System 800xA High Integrity
Emergency Shutdown Solution

800xA High Integrity Emergency Shutdown Solution

With 30 years of experience in designing, implementing and maintaining safety systems, ABB provides a simpler, integrated application solution for Emergency Shutdown systems.

—
Some of the world's largest offshore platforms have emergency shut-down and Fire & Gas solutions based on 800xA High Integrity.

An Emergency Shutdown (ESD) system prevents or minimizes the consequences of emergency situations, helping to avoid loss of human life, damage to the environment, and/or loss of equipment.

System 800xA is ABB's main control system offering in which 800xA High Integrity constitutes the Safety Instrumented Systems (SIS) portion. The ESD safety system can be fully integrated with the System 800xA Basic Process Control System (BPCS), thereby providing a common operational, engineering and information environment for BPCS and SIS. Note that the level of integration is completely optional and ranges from a completely stand-alone to a fully-integrated configuration, all enabled by the uniquely flexible System 800xA architecture.

System 800xA includes a comprehensive library of standard reusable components that include extended automation entities such as faceplates, graphic elements, trends, document links and alarms and events.

In addition, ABB provides a broad family of industry -specific libraries that contain Control Modules, Function Blocks, Data Types and graphic elements including special safety systems features for ESD applications. These pre-tested and safety-certified libraries significantly reduce the time required to engineer, test and maintain control while minimizing project risks.

In compliance with traditional industrial risk analyses for ESD functions, these libraries are certified for Safety Integrity Level 3 (SIL 3).

Based on the powerful graphical builder of System 800xA, ESD system visualization can be freely designed and tailored to each specific installation. This provides the operator with an immediate understanding of the relations between sets of inputs (triggering events) and outputs (actions).

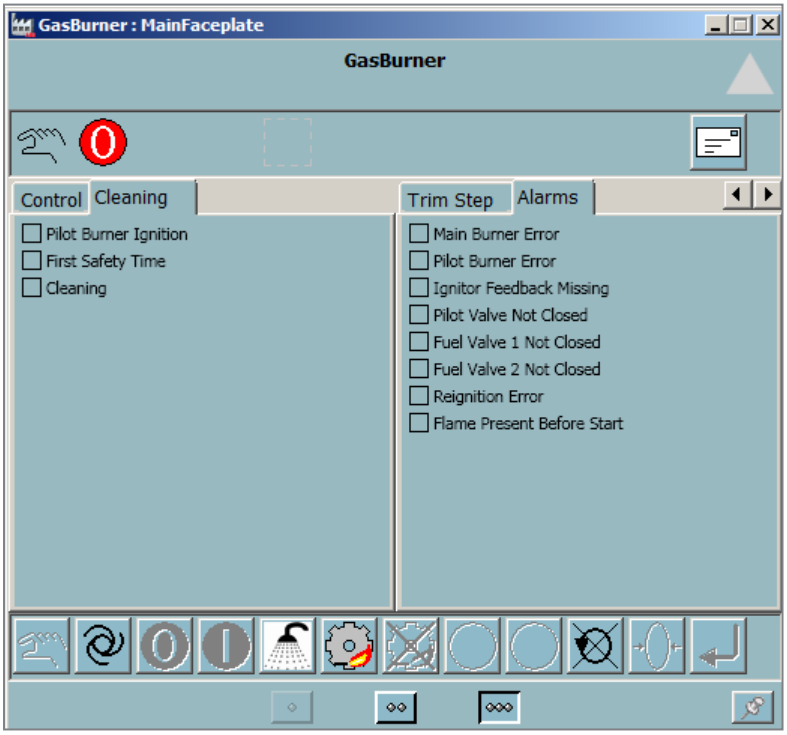
—
01
Predefined descriptive graphic displays of common objects speed up engineering work.

—
02
Function blocks with SIL-levels clearly indicated in the engineering environment.

