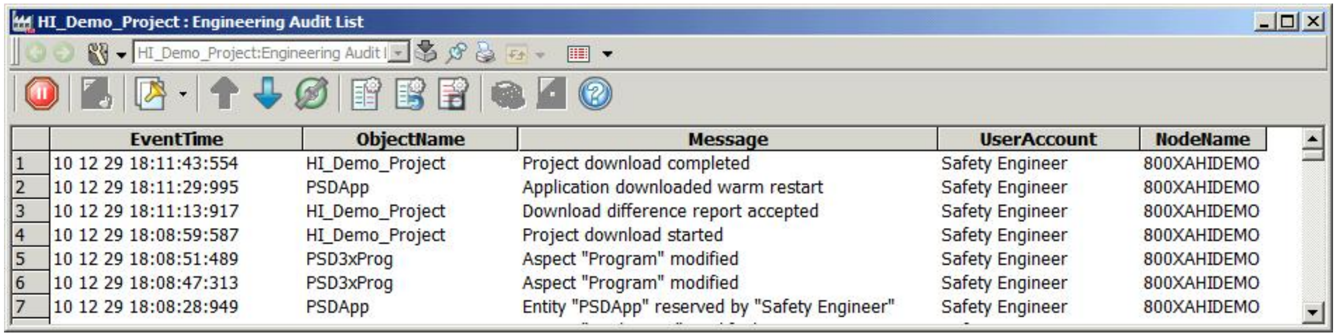
Version in Control Builder

```
:58:12.320" BuildVersion="5.1.48.40" SaveDate="2010-12-28-19:58:12.465

="" ReadPermission="" WritePermission="" AuthenticationLevel="None" /:
="" ReadPermission="" WritePermission="" AuthenticationLevel="None" /:
[redacted]


 c.PT200A.GTHHAct   or   c.PT200B.GTHHAct   or  c.LSH200Voted.Act;
```

Live Code Evaluation
Audit Trail

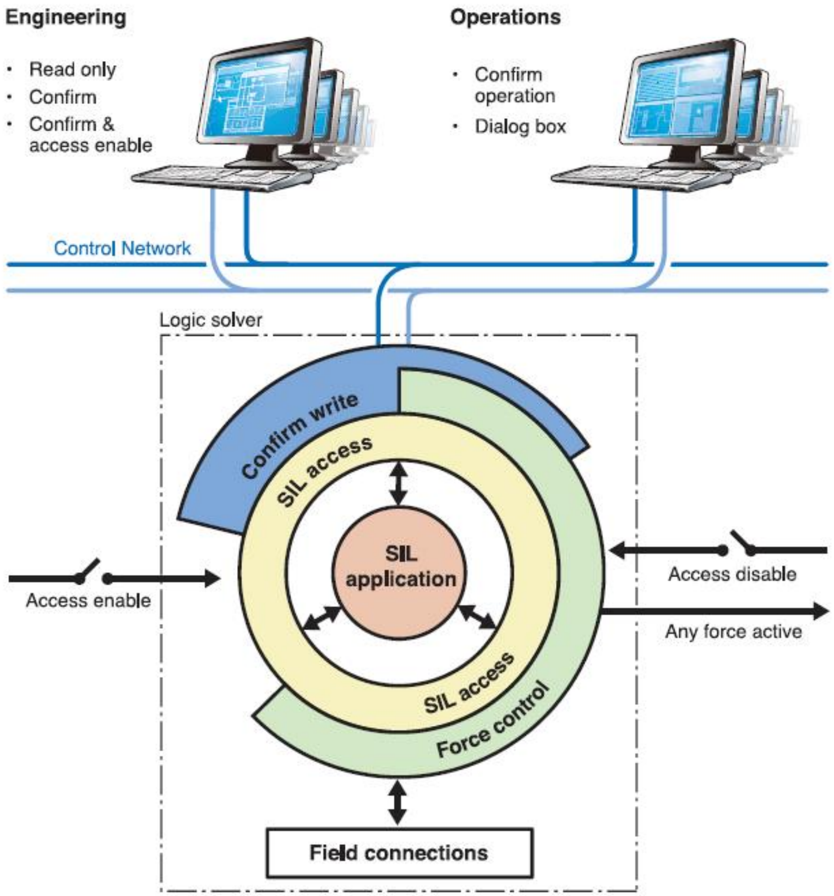
- Enables audit of all operator and engineering actions
- Possible to disabled during commissioning
- Audit actions examples
  - Configuration changed
  - Signal forced
  - Download
  - Reserved/Released

- Audit log contains:
  - Date and time
  - Node information
  - User name of the individual performing the operation
  - Type of operation
  - Object, property or aspect affected by the operation


HI_Demo_Project : Engineering Audit List
HI_Demo_Project:Engineering Audit l

	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

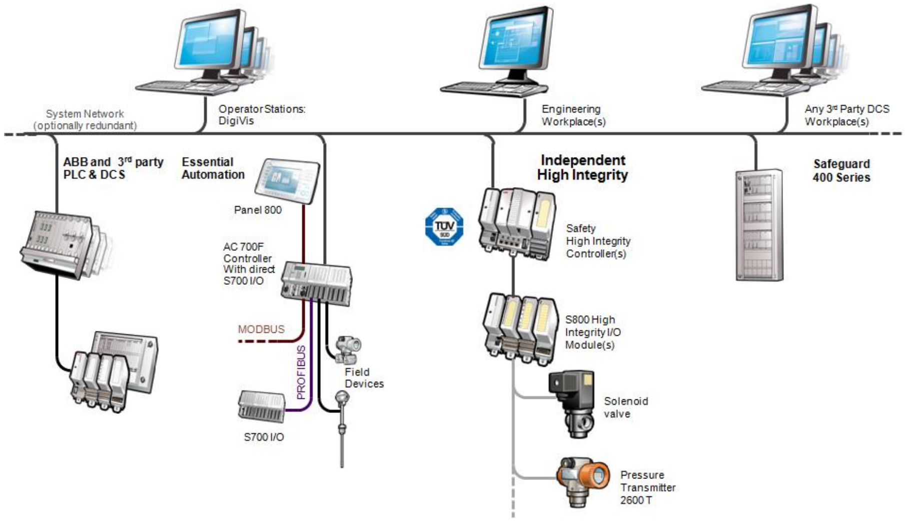
Security
System Security And Embedded Firewalls



