—

ABB Ability™ System 800xA
Safety Overview

Introduction

ABB has over 35 years of experience in the design, manufacture and implementation of process safety systems. With operations on all continents and dedicated safety system teams around the world, ABB provides not only highlyqualified technical resources during project delivery, but also ensures competent local support and service in operation.

The ABB Ability™ System 800xA High Integrity safety system was released in 2005 and is TÜV certified for SIL 3 operation according to IEC 61508 and IEC 61511.Through System 800xA's common operations, engineering and information environment for Basic Process Control Systems (BPCS) and Safety Instrumented Systems (SIS), ABB provides safety solutions that are easily scalable from a few loops to completely integrated safety systems.

In addition to standard safety system functionality, ABB's High Integrity safety system includes a comprehensive array of extended automation components such as faceplates, graphic elements, trends, document links and alarms and events.

The industry leading 800xA Extended Operator Workplace provides a unique collaborative operator environment that can include process, safety and electrical control functionality. This common environment ensures efficient operator response to both normal and abnormal conditions.

As part of the System 800xA extended automation solution, the High Integrity safety system is tailored for a wide range of industry applications including:

- Emergency and Process Shutdown (ESD and PSD)
- Interlock Systems
- Burner Management/ Boiler Protection (BMS)
- Fire and Gas (F&G) Systems
- High Pressure Protection Systems (HIPPS)

The 800xA Safety Offering as described in this document includes:

- Flexible diverse system architecture
- Powerful integrated control and safety functions
- Safety lifecycle services
- Complete SIS portfolio and experience

—

Safety Lifecycle

With increasing acceptance and implementation of 'smart' safety automation technologies, the process industries are experiencing a revolution. To meet their functional safety management requirements, end-users now demand closer integration of their safety and control systems, safety functions at varying process states, and flexibility, scalability, and reusability of their safety components.

With a wide variety of options available, the challenge is to determine the safest, most reliable and cost effective safety instrumented system (SIS). The standards provide some guidance, but by engaging ABB during all phases of the safety lifecycle, we can help you choose the right solution for your safety and business needs.

Determine the Safety Requirements
Due to the complexity of the hazards in the process industry, it is required that a systematic process is used to identify all foreseeable major accidents. ABB offers a proven set of techniques and methods to enable identification of hazards, assessment of risks, and determination of appropriate risk reduction strategies.

Our hazard study methodology includes the following techniques:

• HAZOP (Hazard and Operability) Studies
• Past accident and incident reviews
• FMEA (Failure Mode and Effects Analysis)
• Industry checklists
• Process Hazard Review (PHR)

• SIL Determination
• Human Factors Assessment

Design, Engineer and Build the SIS
ABB's engineering environment provides graphical design of the entire SIS loop – from field inputs and logic solver to the safety loop's final elements. We provide a comprehensive library of standard reusable TÜV certified components. These pretested proven libraries significantly reduce the time required to engineer, test, and maintain safety applications, while minimizing project risks.

SIL Achievement is a demonstration that for each Safety Instrumented Function, the target SIL, as derived from SIL Determination, has been met in accordance with the requirements of IEC61508. As part of our TÜV certificate, safety systems integration and engineering services, we perform SIL Achievement using proven methodologies and provide comprehensive reports of the results.

Only when a safety instrumented function meets the criteria set by IEC 61508 in terms of architectural constraint, target failure measure and systematic capability, can the target SIL be said to be achieved.

—

Reducing risk through High Integrity Safety Automation

ABB Ability™ System 800xA improves process availability while reducing the risk to overall plant operation by providing a common environment for production control, safety supervision and production monitoring. Within this environment, System 800xA offers a complete Safety Instrumented System (SIS) solution, complying with the IEC 61508 and IEC 61511 standards. ABB offers, as part of our standard portfolio, not only the logic solver, but TÜV certified equipment for the entire safety loop, consisting of field instruments, safety controllers and final control elements (positioners).

