Features and Benefits

- **Safety Integrity:** With its 1oo2 architecture, Safeguard 400 Series controllers satisfy Safety Integrity Level 3 as defined in the IEC 51408 standard.

- **Very High Availability:** Wide diagnostic coverage is implemented per control branch, which means that if a failure is detected in one branch, the other will ensure uninterrupted production. Because diagnostic coverage is extensive, Safeguard 400 Series controllers reach an availability on the same level as 2oo3 architectures.

- **Stand-alone or Integrated:** A fully integrated member of System 800xA, Safeguard 400 Series controllers can also be configured as complete stand-alone, safety systems.

- **Easy Engineering:** An object-oriented engineering environment with SIL-compliant function libraries supports efficiently the entire lifecycle, from concept, design and implementation, to operation and maintenance.

- **Easy Maintenance:** Extensive diagnostics ensure fast and simple repair and replacement of components. All system modules can be replaced, and applications programmed and tested, while the system is in operation.

Reducing Risk through Safeguard 400 Series

For 30 years, ABB has been in the forefront of industrial safety instrumentation and automation. Safeguard 400 Series embodies the company’s accumulated know-how in the field.

The system consists of programmable safety controllers, a wide range of input/output boards, operator and engineering workplaces, communicating over an industry-standard communications network. It is an integral part of ABB’s Industrial IT Extended Automation System 800xA, allowing for easy integration of the system’s many productivity-enhancing applications, such as its information management features.

Safeguard 400 Series controllers are certified to the leading standards in industrial safety, IEC 61508 and IEC 61511, and boasts an outstanding performance record: millions of operating hours to date in safety-sensitive industrial facilities around the world without any performance failures.
Introduction

A Pioneer in Safety Systems

In today’s fast-paced global economy, competitive advantages result when a company can tap into its assets’ unused productivity safely and effectively to meet changing demand. Continuous pressures to reduce costs are balanced by the company’s social responsibility to protect their people, property, environment, and the surrounding community from harm. With the increasing acceptance of “smart” equipment, the process industries are experiencing a revolution; demanding closer integration of safety and control systems, safety functions at varying states, and flexibility, scalability, and reusability of safety components. In addition, the process industries require safety system certification and protection of their installed system investments. Since the late 1970s, ABB has supplied more than 500 complete safety system solutions to the offshore industry alone.

Based on 30 Years of Experience

800xA Safety solutions today are the result of step-by-step development, where new technology has never been implemented at the risk of compromising safety. This can best be documented through tens of millions of operating hours with no performance failures. Safeguard 400 Series meets the strictest demands for safety and availability, and is designed in accordance with international standards.

Lifecycle Safety Functionality

800xA Safety solutions are delivered and supported in accordance with the strictest current safety standards. IEC 61508 is fully implemented and is the base for TÜV approvals. The quality assurance programs applied to manufacturing, engineering and installation meet industry standards, ensuring that the systems always satisfy the applicable safety requirements. To maintain absolute safety functionality, the IEC 61511-compliant safety plan must specify procedures and routines for all activities related to the system throughout its lifetime, including training, system operation, service and maintenance, reprogramming and upgrading.
Safeguard 400 Series products and systems are utilized around the world in industries where production processes can present a danger to people, facilities, equipment and the environment. ABB installations can be found on all continents and the users among the world’s largest in oil, chemicals, petrochemicals, power, offshore and shipping.

- **Emergency Shutdown Systems:**
  From smaller systems with single processes, to larger, hierarchical plant-wide solutions with safety levels such as process section shutdowns, total process shutdowns and total plant shutdown.

- **Fire and Gas Systems:**
  Total system solutions for fire & gas detection and protection, providing a high level of alarm integrity and the most advanced principles for early warning and monitoring.

- **Critical Control:**
  Control of processes that, from an economic or safety point of view, requires continuous, uninterrupted operation. Typical applications can be found in energy supply, chemicals, petrochemicals and in oil & gas.