- 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

Independent High Integrity
Connectivity and Interfacing

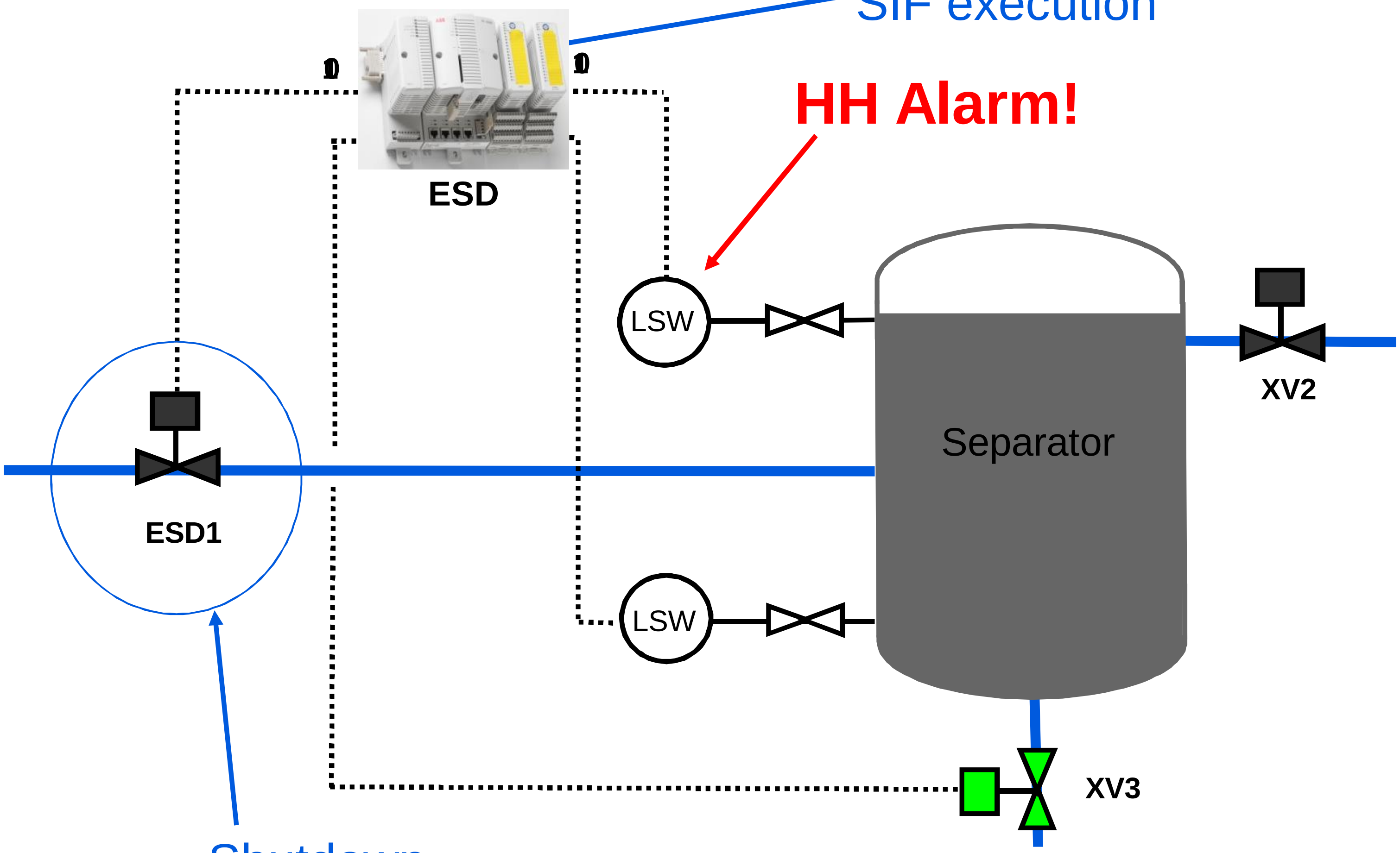
- Available protocols…
  - Safety Peer to Peer
  - OPC
  - ABB protocols
  - Modbus TCP *
  - RS232 *
- ..to connect to..
  - AC800M HI controllers
  - Process panels
  - ABB or 3rd party DCS & PLC
  - 3rd party HMI software