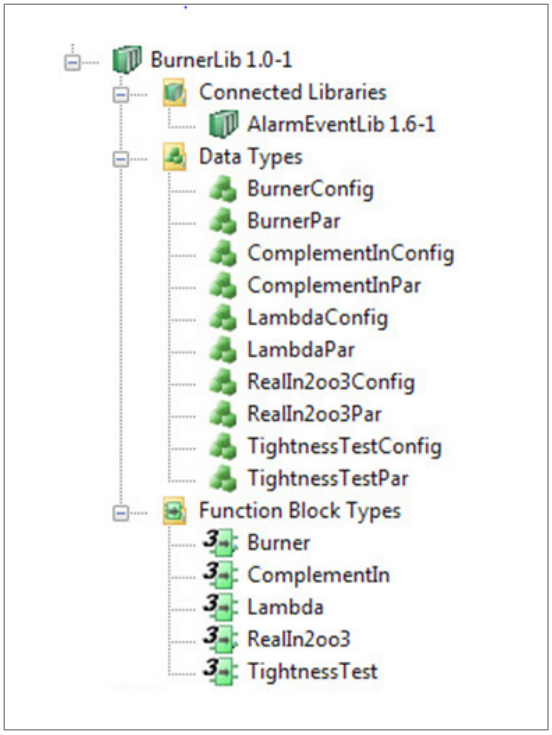
From smaller systems for single processes to larger, hierarchical plant-wide solutions with several safety levels, e.g. process-section shut-downs, total-process shutdowns and total-plant shutdown, ABB provides a solution for Emergency Shutdown systems. Integration of state-of-the-art, certified products for ESD applications utilizing standardized, high-performance plant network solutions with TÜV-approved AC 800M High Integrity controllers results in a powerful and homogenous, ESD system. ABB provides certified building blocks for ESD applications. This enhances functionality, increases safety and considerably simplifies the engineering process.

ESD Libraries
ABB offers a wide range of control modules for monitoring and controlling safety systems. A complete range of high-level Control modules, Faceplates, Graphic Elements, Alarm management and operational templates and strategies are included as part of the standard 800xA High Integrity offering.

The SIL3-certified Supervision Basic Library includes a range of function blocks typically used in ESD applications. Easily identifiable safety-certified function blocks provide engineers and operators with a clear-cut visual separation between safety-critical and process-control application code.



—
01



—
02

800xA High Integrity functionality

Diverse technology for maximum reliability
The AC 800M HI offers a SIL3 TÜV certified control environment for combining safety and business critical process control in one controller without sacrificing safety integrity. The AC 800M High Integrity controller is realized by combining different technologies in the processor module and the Safety Module (co-processor).

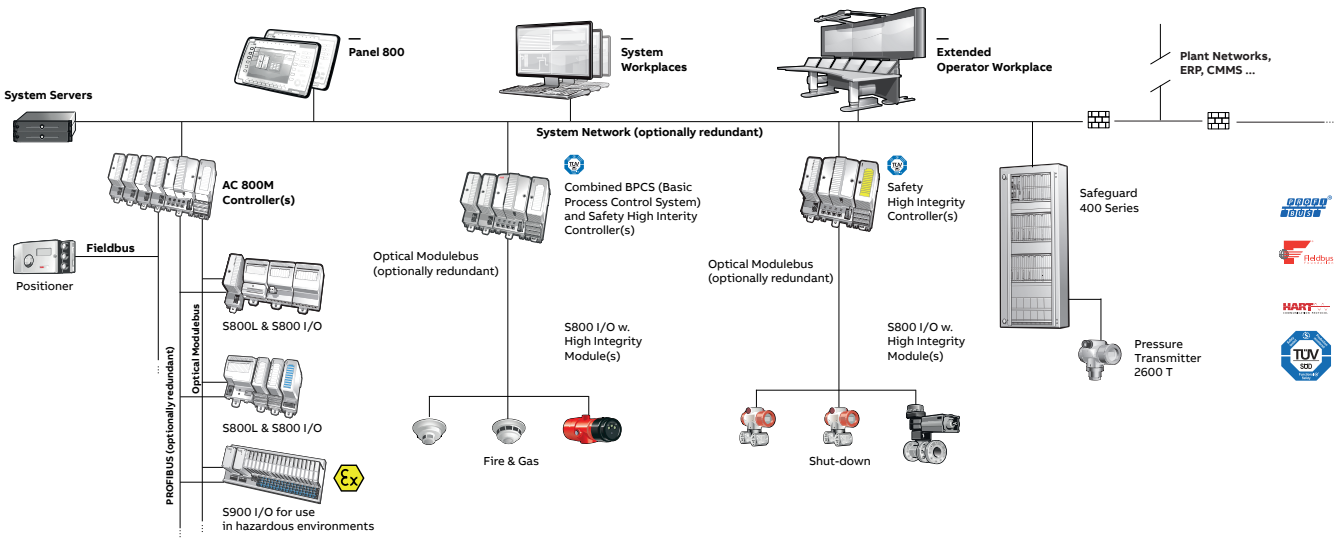
Fault tolerance for maximum availability
Flexible redundancy schemes enable controller configurations up to and including Quad configuration. Libraries are marked non-SIL or SIL to show their usability. Embedded safety measures prevent inadvertant degradation of safety applications.