- **Equipment Protection Systems:**
  Monitoring and control of vulnerable, expensive, production equipment, e.g. rotating machines, turbines, generators, and compressors.

- **ABB’s certified Safeguard 400 Series Systems:**
  Used successfully in a wide variety of industrial facilities around the world to prevent accidents.
800xA for Safeguard

ABB has now combined the two worlds: Safeguard 400 Series as safety supervision system with System 800xA, featuring best-in-class productivity enhancement software such as 800xA Process Portal, Asset Optimization, and Information Management.

With Industrial IT System 800xA for Safeguard, plant operations are provided with the technology and solutions needed to achieve a sustainable competitive advantage by enabling the plant to perform with optimal productivity, safely and at substantial cost savings.

In short, the integrated functions of System 800xA can be added to Safeguard 400 to extend the plant system's capabilities.

Based on ABB's Industrial IT Aspect Object™ technology platform, 800xA for Safeguard seamlessly integrates 800xA process controllers and Safeguard 400 Series controllers on the same MB500 Ethernet network. All connected controllers are supervised and controlled from 800xA Process Process Portal workplaces.
Safeguard 400 Series Safety Controllers

The Safeguard 400 Series safety controllers are the main building blocks for System 800xA SIL3 safety applications. It combines the features of a high-integrity programmable electronic system for safety applications with the functionality and software architecture of a modern process controller.

Safeguard 400 Series is based on a duplex architecture that utilizes refined versions of standard controllers from ABB’s automation portfolio. The idea of offering safety systems with high safety integrity combined with an inherent ability to easily be integrated into modern control systems, is a core strategy in ABB’s safety products development.

Safeguard 400 Series controllers comply with the design standard 1oo1D or 1oo2D, two of the designated architectures for safety systems defined by IEC 61508, the international standard for functional safety in electronic safety systems. One main benefit of this architecture is the detection and identification of potential failures by means of active selftesting.

Predefined functions are available at all levels - signal descriptions, function blocks, operator functions and communication. Carefully selected default values are provided for all process signals to be connected. All parameters are preset to yield a carefully chosen standard function, thereby limiting the changes required to a minimum (for example tagname, alarm limits, etc.). The operator station involved is connected the moment the signal is defined. It only requires confirmation by entering a simple command and the signal name.

Some examples of predefined operator functions are event and alarm handling, bypass management, signal object displays, system diagnostic and query-based reporting.

The application program is created by interconnecting the functions needed in a functional, high-level, language that provides function blocks for both logic and analog control. The function-block library also contains the elements required for voting and cause-&-effect programming.

Simple, efficient, consistent and understandable programs save time and money during development, maintenance and redesign. Good program quality flows from division of the entire application program into suitable function blocks and subprograms.

Figure 2. Safeguard 400 Series offers dual or single configurations, for SIL 3 or SIL 2 applications.
Safeguard 400 Series - Key Features and Benefits

**Fully configurable standard models:** Safeguard 400 Series safety controllers are delivered in three standard versions:

- Safeguard 410
- Safeguard 415
- Safeguard Compact

The choice of model depends on the configuration. The exact I/O capacity for all models depends on the I/O mix. The maximum capacity of Safeguard 400 is approximately 1,400 I/O. A wide range of I/O modules means easy adaptation to any application.

**Safety integrity:** With its 1oo2 architecture, Safeguard 400 Series controllers satisfy Safety Integrity Level 3 as defined in the IEC 51408 standard.

**Very high availability:** Wide diagnostic coverage is implemented per control branch, which means that if a failure is detected in one branch, the other will ensure continuous production. Because diagnostic coverage is extensive, Safeguard 400 Series controllers reach an availability on the same level as 2oo3 architectures.

**Stand-alone or integration:** Safeguard 400 Series controllers are complete, stand-alone, safety systems but can also be directly and fully integrated into System 800xA control networks. Standard communication solutions are available for interfacing with distributed control systems.

**Safe ethernet communications:** Safeguard 400 Series controllers provide safe communications in compliance with IEC 61508 SIL 3.