* Planned for a future release

Typical Applications

Emergency Shutdown Systems - ESD
PSD - Primary Protections LAHH

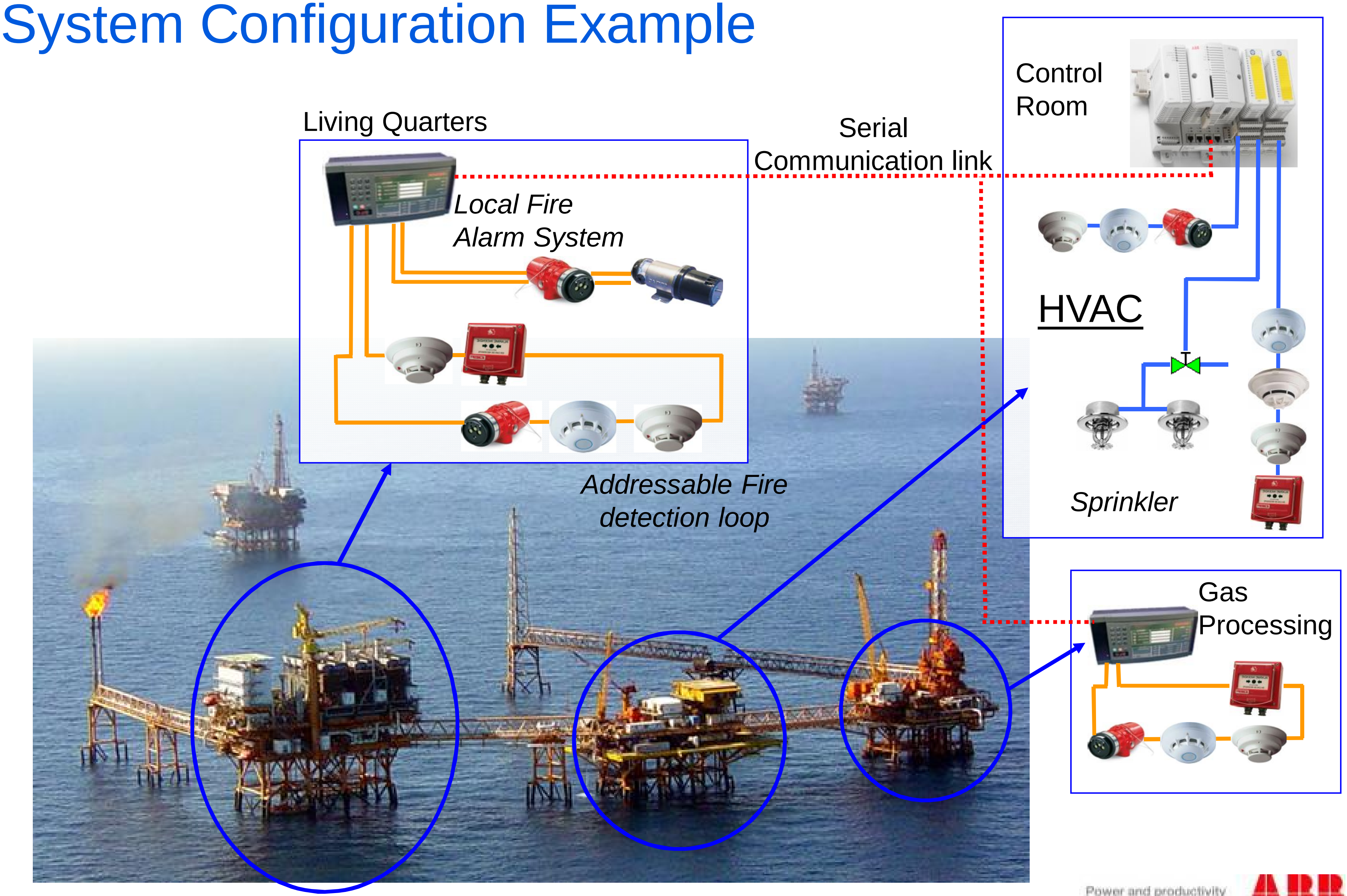


SIF execution

HH Alarm!

Shutdown Executed

Fire & Gas System – F&G System Configuration Example



Living Quarters

Local Fire Alarm System

Serial Communication link

Control Room

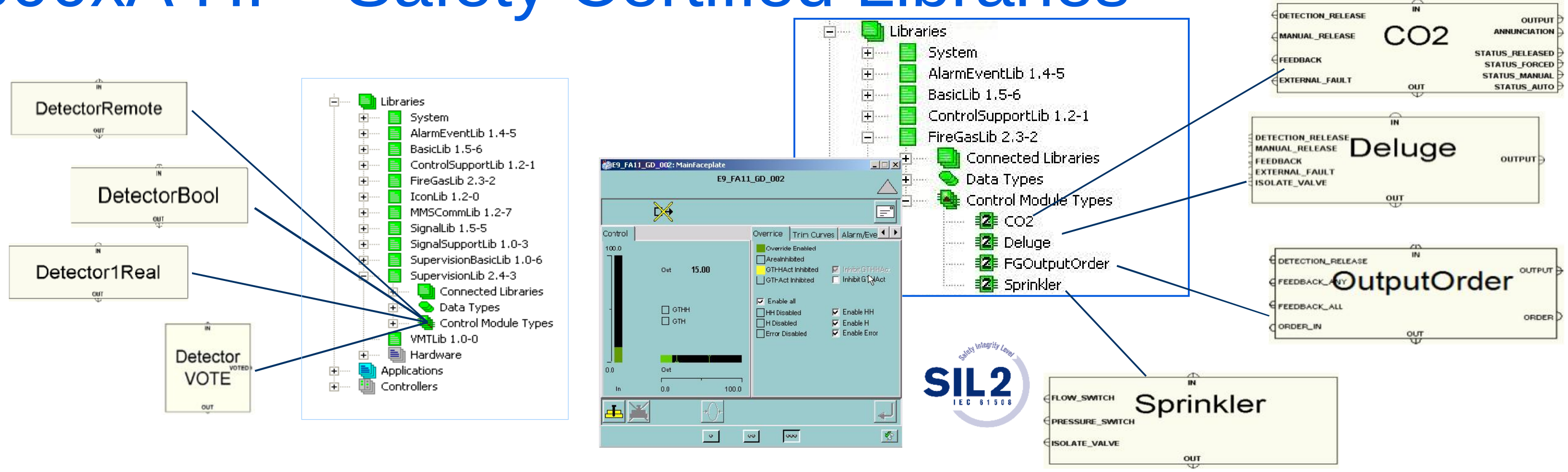
HVAC

Sprinkler

Addressable Fire detection loop

Gas Processing

Fire & Gas System
800xA HI – Safety Certified Libraries



Libraries
- System
- AlarmEventLib 1.4-5
- BasicLib 1.5-6
- ControlSupportLib 1.2-1
- FireGasLib 2.3-2
- IconLib 1.2-0
- MMSCommLib 1.2-7
- SignalLib 1.5-5
- SignalSupportLib 1.0-3
- SupervisionBasicLib 1.0-6
- SupervisionLib 2.4-3
  - Connected Libraries
  - Data Types
  - Control Module Types
- VMTLib 1.0-0
- Hardware