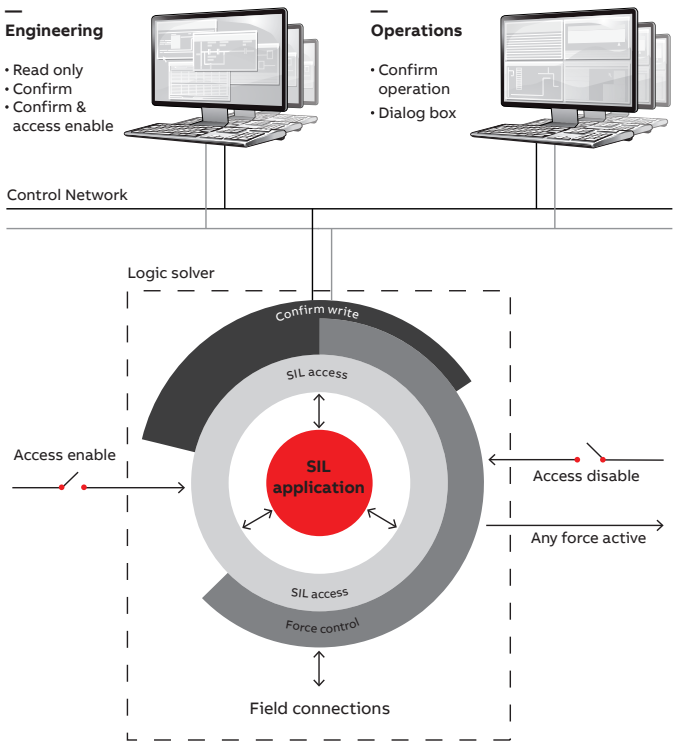
Flexible integration to System 800xA
800xA High Integrity and System 800xA utilize common engineering tools as well as operator interface, historian, audit trail, asset and device management applications and instruments. This enables system-level tools and functions to be leveraged across an entire integrated plant automation solution, including the safety system. Such an environment offers safe and instant interaction between applications, which leads to a host of benefits, including easier handling through better technical solutions and reduced cost of ownership throughout the system life cycle.

Access management
Access Control, Confirm Operation and Force Control are all firewall mechanisms embedded within the safety controller. Access control to SIL applications includes functionality for configuration, operation and maintenance. In accordance with several safety standards, a physical input implemented as a hard-wired signal to the safety controller must be activated to enable the highest level of authorized access. When the Access Enable input is actived, permission is given to make online changes in a SIL application.

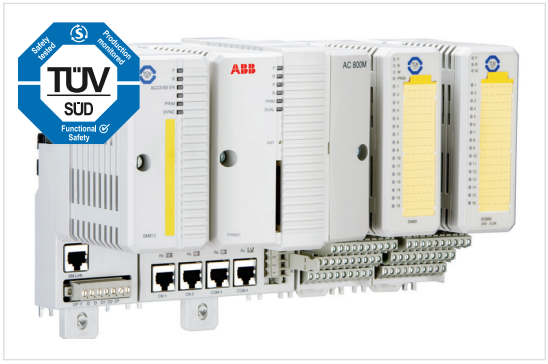
High Integrity I/O
System 800xA's S800 I/O is a distributed, highly -modular and flexible I/O system that allows easy installation of I/O modules and process cabling. SIL3-compliant High Integrity I/O modules within the S800 I/O family can be used for safety-critical applications. These I/O modules include those for 4-20 mA analog inputs, 24 Vdc supervised digital inputs and 24 Vdc digital outputs. The digital output module provides both Normally Energized and Normally Deenergized outputs typically used in ESD and Fire & Gas (F&G) systems respectively. The digital inputs support local time-tagging of signal changes for high-resolution sequence-of-events logging. Analog inputs support HART pass -through for easy calibration, monitoring and diagnosis with configurable access when using HART device integration.