The Integrated Control and Safety System (ICSS) based on System 800xA and it's Aspect Object Technology brings significant benefits to end users. One of the main benefits being risk reduction in each phase of the ICSS systems lifecycle including Engineering, Installation and Commissioning, and Operation and Maintenance. Risk reduction can be achieved in the following areas:

Engineering
- Reuse of components via certified Libraries
- Engineering tool limits programming choices to assure safety integrity and standards compliance
- Compiler restrictions ensure correctly compiled code is downloaded to safety controller

Product (High Integrity Safety)
- Diverse architecture and diverse implementation
- Elimination of common cause failures
- Redundancy for high availability and hot swap
- Certified remote I/O solution for flexible installation
- Specific SIL3 IO interfaces to fullfill the most demanding industry applications

Operations
- Single operator environment with personalized workplaces for timely response to abnormal conditions
- Consolidated alarms and events for ICSS
- Built in, TÜV certified override capability

Maintenance
- Standard certified interfaces between DCS, safety, alarm and events, history, asset management etc.
- Validation of changes against live I/O prior to download (load-evaluate-go function)
- Re-authentication for maintenance features including confirmed online write
- Built in partial valve stroke testing
- Difference report and audit trail for root cause analysis

Integrated Process Control and Safety

The ABB Ability™ System 800xA extended automation system has been designed from the beginning as an integrated control and safety system. It's High Integrity component is a "next generation" safety system built according to the requirements of IEC 61508 Edition 2. Not only does the 800xA High Integrity safety system meet the traditional safety requirements of hardware safety integrity and behavior in the presence of a fault condition, it has been specifically designed to also focus on enhanced diagnostic coverage, diversity, and systematic safety integrity.
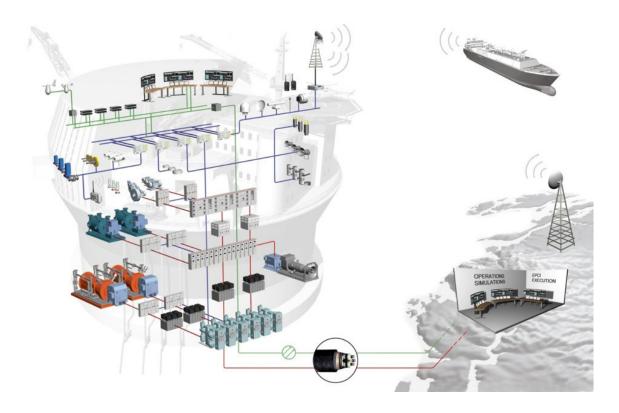
The Benefits of Integration
The operational aspects of safety systems are under increased scrutiny. Beyond the purely financially benefits (which focus on reducing operational cost throughout the system lifecycle) the real driver is safer operations.

The industry is struggling with increased system complexity. A larger number of systems in any given plant, combined with a competence pool that is depleting through retirement, 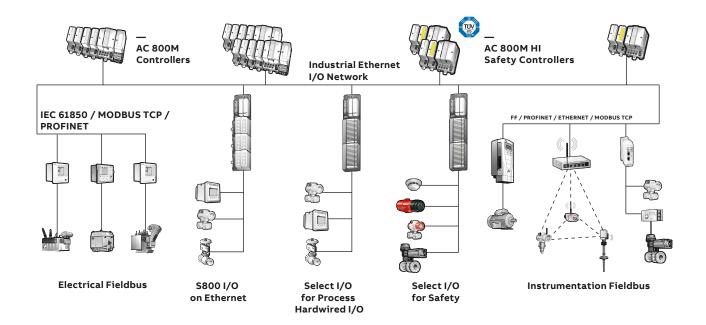increases the risk of safety critical mistakes. An obvious counter-measure to negate this risk is a reduction in both system complexity and number of systems employed.