Applications

Controllers

E9_FA11_GD_002: MainFaceplate

E9_FA11_GD_002

Control | Overrice | Trim Curves | Alarm/Eve

Out 15.00

□ GTHH
□ GTH

🟩 Override Enabled
□ AreaInhibited
🟨 GTHHAct Inhibited ☑ Inhibit GTHHAct
□ GTHAct Inhibited □ Inhibit GTHAct

☑ Enable all
□ HH Disabled ☑ Enable HH
□ H Disabled ☑ Enable H
□ Error Disabled ☑ Enable Error

Libraries
- System
- AlarmEventLib 1.4-5
- BasicLib 1.5-6
- ControlSupportLib 1.2-1
- FireGasLib 2.3-2
  - Connected Libraries
  - Data Types
  - Control Module Types
    - CO2
    - Deluge
    - FGOutputOrder
    - Sprinkler

- 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

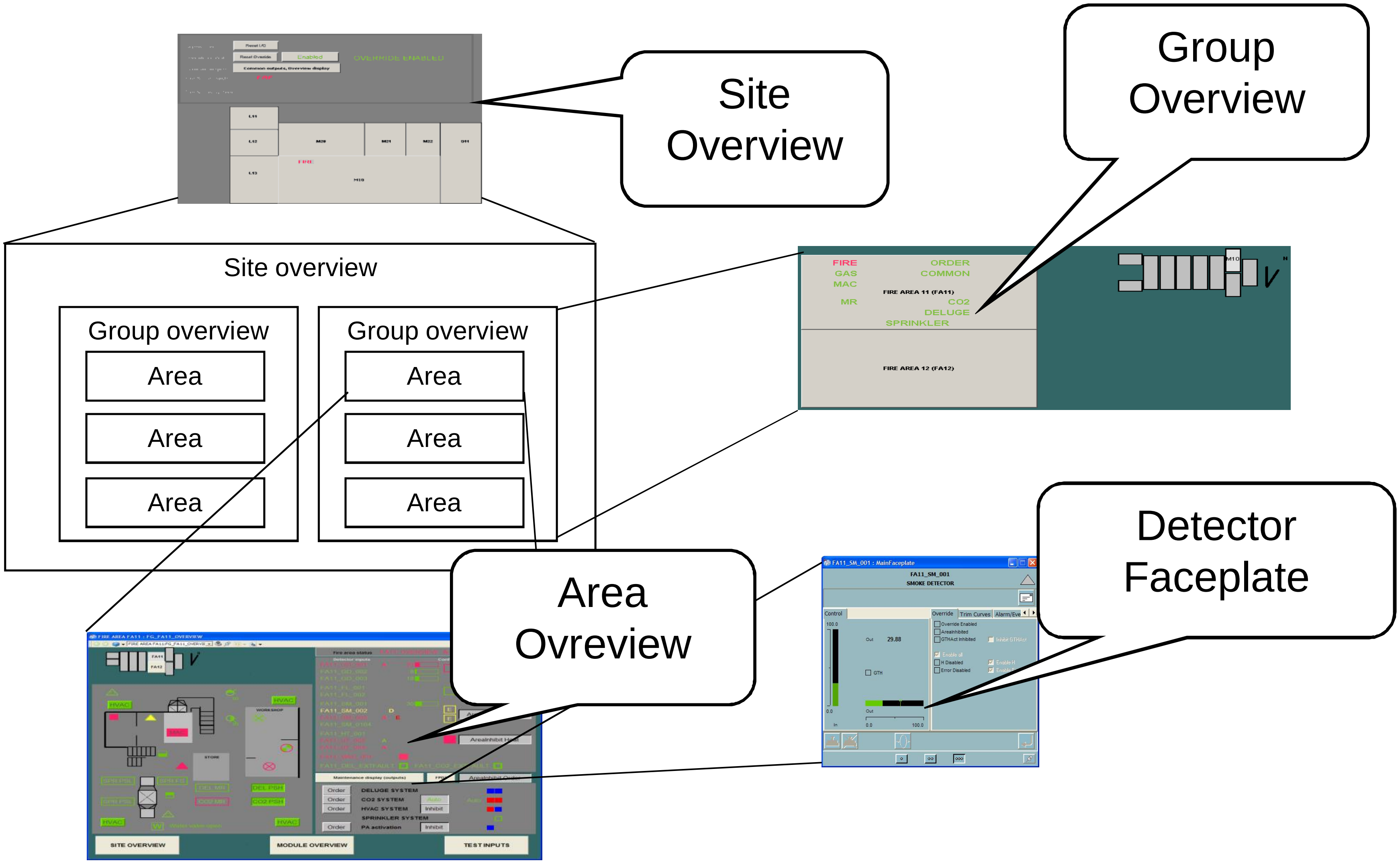
Deluge

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



Site Overview

Group Overview

Detector Faceplate

Area Ovreview

Site overview

Group overview

Area

Area

Area

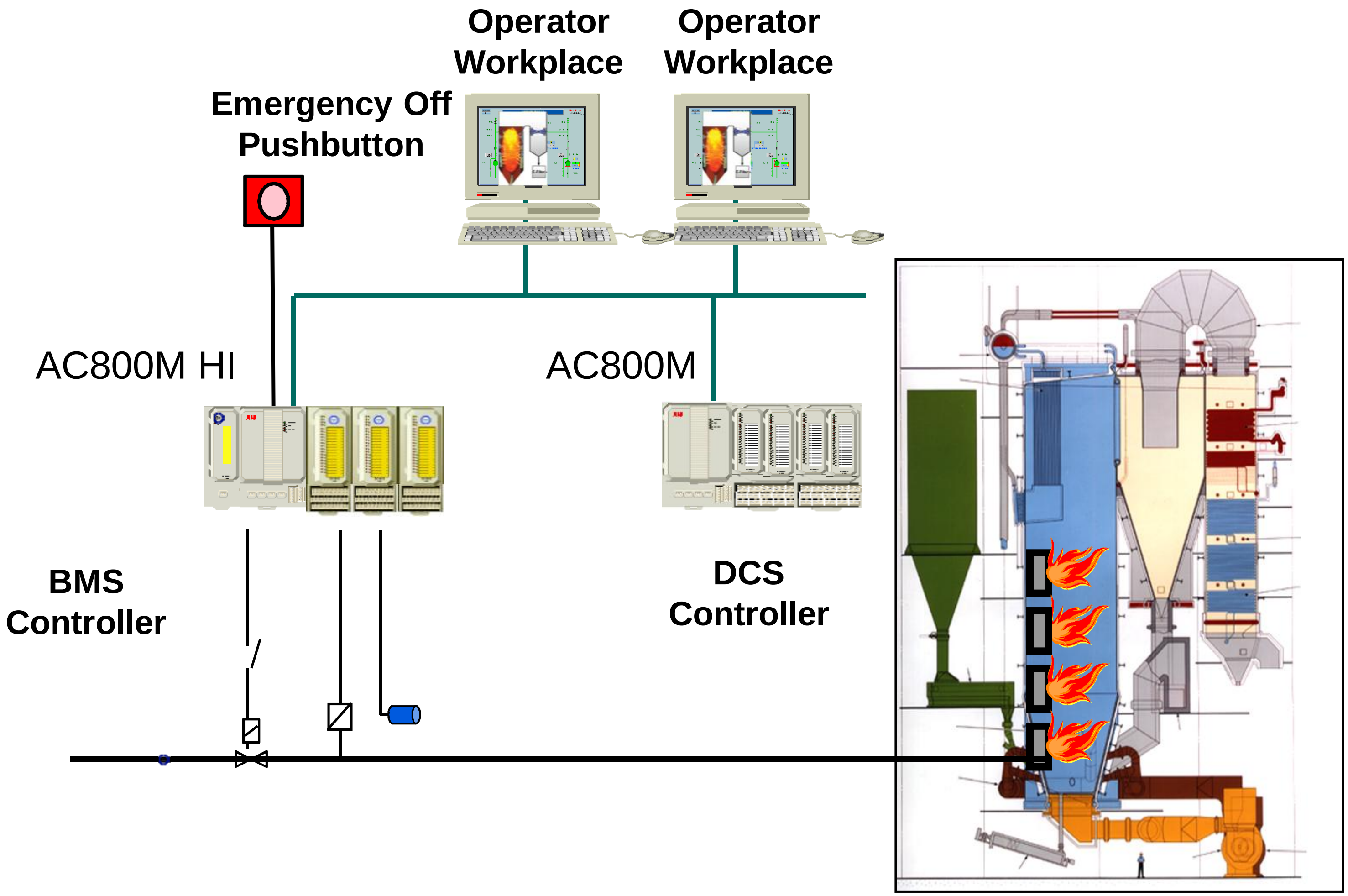
Group overview

Area

Area

Area

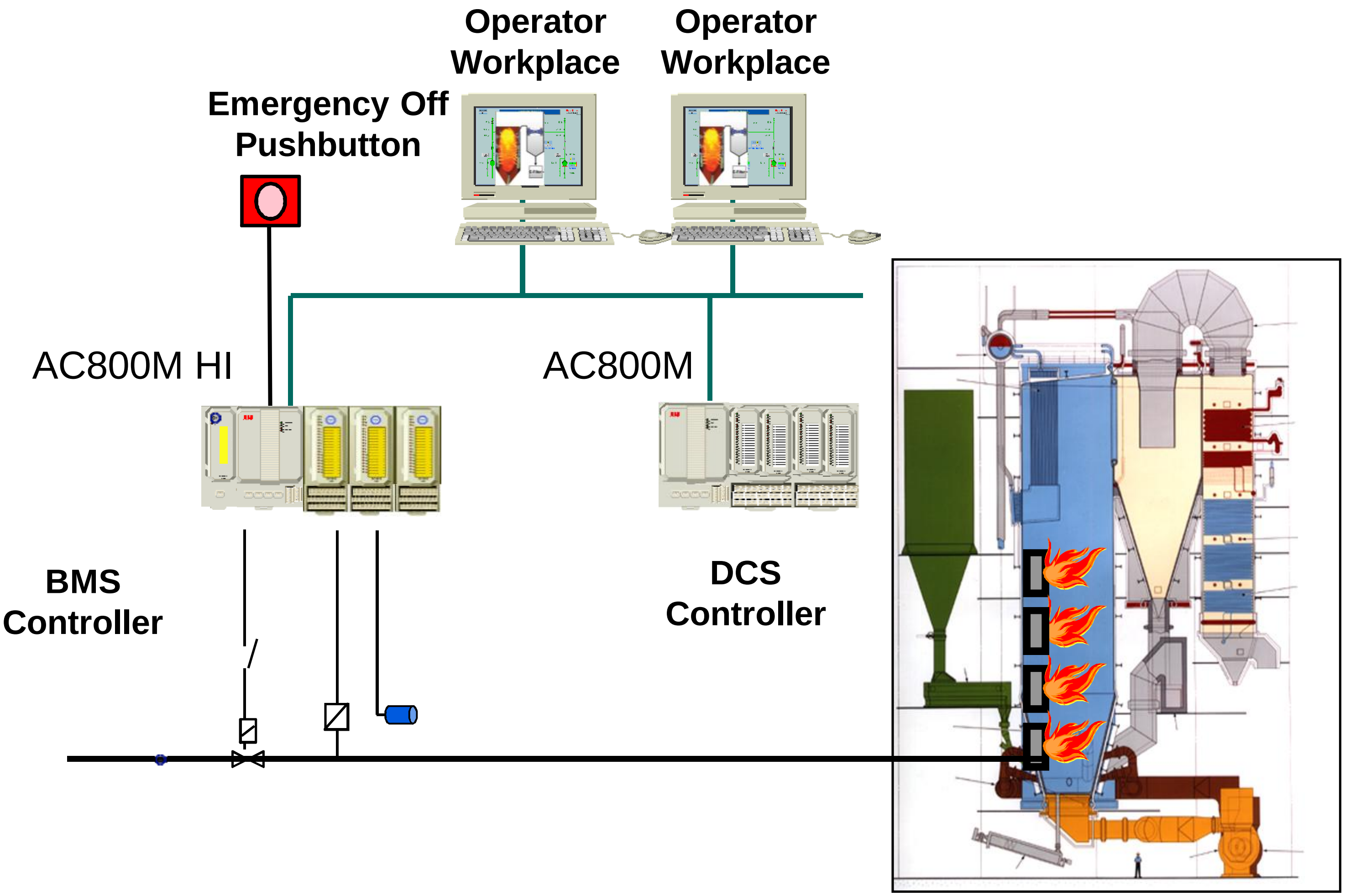
Boiler Management System – BMS
800xA HI - Example System Configuration