**Easy maintenance:** Extensive diagnostics ensure fast and simple repair and replacement of components. All system modules can be replaced, and applications programmed and tested, while the system is in operation.

---

Figure 3. Safeguard 400 Series satisfies Safety Integrity Level 3 as defined in the IEC 61508 standard. Single Safeguard, with its 1oo1D architecture, complies with Safety Integrity Level 2.
Control Architecture and Theory of Operation

RDA - Refined Duplex Architecture

RDA is an architecture for safety-critical control functions that combines the safety factor of the 1oo2 architecture with the availability factor of the 2oo2 architecture.

The Safeguard 400 Series controller architecture consists of two parallel control branches that act independently and with equal priority on the control decision. Consequently, any common mode of operation and any common source of failure is reduced to a minimum. Selftests instead of voting mechanisms reduce the probability of accumulated unrevealed dangerous failures in the system.

Theory of Operation

The two parallel control branches read field signals, execute the safety control logic, calculate the control outputs and set the field output signals individually and independently of each other. However, each control branch is able to set the field output signals only when its diagnostic control issues an active permissive signal.

The combination of active selftesting with permission control of any control action adds optimal failure tolerance capability to the superior attributes of the 1oo2 architecture regarding safety integrity.

Extensive and active selftests with replication are implemented individually in both control branches. Detected failures are generally prevented from causing spurious interruptions in outputs, and, in the event of a correlated failure in both branches, a fail-to-safety action takes place.
IEC 61508 - Functional Safety

This international standard sets out a generic approach for all safety-lifecycle activities of programmable electronic systems, utilized to perform safety functions. A safety instrumented function is defined to include sensors, controller and actuators. IEC 61508 defines four safety-integrity levels (SIL) for control systems installed to maintain functional safety. Safeguard 400 Series is certified to meet the requirements of Safety Integrity Level 1-3 (SIL 1-3) or, in the case of Single Safeguard, SIL 1-2. Safety functions at these integrity levels require a safety control function with a maximum probability of failure on demand in the range of $10^{-3}$ to $10^{-4}$.

**Designated architecture:** IEC 61508 defines a number of standard or designated control architectures for safety applications. Safeguard RDA systems belong to the type 1oo2D of this standard. In Safeguard 400, however, both control branches are allowed to execute shutdowns. The D stands for diagnostics. Each of the two control branches of Safeguard 400 contains diagnostics based on active functional selftesting.

**RDA principles:** Refinement of the classical 1oo2 control architecture by adding extensive, active diagnostics and fault tolerance, including a minimum of additional hardware, characterizes the RDA control strategy. In RDA systems, an optimal balance of safety and availability is achieved with safety as a priority. This is critical because:

- Voting mechanisms require dynamic changes to recognize differences (passive failures). The majority of safety functions are static (on-demand) functions.

- Dangerous failures (potential dormant failures, preventing safety actions) are detected by active continuous selftests to minimize accumulation of dangerous, undetected, failures. Diagnostics by active selftests are the generic property of an 1oo2D RDA system.

---

**Figure 6.** Block diagram of a 1oo2D system architecture according to the IEC 61508 standard.

---

Figure 5. 800xA for Safeguard offers a common platform for both engineering and operations supervision.
Input Modules

The Safeguard 400 Series input subsystem is built up of modules, each consisting of two completely separate input boards, one for each control branch (A and B). The sensor signal is split in a field termination unit and transmitted to each of the two input boards by separate ribbon cables. Completely independent of each other, these measure the signal, determine status and enter the values in input databases A and B, respectively.

A wide range of input modules is supported, ranging from simple noncritical input types to high-integrity safety modules. High-integrity safety input modules are available in the following types:

- Fail-safe digital modules
- Supervised digital modules, normally open/closed
- Fire detector modules with reset pulse
- Electrocatalytic gas-detector modules
- Analog modules, 0 - ±10V or 0 - ±20mA

Extensive Supervision and Testing

It is generally assumed that 35% of all failures occurring in safety-related systems are caused by the input subsystem (ref.: IEC 61508, SIL target failure measure). To avoid spurious trips and achieve maximum reliability, Safeguard 400 Series input modules feature extensive testing and monitoring possibilities.