By installing an integrated control and safety system, the following operational benefits can be achieved:

• A single process automation platform in the facility provides:
• One operator interface for operations to learn and operate
• One engineering tool for programmers to learn
• One hardware platform for maintenance to maintain
• Field instrumentation wired to the common system
• Less field splitting and communications required
• Easier design and field wiring
• All ICSS information seamlessly available for both the DCS and Safety system
• Automated SIS bypasses and enables can be used to coordinate with process operations
• Optional integration of process and safety applications into the same controller reduces cost and communications complexity

ABB Ability™ System 800xA Flexible I/O solution

ABB's System 800xA High Integrity has a flexible and diverse architecture, which not only meets the requirements of the safety standards, but can address almost any architecture required for project implementation. The available configurations include:

- Integrated (separate process and safety controllers on the same control network)
- Combined (process and safety applications in the same physical controller)
- Separate (separate process and safety controllers on separate networks with a hardwired or direct communication link between controllers)
- Independent (the high integrity controller can be used with any HMI or DCS system separate from System 800xA)

These available options enable users to implement their preferred architecture using the proven certified 800xA High Integrity solution.
——

It is the diversity of both architecture and product implementation that enables 800xA High Integrity to be certified by TÜV according to IEC 61508 Edition for SIL 3

without resorting to redundancy. Redundancy is available when high availability or hot swap are required.

System 800xA High Integrity's diversity comes from a combi-nation of technology and implemen-tation. The specific measures implemented (to achieve systematic safety integrity per the standards) are described below:

Product Diversity
- Diverse application execution engine in the controller and safety module
- Diverse architecture (MCU & FPGA) in I/O modules
- Use of different toolsets during design and implementation
- Different manufacturers of electronic compo-nents

Development / Implementation Diversity
- Application of rigorous TÜV certified Functional Safety Management System
- V-Model implementation
- Coding Guidelines
- Independent development and validation teams (Malmo and Vasteras, Sweden)

TÜV certified to industry standards

System 800xA High Integrity is designed, delivered and supported in accordance with the latest versions of the strictest safety standards including IEC 61508, IEC 61511, IEC 62061, EN 954, NFPA 85 and NFPA 72.

Our TÜV certifications include the safety system product certiication, the product development and test organization certification, our functional safety management system and individual certifications for our Safety Execution Centers.

Product Certification
The 800xA High Integrity product including controllers, I/O modules, communication modules, firmware, libraries and engineering tool are certified according to IEC 61508 Edition 2 and IEC 61511-1. All relevant standards and tests are documented with the certificate and report which are available upon request.

Product Development Organization
ABB's Control Technologies Development organization has been certified by TÜV for creating and maintaining a management system that meets the requirements of the IEC 61508 standard.

Functional Safety Management System
ABB's Functional Safety Management System (FSMS) has been developed and certified to be in compliance with the relevant clauses in the IEC 61508 and IEC 61511 standards by TÜV. ABB's approach to functional safety is based on a multi-tiered approach that includes the use of certified products, use of competent (certified) persons and implementation of safety system through the certified organization (partners or ABB Safety Excecution Centers).

Safety Execution Centers (SEC)
ABB's safety execution centers execute safety projects based on our certified Functional Safety Management System. They have been authorized to design, execute and deliver safety automation projects and employ competent functional safety engineers, experts and assessors.

In addition to executing safety projects, the SEC's can also offer functional safety services including development of safety requirement speci-fications, functional safety assessments, HAZOPs, SIL determination and training.

To date, there are over 30 SEC's established worldwide. It is ABB's policy to have each SEC independently certified by TÜV as a functional safety certified company according to IEC 61511 Ed2.

System 800xA High Integrity is certified to SIL 3 by TÜV to the IEC61508 and IEC61511 standards for Safety

ABB Ability™ System 800xA High Integrity safety system

System 800xA High Integrity features a flexible and scalable SIL compliant design. The modular design of the hardware platform supports safety applications from small to large, single or redundant, with local or remote cabinet installations in configurations from integrated to combined to independent.