BMS and Burner Library

Power and productivity
for a better world™

Boiler Management System – BMS
800xA HI - Example System Configuration



Operator Workplace

Operator Workplace

Emergency Off Pushbutton

AC800M HI

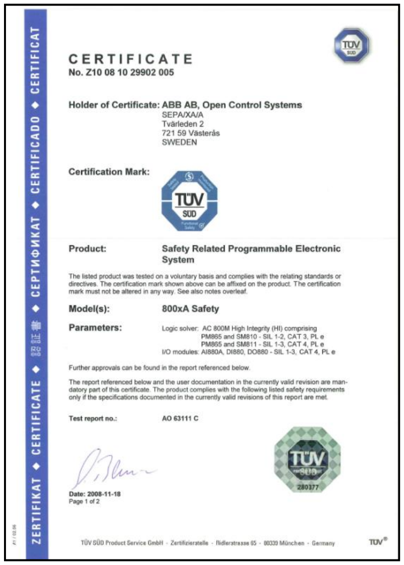
AC800M

BMS Controller

DCS Controller

Burner Management Systems
Benefits of Library

- Reduce engineering effort
  - Use of compliant building blocks
  - Increase consistency across applications
  - Increase flexibility and reduce documentation
- Reduce certification effort over the installation lifecycle
  - Library has Letter of Conformance by TÜV
  - Documentation is according to standard
    - Safety Manual
- Improves operation



ZERTIFIKAT ◆ CERTIFICATE ◆ [illegible] ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE
No. Z10 08 10 29902 005

Holder of Certificate: **ABB AB, Open Control Systems**
SEPA/XA/A
Tvärleden 2
721 59 Västerås
SWEDEN

Certification Mark:

Product: **Safety Related Programmable Electronic System**

The listed product was tested on a voluntary basis and complies with the relating standards or directives. The certification mark shown above can be affixed on the product. The certification mark must not be altered in any way. See also notes overleaf.

Model(s): **800xA Safety**

Parameters:
Logic solver: AC 800M High Integrity (HI) comprising
PM865 and SM810 - SIL 1-2, CAT 3, PL e
PM865 and SM811 - SIL 1-3, CAT 4, PL e
I/O modules: AI880A, DI880, DO880 - SIL 1-3, CAT 4, PL e

Further approvals can be found in the report referenced below.

The report referenced below and the user documentation in the currently valid revision are mandatory part of this certificate. The product complies with the following listed safety requirements only if the specifications documented in the currently valid revisions of this report are met.

Test report no.: **AO 63111 C**

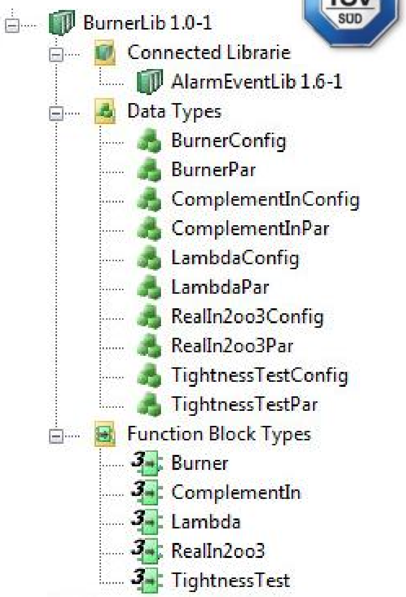
280377

Date: 2008-11-18
Page 1 of 2

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstrasse 65 · 80339 München · Germany

Burner Management System
BurnerLib

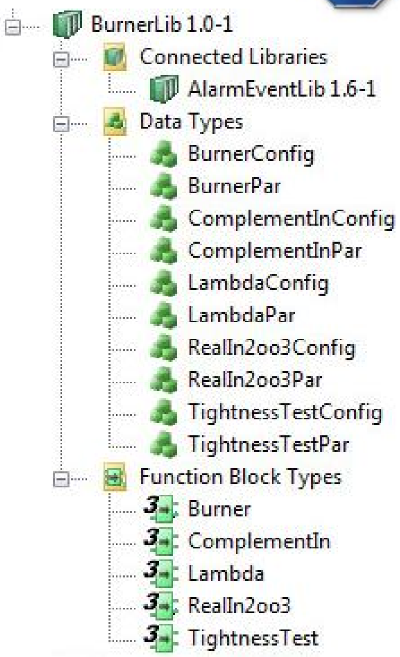
- AC800M High Integrity Burner Management Library (BurnerLib) is fully integrated.
- Contains five SIL 3 classified function block types to implement complete Burner Management applications.
- Includes complete control over startup and operation.
- Has built in Alarm Handling, Faceplates and Display Elements.
- Satisfies most relevant standards.
- Allows complete visualization of the process (No more “black box”).