- All connected sensor loops are monitored for ground faults, short circuits, cable breaks and power failure.
- Input signals are compensated for variations in sensor loop power supply, variation in gain and differences between the analog grounds of the termination unit and the input board.
- All boards have reference voltage to verify that the complete multiplexer, A/D converter, and bus interface operate correctly.
- Front-mounted LEDs indicate board, and signal-loop status.
**Input Voting**

Safeguard 400 Series controllers offer predefined functions for majority voting on digital and analog input signals. In principle, the system can be designed for any voting scheme, e.g. 1 out of 2, 2 out of 3, etc.

The adjacent figure shows a tripled configuration with three sensors and three separate input channels per control branch. The input database in each of the two control branches receives three independent sensor values.

For example, with a 2-out-of-3 voting scheme the control logic utilizes the status values it receives from at least two of the three sensors. Any discrepancy in signal values will immediately be detected and reported as an error.

**Figure 8.** Example of a tripled sensor input scheme.

**Redundant Power Supply**

System and field power supply is installed in separate racks and galvanically isolated from each other. Both power systems are built up of modular plug-in units and can be delivered for a wide range of input voltages.

System power is always delivered with full redundancy, utilizing separate power modules for each control branch. If further redundancy is required, the rack has space for one extra module per control branch (n+1 redundancy). In principle, field power supply can be configured for any redundancy desired. All power modules have stabilized output voltage and AC modules can be delivered with power-correction factor, which often means that UPSs can be downsized.

**Figure 9.** The modularized system power supply arrangement is always configured with redundancy and each signal branch is always powered from a separate unit.
Safeguard 400 Series – Output Subsystem

High-integrity Output Modules

Safeguard 400 Series's output subsystem is designed to guarantee safety action on demand and, at the same time, eliminate spurious trips and provide continuous, uninterrupted production.

Based on output signals and diagnostics from each of the two control branches, as well as testing routines that monitor its own functionality and the field loop, the output subsystem determines and yields the correct output action to the final field element.

Fault-tolerance and Availability

The system’s fault-tolerance capabilities are based on active individual testing of each control branch. If a critical failure is detected in one branch, it will immediately be isolated, and production continued under control by the other.

The possibility to isolate one control branch is also utilized for maintenance purposes. Service, application programming and testing tasks can be completed while the system is in full operation.

Output Modules

The output subsystem is built up of digital output boards and voting/field termination modules. Two types of modules are available:

- Normally energized output modules are utilized for shutdown valves and other types of equipment where fail-to-safety action is required, i.e. where de-energized is the safe state.

- Normally de-energized output modules are utilized for field devices that are not powered during normal operation, i.e. for devices powered to cause action.

Figure 10. The output-voting/field-termination modules determine the correct output actions from the system.
Figure 11 shows a simplified schematic overview of the basic operation of a normally energized output.

The two control branches independently execute the control logic, and send their output signals to the output voting/field termination modules.

Simultaneously, the output modules receive diagnostic information on each of the two control branches. In a 2oo2 voting block (one for each control branch), the output signal is run against the diagnostics. If the diagnostics yield a permissive signal, we have a 2 out of 2 situation (output signal + control branch permitted). The output signal is then forwarded to final 1oo2 voting.

The final 1oo2 voting block must receive a permitted output signal from at least one of the control branches to send the final output signal to the field. In a normal situation, permitted output signals will be received from both control branches.

If a failure is detected in one of the control branches, the process will still continue uninterrupted. The failure will be isolated immediately thus preventing spurious trips. Safeguard 400 Series will then operate as a 1oo1 (single) system. Alarm messages and detailed diagnostic information will be sent to the operator so the fault can be repaired quickly.

In the event that failures are detected in both control branches simultaneously, a fail-to-safety action will be initiated.