AC 800M High Integrity Controller
The AC 800M HI offers a SIL3 TÜV certified control environment for process safety in a single controller. The AC 800M High Integrity controller is realized by combining a processor module with a safety module (i.e PM867 with SM812). Multiple controllers are available to provide scalability and flexibile redundancy schemes are available enable up to and including Quad configuration.

Flexible I/O Solutions
Two SIL rated systems are available as part of System 800xA's High Integrity offering:

The S880 High Integrity I/O system is a distributed, highly modularized and flexible I/O system,
providing easy installation of I/O modules and process cabling. S880 I/O modules and their termination units can be mounted and combined in many different configurations. Within the S880 I/O family, there are SIL3 compliant modules for safety critical applications including 4 - 20 mA analog inputs, 24 Vdc digital inputs and 24 Vdc digital outputs.
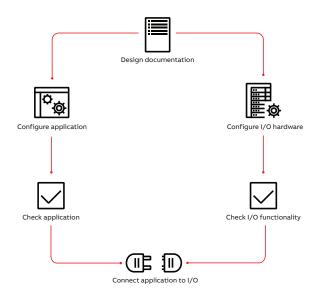
Analog inputs support HART routing and the digital inputs support local time stamping of signal changes for high accuracy sequence-of-events logging. Redundancy of the S800 I/O modules can increase system availability and allow for maintenance activities, such as hot swap, without process interruption.

Select I/O for Safety is a modular, ethernet based, single channel granular I/O system that promotes using xStream Engineering to help decouple project tasks, minimizes the impact of late changes and optimize project schedules. Select I/O for Safety offers flexible redundancy schemes and conditions each individual signal coming from the field with a Signal Conditioning Module (SCM) designed for safety applications. In addition to SIL 3 certified 24v HART enabled AI, AO and 24v DI, DO SCMs, a 3 Amp DO is available. Each SCM offers line monitoring, current limiting, galvanically isolated and is rated for Zone2 / Class 1 Division 2 environments with extended temperature ranges (-40 - +70 deg C).

Select I/O for Safety

System 800xA Integrated Engineering

Design documentation

Configure application

Configure I/O hardware

Check application

Check I/O functionality

Connect application to I/O

—
System 800xA security protection model

Providing a single, accurate, source of system information helps ensure data consistency and improves engineering performance throughout the lifetime of the plant automation system. Working within a common engineering environment, 800xA Engineering supports a consistent information flow from design, through installation and commissioning, to operation and maintenance. In general, System 800xA Engineering features include:

xStream Engineeering
The Select I/O for Safety together with the innovative xStream Engineering tools helps decouple project tasks, minimize the impact of late changes and supports standardization of hardware and cabinets helping projects come on time and under budget.

Graphical Function Design
Graphical function design enables engineers to be engineers instead of programmers. Provides graphical design of the entire control loop - from field devices to process logic. This enables easier engineering and maintenance of IEC 61131-3 applications.

Device Management
Device management for intelligent devices provides the tools to engineer device integration from topology on down to the field elements, including device parameterization, application planning, commissioning and detailed diagnostics.

Reusable Solutions
Facilitates the incorporation of "best practice" standards. The common framework allows logically defined solutions to be quickly reproduced and adapted to meet specific needs with minimum engineering and re-validation. When modifications are made to existing standards, instances are automatically updated.

Operator Graphics
Interactive operator graphics can easily be customized through the use of predefined elements and symbols. See the System 800xA Operator Effectiveness brochure for additional details.

SIL compliant application environment
800xA's object oriented engineering environment with SIL compliant function libraries efficiently supports the entire safety lifecycle. The 800xA engineering environment includes safeguards against non-SIL compliant configurations. Once identified as a safety application, the engineering system will automatically limit user configuration choices and will prevent download if SIL requirements are not met.