- BurnerLib 1.0-1
  - Connected Librarie
    - AlarmEventLib 1.6-1
  - Data Types
    - BurnerConfig
    - BurnerPar
    - ComplementInConfig
    - ComplementInPar
    - LambdaConfig
    - LambdaPar
    - RealIn2oo3Config
    - RealIn2oo3Par
    - TightnessTestConfig
    - TightnessTestPar
  - Function Block Types
    - Burner
    - ComplementIn
    - Lambda
    - RealIn2oo3
    - TightnessTest

Burner Management System, BMS
Function Block Types

- Burner
  - Start-up sequence and supervision of Burner
- Complement.In
  - Monitor quality of Boolean inputs
  - Detect short-circuit and open-circuit
- Lambda
  - Calculation of air/fuel ratio
- Real.In2oo3
  - 2 out of 3 voting function for Real inputs
- TightnessTest
  - Tightness test for gas supply valves
- Datatypes and Connected Libraries



- BurnerLib 1.0-1
  - Connected Libraries
    - AlarmEventLib 1.6-1
  - Data Types
    - BurnerConfig
    - BurnerPar
    - ComplementInConfig
    - ComplementInPar
    - LambdaConfig
    - LambdaPar
    - RealIn2oo3Config
    - RealIn2oo3Par
    - TightnessTestConfig
    - TightnessTestPar
  - Function Block Types
    - Burner
    - ComplementIn
    - Lambda
    - RealIn2oo3
    - TightnessTest

What does it mean for you?
AB Tändkulan – Interview

What are the benefits of ABB products and systems for this application?	A fully integrated burner management system
What is the benefit of using a library for this application?	Certified Function Blocks and easier approval.
Can you describe the technical benefits of this approach?	No need for “black box” solutions or communication interfaces.
Have you measured any economic benefits of this approach?	This was the 1st installation, we expect to benefit on upcoming projects. Easier cooperation with assessor

Summary

Summary

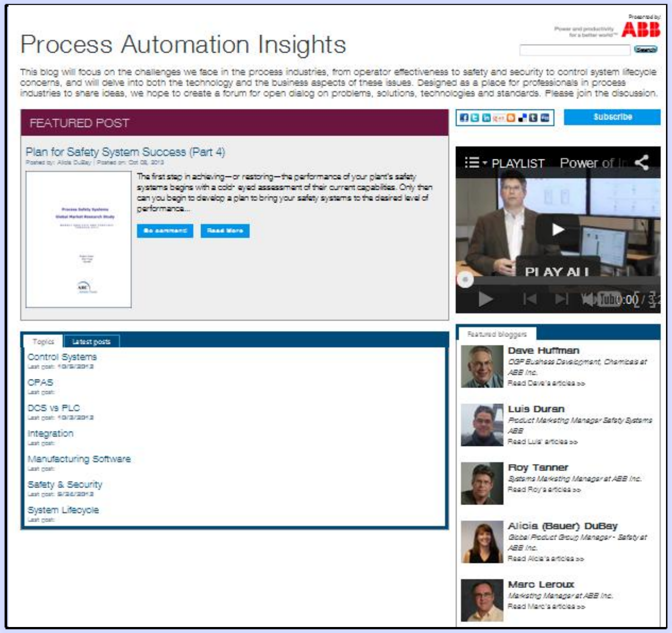
- Reliable hardware is not enough
- Need to look at
  - What is the risk, and how can it be reduced
  - How to avoid failures
  - Entire lifecycle to be considered
  - Work processes established for each phase in the lifecycle
- Importance of Competence
- SIL is applicable for a function not for a component alone

Questions & Answers

Where to find information?

Where to find information
Resources and Communication

- www.abb.com
- ABB's Power of Integration Knowledge Center
- Safety Channel on Process Automation YouTube site
- Safety eGuides



Presented by:

Power and productivity for a better world™ ABB

Process Automation Insights

Search

This blog will focus on the challenges we face in the process industries, from operator effectiveness to safety and security to control system lifecycle concerns, and will delve into both the technology and the business aspects of these issues. Designed as a place for professionals in process industries to share ideas, we hope to create a forum for open dialog on problems, solutions, technologies and standards. Please join the discussion.

FEATURED POST

Plan for Safety System Success (Part 4)

Posted by: Alicia DuBay | Posted on: Oct 08, 2013

The first step in achieving—or restoring—the performance of your plant's safety systems begins with a cold- eyed assessment of their current capabilities. Only then can you begin to develop a plan to bring your safety systems to the desired level of performance...

Be comment | Read More

Subscribe

PLAYLIST Power of I

PLAY ALL

0:00 / 3:

Topics | Latest posts

Control Systems
Last post: 10/8/2013

CPAS
Last post:

DCS vs PLC
Last post: 10/3/2013

Integration
Last post:

Manufacturing Software
Last post:

Safety & Security
Last post: 9/24/2013

System Lifecycle
Last post:

Featured bloggers

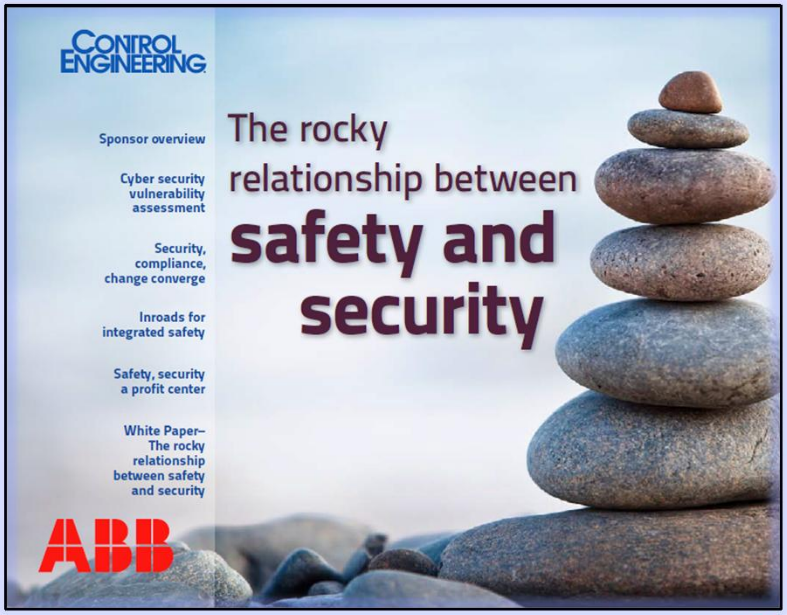
Dave Huffman
OGP Business Development, Chemicals at ABB Inc.
Read Dave's articles >>