The output modules run continuous tests, monitoring their own total functionality. Each output channel is tested cyclically. In addition readback of output signals provides continuous feedback on the true output status. A loop status feedback function constantly checks that the current in the field loop is normal. This is an important function in control circuits of safety devices that are normally inactive for longer periods of time.
800xA for Safeguard software architecture offers object-oriented instrument database configuration and structured function-block programming. Data integrity is ensured by single entry and storage of data. Each field instrument and I/O board has its dedicated database record and is identified by its unique instrument-tag or board name.

Signal conditioning and treatment are individually controlled by properties in the instrument database. Configuration work is minimized by the use of default settings. By just setting a few properties in the database, the full functionality of event and alarm handling, database query and system and I/O module diagnostic reporting are automatically put into operation without further engineering.

800xA for Safeguard provides a set of high performance engineering tools for configuration, application programming, documentation, testing and commissioning of Safeguard 400 controllers. This tool set offers structured programming in a modern graphical workstation environment.

Safeguard 400 Series offers load and dump of the database and the application programs, both locally and via the network, as well as off-line and on-line programming. Import from remote instrument engineering databases is easily achieved. The well defined structures of Safeguard 400 application source code files allow standardized interfaces and the use of excellent tools for data acquisition and management, e.g. MS Excel, Access, etc.

Safety function application software may be structured in any convenient way to achieve maximum safety function integrity.

**Figure 12.** Signal descriptions and application programs are separated. The database is the common source of information. Predefined signal, communication and operator-function descriptions reduce the application engineering workload significantly.
800xA for Safeguard programming tools include:

- Application Builder for the handling of projects, nodes, control circuits and type circuits.

- On-line Builder for configuration and application configuration of Safeguard 400 controllers (optional).

- Function Chart Builder for application configuration of Safeguard 400 controllers in off-line mode.

- Safety Builder for cause-&-effect application programming of Safeguard 400. It also provides an interface to Engineering Studio and suitable Aspect Object Types.

Cause and effect matrices are used to design, verify and document shutdown and protection-related applications. This represents the relationship between a set of process inputs and the actions they trigger.

This tool supports the design of hierarchical safety shutdown levels and may be used to organize the overall shutdown strategy. The application logic and its connections to the signal database are automatically generated from the tool, ready-made for installation.
System 800xA's Process Portal provides a single, consistent, and intuitive human system interface to access and interact with information included within the extended automation scope.

The focus on environmental and safety issues is increasing in modern industrial plant operations. Lifecycle safety management is the focus of new and coming standards that will affect all parties involved in industrial activities.

In day-to-day operations, the safety level of a plant depends mainly on the quality of the equipment, the quality of the execution of the different activities and on the quality of work management. Analysis of major accidents and catastrophes generally document that a series of unfortunate coincidental events have taken place prior to such incidents, and that adequate actions were not taken in the first critical phase of fighting them. Knowledge, information availability and awareness are key factors and important safety criteria in the daily achievement of plant safety.

No operator can stay on alert all the time, waiting for a potential emergency situation where he is expected to intervene. It is therefore the task of the system to alert the operator when an exception to the normal situation occurs, identify where it has happened, and support the operator in dealing with it.

800xA Operations offers a complete range of devices, subsystems and functions for safety supervision and control. From rugged, yet competent, control panels for field mounting, through full-functionality PC-based work stations, to multi-pane projection systems offering an outstanding overview of the entire plant and process.

All basic functions required in a safety system are predefined, requiring only a few steps to be put into displays for both information provision and operator intervention.

Unique to 800xA Operations is its ability to gather data from multiple plant sources and transform it into relevant user information. For example, it allows users, such as safety operators, maintenance technicians, engineers, and safety managers, to organize information and navigate throughout the system intuitively in the context of their job functions, never having to be bothered by irrelevant information.

Thereby, root causes of problems can quickly be identified and analyzed, allowing users to react to specific process- and safety-related events promptly, yet safely.