A series of safety measures are implemented both for the downloading process and runtime environment. These measures form an important part of the firewall mechanism for combined Control and Safety. CRC protection on different levels, double code generation with comparison and compiler with revalidation are just a few examples of the embedded firewall mechanisms.

Certified Libraries
Control Builder is delivered with an extensive set of predefined type solutions stored in standard libraries. These include data types, functions, function blocks and control modules that can be used to create safety applications. The SIL certified objects and functions in the standard libraries are identified with a SIL marking in the engineering tool.

All necessary SIL certified objects and functions can be found in the certified engineering libraries. Other available libraries contain some components certified for use in SIL compliant applications. See the AC800M High Integrity Safety manual for details.

System 800xA High Integrity Core Functionality

The High Integrity safety system has many built in functions that simplify engineering and ensure consistent and safe operations. A number of these functions are actually part of System 800xA and as such only need to be engineered or configured once for both the process control and safety systems (yet another benefit of the integrated solution). These function include:

- System security and embedded firewalls (Access Control, Confirm Operations and Force Control)
- Access control to SIL applications such as Read, Configure, Confirm or Confirm and Access Enable
- Time tagging events to millisecond accuracy for Sequence of Events (SOE)
- Time stamped audit trails document all changes made to the system by user and change type
- System diagnostics and Difference Report
- Safety supervisory functions

Sequence of Events
By time stamping process and safety events to millisecond accuracy, common event and alarm SOE displays can help identify root causes.

Access Management
During process startup, maintenance, and testing, it is necessary to inhibit specific safety functions. With System 800xA, specific inputs may be inhibited and outputs bypassed through standard-ized

operator dialog. Care has been taken in the design of access control, safety integrity and bypass status overview of System 800xA to combine ease of operation with maximum safety integrity.
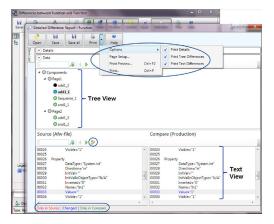
Diagnostics
There are extensive system and hardware diagnostics including CPU load, ethernet statistics and status of controllers, I/O, communication, power supplies etc. System status viewers provide detailed information about the health of each component.

By using different technologies in a redundant scheme (diverse redundancy) and combining with voting, software diagnostics and diverse implementation, it is possible to avoid Common Cause Failures and meet the reliability SIL 3 requirements without hardware redundancy.
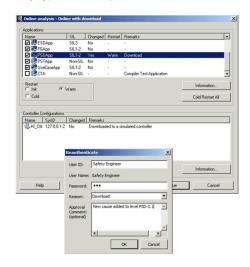
Connectivity and Interfacing Options
In addition to the TÜV certified safety peer to peer protocol, System 800xA comes with certified interference free communi-cations modules for Modbus RS232, Modbus TCP, OPC, Profinet and other ABB protocols. These options enable safety data to be shared with other systems for the purpose of information and display. Data may only be written to the safety controllers via the TÜV certified confirmed on line write functionality or through use of the non-SIL control element.

Difference report – code comparison after importing applications

---

Changing parameters – Optional Re-Authentication Function

System 800xA High Integrity Security

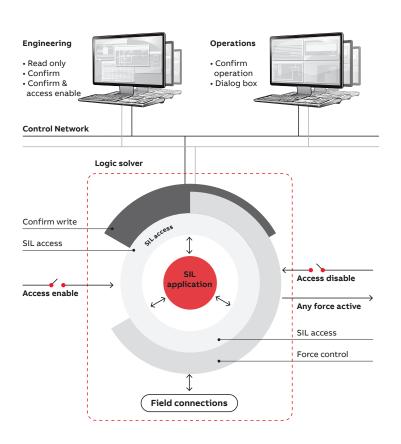**The Rocky Relationship between Safety and Security**
Users have connected (interfaced) safety systems to BPCS systems since the mid 1980s and aimed to develop tighter connectivity since the mid 1990's. These efforts were based on proprietary protocols until the adoption of open network protocols and Windows use in industrial control systems increased the connectivity to business systems and at the same time exposed them to the same security issues (virus, cyber attacks, etc).