Luis Duran
Product Marketing Manager Safety Systems ABB
Read Luis' articles >>

Roy Tanner
Systems Marketing Manager at ABB Inc.
Read Roy's articles >>

Alicia (Bauer) DuBay
Global Product Group Manager - Safety at ABB Inc.
Read Alicia's articles >>

Marc Leroux
Marketing Manager at ABB Inc.
Read Marc's articles >>



CONTROL ENGINEERING

Sponsor overview

Cyber security vulnerability assessment

Security, compliance, change converge

Inroads for integrated safety

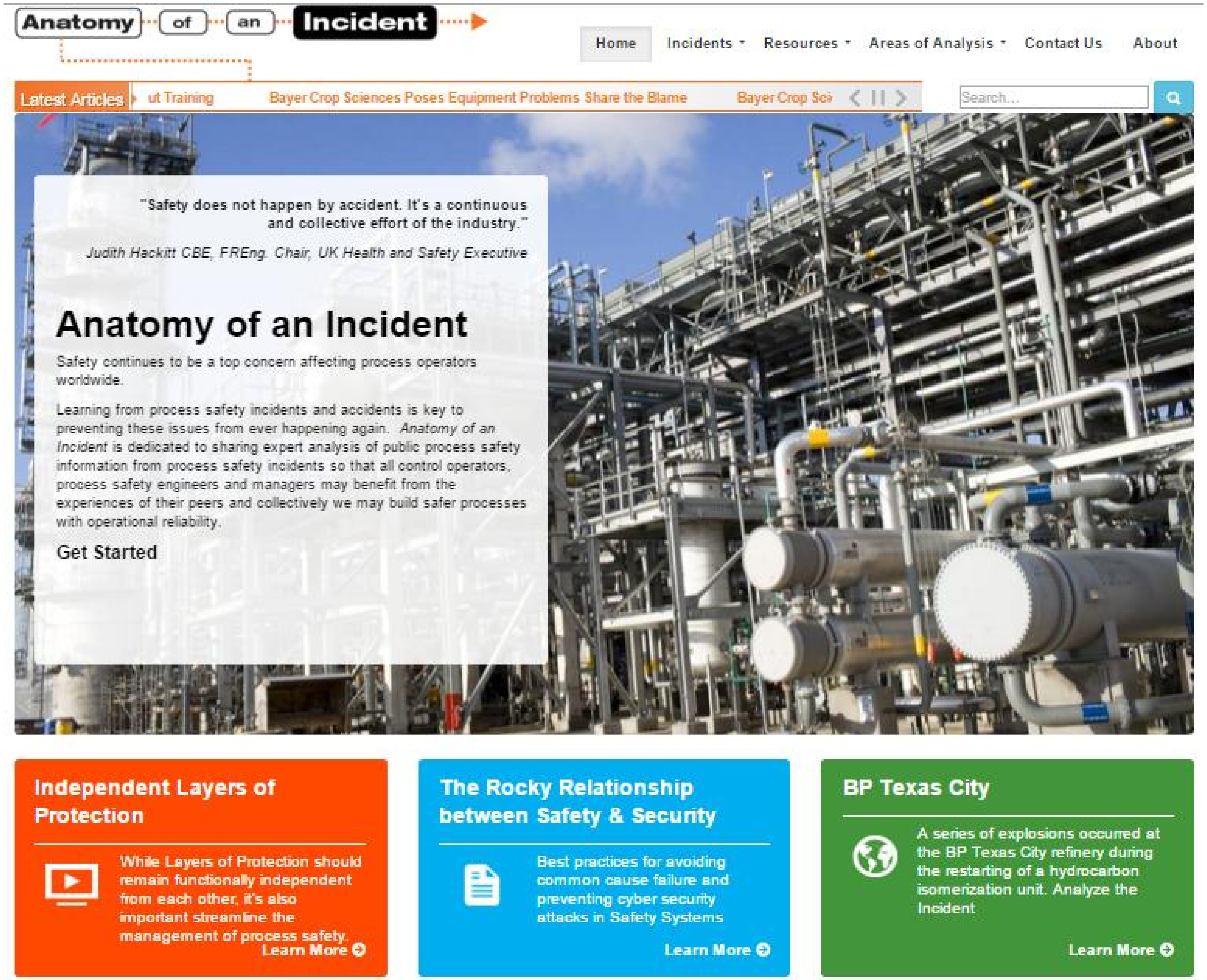
Safety, security a profit center

White Paper– The rocky relationship between safety and security

ABB

The rocky relationship between **safety and security**

Where to find information
Resources and Communication



"Safety does not happen by accident. It's a continuous and collective effort of the industry."

Judith Hackitt CBE, FREng. Chair, UK Health and Safety Executive

Anatomy of an Incident

Safety continues to be a top concern affecting process operators worldwide.

Learning from process safety incidents and accidents is key to preventing these issues from ever happening again. *Anatomy of an Incident* is dedicated to sharing expert analysis of public process safety information from process safety incidents so that all control operators, process safety engineers and managers may benefit from the experiences of their peers and collectively we may build safer processes with operational reliability.

Get Started

Independent Layers of Protection

While Layers of Protection should remain functionally independent from each other, it's also important streamline the management of process safety.

Learn More

The Rocky Relationship between Safety & Security

Best practices for avoiding common cause failure and preventing cyber security attacks in Safety Systems

Learn More

BP Texas City

A series of explosions occurred at the BP Texas City refinery during the restarting of a hydrocarbon isomerization unit. Analyze the Incident

Learn More

Power and productivity
for a better world™

ABB