—
Process control and safety systems can be seamlessly integrated in System 800xA.





—
01



—
02

—
03

—
01
Embedded firewalls and confirmation procedures protect the SIL application from inadvertent/ accidental control actions.

—
02
AC 800M High Integrity controller is SIL3-certified both in single and redundant configurations.

—
03
ABB's range of safety-certified instruments includes flow, pressure, temperature, etc.

Force Control
Force Control in the 800xA High Integrity system has been implemented to support all operational, engineering, maintenance and management activities throughout the system life cycle. When designing SIL applications, the safety engineer defines the maximum number of concurrent forced inputs and outputs. During operation and maintenance, the Access Management software restrict access to SIL applications to prevent unauthorized changes, additionally keeps track of the active number of forced I/O points. This information can be made available via the safety operator's personalized workplace.

For emergency reset of all forces, a firmware function that includes a dedicated physical input is available in the safety controller. This complies with regulatory requirements and reduces time-consuming application design, implementation and testing.

High Integrity instrumentation
ABB can provide a wide range of safety-certified sensors and positioners. Various solutions are available ranging from full-redundancy, high-integrity transmitters designed and certified by TÜV to comply with IEC 61508 requirements to standard transmitters with enhanced internal diagnostics to minimize the Probability of Failure on Demand.

System 800xA functionality

Functional Safety Management via Aspect Objects platform
The framework of the 800xA High Integrity system environment is built on ABB's Aspect Object technology. Managing data within this singular virtual database environment, System 800xA makes all the information required to install, operate and maintain the system available through a common interface. This makes it possible to access data (aspects) directly from its source in the context of the asset (object) without needing to know where the data comes from, and without concerns about data integrity and concordance.

System 800xA's system platform opens new perspectives during the design and realization of safety and control applications, as well as during Functional Safety Management (FSM) and other safety-related support functions.

For example, safety aspects could include hazardous operation studies, safety-requirement specifications, safety allocation specifications, SIL Assessments, installation and test support, maintenance, modifications and change management, configuration management as well as SIL monitoring, validation and verification.

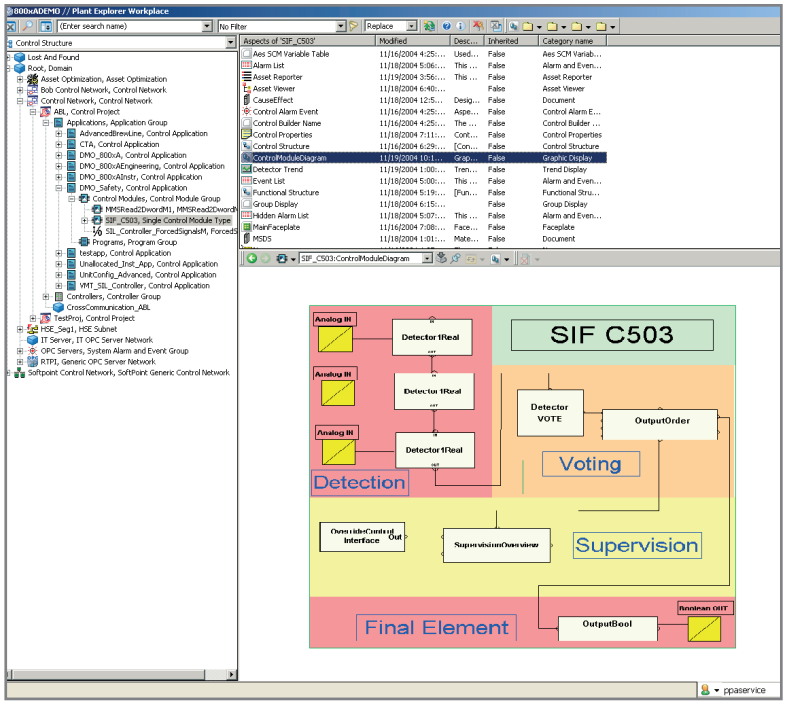
Sequence of Events (SOE) and Alarms
Alarms and time-tagged Event messages are stored and presented with milli-second accuracy in alarm lists and SOE displays. This standard feature of the 800xA system constitutes a powerful tool to quickly identify the root cause should a shutdown or hazardous event occur. In an integrated BPCS and SIS system configuration, common SOE handling across the process control and safety systems enables faster and safer process start-up in the event of a shutdown.