The key to security is to ensure that the integration between the safety system and the Basic Process Control Systems (BPCS) DOES NOT compromise Functional Independence and to define the best practices to secure an industrial system and in particular safety systems in this integrated environment. This section provides an overview of the security measures that are built into the System 800xA integrated control and safety system.

System security and embedded firewalls
At the highest level, 800xA safety system integrity is protected through inherent system security

features, such as user log-overs, data access controls, and advanced security features. Operator actions in the system can be assigned different permissions. This assignment defines the permissions a user needs to perform his/ her duties. Examples of permissions are: Read, Configure, and Operate. Time-stamped audit trails document all changes made to the system in terms of user and change type.

Embedded firewall mechanism (access control)
Access Control to applications, Confirm Operation and Force Control are all firewall mechanisms (Access Management) embedded within the safety controller.

Access Control to SIL applications includes functionality for configuration, operations and maintenance. When designing a SIL application, each safety object is given an applicable access level; Read Only, Confirm or Confirm and Access Enable. In Operations, these SIL access levels are automatically enabled. However for the highest access level, a physical input must be enabled to secure authorized access. When Access Enable is active, permission is given to make online changes in the SIL application.

Confirm Operation, together with Access Control, is the embedded firewall mechanism for safe access of object variables during operation and maintenance. Force Control, Override Control, or Bypass Management functionality are necessary to maintain availability of the process in many situations, for example during automatic startup or maintenance of SIS related field equipment. The Force Control in the AC 800M HI follows the lifecycle of the SIS. During design of a SIL application, the safety engineer defines the maximum number of concurrent forced inputs and outputs.

During operations and maintenance, the Access Management software keeps track of the active number of forced I/O points. This information is presented via the safety operator's personalized workplace. The Operator may set and reset forces from the workplace. For an emergency reset of all forces a firmware function including a dedicated physical input is available in the Logic Solver. This both complies with regulatory requirements as well as reduces time consuming application design, implementation and testing.

—
System 800xA security protection model

Engineering
• Read only
• Confirm
• Confirm & access enable

Operations
• Confirm operation
• Dialog box

Control Network

Logic solver

Confirm write

SIL access

SIL access

SIL application

Access enable

Access disable

Any force active

SIL access

Force control

Field connections

System 800xA High Integrity Core Functionality

—
Operators using their world class operator stations at Statoil Hydro

The latest version of System 800xA provides capabilities that reach beyond earlier versions, creating benefit opportunities with integrated features such as:

- Advanced alarm handling and analysis
- High performance operator environment
- Enhanced asset management capabilities
- Fieldbus technologies supporting fully digital instrumentation
- Standardized integration capabilities with plant and enterprise systems
- Integrated safety functionality (SIL3)
- Built in procedural control functionality
- High availability control logic management (Load-Evaluate-Go)
- Integrated electrical systems
- Wireless infrastructure for operations, maintenance and process instrumentation
- Integrated video for visualization of critical process equipment
- Virtualized server and client software
- Robust cyber security protection

The power of integration can provide improvements in areas such as collaboration, management of change and operational effectiveness. Focusing investment in these areas will yield significant results as described below.

Personalized Workplaces
ABB Ability™ System 800xA provides a single, consistent, and intuitive human system interface to access and interact with information included

within the extended automation scope. In day to day operations, the safety level of a plant depends mainly on the quality of the equipment, the execution of different activities, and the work flow process management. Analysis of major accidents and catastrophes have shown that a series of unfortunate coincidental events have taken place prior to such incidents, and that adequate actions where not taken in the first critical phase of fighting them. Therefore, knowledge, information availability, and overall plant awareness are the keys to the daily achievement of plant safety.