For more information on 800xA operator interaction solutions, please refer to the System 800xA Operations Overview.

800xA Information Management features collect, store, and retrieve historical process and business data from control, safety and related systems, and transforms that data into meaningful information. This helps in mapping out plans to achieve significant productivity improvements. 800xA Information Management features are also integrated with commercial data analysis and business systems. Standards such as ODBC, OLE DB and SQL help to provide access to all real-time and historical data, regardless of where it resides in the process or business network.

For complete 800xA Information Management details, please refer to the System 800xA Information Management Overview.
Sequence of events and alarms (SOE): By time-tagging events with millisecond accuracy, Event and Alarm can always identify the root causes of trouble. An event is a state of change of a variable in the Safeguard database. An alarm is an event which requires acknowledgment by the operator. Alarm functions include process sectioning, first up alarm, and alarm priorities.

Object signal display: Every field device connected to the Safeguard 400 controller has its individual record in the Safeguard 400 database, identified by its tagname. On the operator workplace, a corresponding predefined object display is available for real-time information and dialogue with the object.

Bypass management: During normal process supervision, maintenance and test activities, it is often necessary to inhibit a specific safety function from being activated. In Safeguard 400, specific inputs may be inhibited and outputs bypassed through standardized operator dialog. Care has been taken in the design of access control, safety integrity and bypass status overview of Safeguard 400 to combine ease of operation with maximum safety.

Diagnostics: Every component in Safeguard 400 controllers is automatically included in the system status supervision function. Failure in components like CPUs, I/O boards, communication boards, power supplies, etc., will automatically generate a system alarm. Predefined, dedicated system-status displays provide detailed information about status and location of the components.

Query-based status list reporting: The distributed, object-oriented signal database in Safeguard 400 makes it easy to manually set up event-triggered query-based reports. In a safety system, such a function is crucial to presenting instant or periodic safety-status overview reports.
Evolution through Enhancement

Easily Configured with Various Control Systems

Safeguard 400 Series offers several communication solutions for interfacing with the plant’s installed control systems. The full range of real-time, diagnostic and historical safety data, generated by the Safeguard 400 Series system, can be made accessible to the existing control system’s operator consoles; a solution offering many benefits in safety and economy.

Safeguard 400 Series safety controllers, however, are always complete and independent function units, which means that safety will never depend on communication with other systems.

Multivendor Plug-in Modules

When a Safeguard 400 controller is to be configured for communication with existing plant controllers, this is quickly and safely achieved, using plug-in interface modules. Each of these modules supports a specific, standard, communications protocol, e.g. MODBUS, RCOM, EXCOM, or a proprietary protocol of a specific control system. A library of ready-made communication protocols is available.

Figure 18. Multivendor plug-in interface modules make it easy to communicate with process control systems from other suppliers.

OPC

The safety operator workplace is an OPC client. The OPC protocol makes it easy to connect third-party systems to a network, thereby achieving full integration. The upload function of the workplace retrieves process data from all connected OPC-compliant controllers, from ABB or from third parties. This data includes not only process but also alarm and event data.

Built-in Networking

For direct connection to a plant-wide communication network, the ABB Operator Workplace offers built-in networking with support for TCP/IP.
Safety Services

ABB’s safety-critical systems team provides a wide range of engineering services to a broad spectrum of users globally. The strengths of this team are founded on proven knowledge of engineering issues from an end-user/operator perspective and on on-going access to the capabilities of the total supply chain.

ABB Safety Services assists in the practical implementation of all phases of the IEC 61508 / 61511 safety lifecycle for both existing and new facilities by applying proven techniques and working methods including:

- Safety Integrity Level (SIL) assessments
- Software tools supporting the safety lifecycle
- Identification of safety critical elements / functions
- Safety lifecycle audits
- Functional safety assessments
- Independent validation & verification
  - Hardware / software design
  - System integration
- Support for strategies to implement IEC 61508 / 61511
- Support for in-house training and awareness programs.

For complete Safety Services details, please refer to the System 800xA Safety Services Overview.