Messaging
Remote personnel are notified of critical events via mobile telephones, e-mail accounts and pagers by the system's SMS (Simple Messaging Service) and e-mail messaging service. Using GSM (Global System for Mobile communications) mobile phone technology, 800xA allows remote acknowledgement of notification and confirmation of receipt.

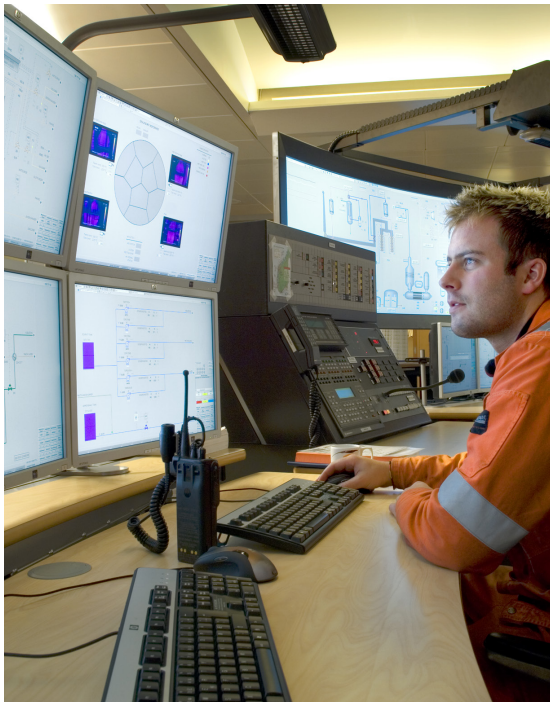
—
01
Dedicated safety workplaces offer overviews as well as easy access to detailed information.

—
02
Top-of-the-line operator environment for safe operation and informed decision-making.

—
01



—
02



—
ABB's ESD solutions help prevent emergency situations in the chemical industry.

System 800xA Information Management
System 800xA collects and securely stores business, process and safety data from all plant sources. Due to the powerful and flexible system functionality and features, this data can be analyzed and transformed into useful information, and presented to plant-users to improve operational efficiency, safety and profitability. Examples of safety compliance reports that can be created include:

- **Override Report.**
  Shows an overview of all tags that are currently in force, blocked, suppressed or in override, etc. In combination with the standard System 800xA Audit Trail functionality, the report also enables historical reviews of when or by whom a tag was blocked or suppressed.

- **Valve Verification Report.**
  Summarizes valve functionality in the system. This report contains valve operation information such as calculated valve travel time and operational status, as well as a fault-frequency report on valves and valve groups.

- **Valve Leakage Test Report.**
  Summarizes results from valve-leakage testing. The Valve Leakage Test Report can be used on all valves, both critical and non-critical. The report consists of logging pressure data for a valve after the operator has created a pressure difference across the valve.

- **Automatic Shutdown Report (ASR).**
  Validates the success of a Process Shutdown (PSD) or Emergency Shutdown (ESD). The ASR report contains an over-view of all shutdowns performed in the system, and gives the operator detailed information of cause and effect relationships, including status of the operations performed.

On-line diagnostics
Each safety controller in the 800xA High Integrity system issues detailed messages about safety-related information and problems. These are typically monitored through the operator station. This high level of diagnostics is essential for the integrity of the ESD. System Status and Asset Viewers provide detailed information about the health and location of every device in the safety system.

Personalized workplaces for safety personnel
The library modules typically used for BMS applications provide a set of easily-configured operator displays and dialogs. These displays can be organized in a hierarchical structure with an overview display for status presentations and detailed displays with object presentations. The overview display contains the status of the whole shutdown system and includes links to Cause & Effect type detail displays and shutdown level displays.

Every ESD field device connected to a safety controller has a corresponding predefined graphic display (faceplate) with real-time information and dialog with the device. Interactive operator graphics can easily be customized through the use of predefined elements and symbols.

abb.com/highintegritysafety

3BSE055220 en B