Unique to System 800xA is its ability to gather information from multiple plant sources and transform it into relevant information for a diverse set of users. This allows a single window environment to include SIS field devices, I/O, and logic solvers, alarm and events, asset optimization functions, safety reports, etc. Therefore, by virtue of the system's integration and its ability to link to all information aspects of a process or safety object, root causes can be quickly identified and analyzed; allowing users to react to specific process and safety related events in a safe, consistent, and timely fashion.

High Performance Operator Environment
Once the aggregated information is available within the control environment of System 800xA, the next step is to consider the effects and advantages of human factors on operator performance. System 800xA provides the foundation for optimal presentation of information to the operator as well as focusing on human factors and the physical environment with the Extended Operator Workplace (EOW). The EOW comes standard with high performance features such as:

- Advanced keyboards for multi-client handling with hotkeys
- Directional sound system and integrated dimmable lighting
- Motorized, adjustable monitoring positions
- Pre-integrated operator desk system with adjustable desk/monitor positioning
- Micro-ventilation for optimal comfort

The Power of Integration

Data Collection, History and Visualization
Timely collection and distribution of reliable information to the plant's decision makers is critical in today's production environment. The information platform at the core of System 800xA provides the ability to collect and securely store business, process, and safety data from all plant sources. This data can be analyzed and transformed into useful information, and presented to plant users to improve operations efficiency, safety, and profitability.

Asset Optimization
System 800xA Asset Optimization significantly increases control and safety system availability while reducing maintenance costs through early detection of asset performance problems. As one of the integrated applications, the 800xA Asset optimization software has access to all of the relevant plant information and can monitor, assess, and report equipment conditions in real time to reduce costly corrective and preventive maintenance activities.

With an integrated control and safety system, it is possible to implement a common asset management strategy with no additional application programming or interfaces.

Alarm Management – An Extra Layer of Protection
System 800xA's built in alarm management functionality gives operators a common view of all alarms and events that are part of the integrated solution including process, safety and electrical systems. This integrated view helps operators effectively manage plant operations and abnormal conditions through the use of alarm management functions such as alarm grouping, shelving and hiding, as well as metrics continuously calculated according EEMUA 191 and ISA 18.2 standards.

Management of Change
Incremental changes to process automation systems are required today more than ever due to regulatory changes, expansions or additions, optimization, and product variances. In some industries, it is acceptable to have frequent shutdowns to safely incorporate these changes. Adversely, in mission critical, continuous processes such as oil and gas, petrochemical, and power,

shutdowns are few and far between. In most cases, major outages in these types of process applications will only occur every 3-6 years, thus changes to a control system's configuration are a necessary and acceptable practice.

ABB Ability™ System 800xA can efficiently facilitate the management of change process. In addition to tracking and documenting change through features such as "audit trails", there are many features that minimize risk when implementing change, such as:

- Change verification. Finding mistakes prior to download with Difference Report for application code and graphics.
- Stepwise change introduction through library versioning
- Cross referencing tool to identify all instances of variables or process points
- Simulation against "soft" controller or an isolated on line controller running against live I/O
- Impact analysis of live versus an "evaluation" version of the program using the Load-Evaluate-Go feature

Hi Integrity Hardware

—
Select I/O HI with TU865 module for Safety

Select I/O High Integrity
Select I/O for Safety is a modular, ethernet based, single channel granular I/O system that promotes using xStream Engineering to help decouple project tasks, minimizes the impact of late changes and optimize project schedules.

Select I/O for Safety offers flexible redundancy schemes and conditions each individual signal coming from the field with a Signal Conditioning Module (SCM) designed for safety applications.

In addition to SIL 3 certified 24v HART enabled AI, AO and 24v DI, DO SCMs, a 3 Amp DO is available. Each SCM offers line monitoring, current limiting, galvanically isolated and is rated for Zone2 / Class 1 Division 2 environments with extended temperature ranges.

S800 I/O HI Integrity
The S880 High Integrity I/O system is a distributed, highly modularized and flexible I/O system, providing easy installation of I/O modules and process cabling. S880 I/O modules and their termination units can be mounted and combined in many different configurations.

Within the S880 I/O family, there are SIL3 compliant modules for safety critical applications including 4 - 20 mA analog inputs, 24 V dc digital inputs and 24 V dc digital outputs.

Analog inputs support HART routing and the digital inputs support local time stamping of signal changes for high accuracy sequence-of-events logging. Redundancy of the S800 I/O modules can increase system availability and allow for maintenance activities, such as hot swap, without process interruption.

Non-interfering Communication Interfaces are available and can be used for non-safety critical functions. These communication modules are installed to the left of the safety module (SM812 for example). See the ABB Safety Manual for the latest list of interference free modules available.

—
Redundant S800 High Integrity I/O

ABB Safety Portfolio and Experience

ABB has a comprehensive portfolio of safety systems, instrumentation, tools, certified execution centers and safety consulting services. We can deliver certified safety instrumented systems for all applications that meet the lifecycle requirements of the IEC standards.

Safety Systems
We offer a broad portfolio of safety systems for all applications from "stand alone" (Independent HI) to completely integrated (System 800xA HI). There are systems for process safety (BMS, ESD, HIPPS etc.) as well as machine safety.

Instrumentation
ABB has a wide portfolio of instrumentation suitable for use with a Safety Instrumented System (SIS). Our SIL certified positioners and transmitters (both flow and level) ensure we can meet the most stringent safety requirements.

Tools
Our tools such as TRAC and TRAM are designed to help you execute and document SIL assessments and maintain your safety performance through alarm and trip management.

Consulting
In order to implement a safety system according to the IEC61511 standard, it is necessary to do a proper assessment of your safety needs and to employ a formal functional safety management system. ABB has the experts available to assist with the following parts of the safety lifecycle:

- Hazard Identification
- SIL Assessments
- Functional Safety Assessments and Audits
- Safety Requirement Specification development
- SIS Design and Engineering
- Training

Project Execution
ABB has over five hundred certified functional safety engineers around the world as well as a network of certified partners that can design, implement and install safety systems according to our certified Functional Safety Management System. From "kick start" consulting all the way to full project management, we can support you through the entire safety lifecycle.

ABB has over 2500 system installations around the world using the AC 800M HI safety controller. We are present in over 55 countries with more than 5500 controllers and over 750 million SIL certified I/O points. Here are some notable projects over the years.

- Statoil Gullfaks A, North Sea (ESD, F&G)
- Statoil (previously Norske Shell) Troll A, North Sea (ESD, F&G)
- Pemex, Burgos Complex, Reynosa, Mexico (ESD, F&G)
- Rexchip Electronics, Taichung, Taiwan (ESD)
- Vale, Goro Nickel, New Caledonia (BMS)
- Pemex Refining, Cadereyta, Nuevo León, Mexico (ESD)
- Repsol YPF, Lujan de Cuyo Refinery, Mendoza, Argentina (BMS, ESD)
- China National Offshore Oil Corp (CNOOC), Wellhead Platforms Qi Kous 181 & 172 for the Boxi Oil Field
- ADCO, Bab Thamama, Abu Dhabi, UAE (ESD, F&G, HIPPS)
- ADCO, ASAB Wellheads, Abu Dhabi (ESD, F&G)
- Inagip Annamaria Gas Field Development, Adriatic Sea (ESD, F&G)
- Shell Ormen Lange Gas Field, North Atlantic (ESD, Anti-Surge)
- Spectra Energy McMahon Sour Gas Processing Plant, British Columbia, Canada (HIPPS)
- Atanor Rio Tercero Plant, Cordoba Province, Argentina (ESD)
- Turano Lodigiano combined cycle power plant, Italy (BMS)

ABB

—