

Safety Manager



Honeywell's Safety Manager™, part of the Experion® Process Knowledge System (PKS), enhances process safety by protecting people and plant assets.

Safety Manager combines Honeywell's proven Quadruple Modular Redundancy (QMR®) 2oo4D technology with Honeywell's extensive process safety management expertise in integrating process safety data, applications, system diagnostics and critical control strategies.



Honeywell's TUV IEC 61511 and IEC 61508 certified solution provides the optimal level of safety and process integration while still maintaining functional safety separation. Through operational integration with Experion, safety systems are unified into one architecture, offering a unique opportunity to improve both safety and process availability.

Experion provides unprecedented connectivity through all levels of process and business operations to optimize work processes, improve routine maintenance efficiencies, enhance safety management and release personnel from manual processes.

Safety Manager delivers the following benefits:

- **Safe and Secure** – Every Safety Manager includes an embedded and certified safety firewall to protect the critical Safety Instrumented System (SIS) layer of protection from cyber attacks and disruption of service.
- **High Availability Architecture** – Honeywell's field-proven QMR 2oo4D architecture provides the highest availability with a fail-to-safe architecture. Applying QMR technology allows uninterrupted process operation in the event of any system degradation.

- **Easy, Intuitive, Error-Free Engineering and Modifications** – Safety Builder, an intuitive and comprehensive configuration tool, provides plant-wide management of safety-critical databases and application programming for easy safety network design. TUV-approved, menu-driven online modifications prevent errors while maintaining and optimizing the safety application.
- **Operational Integration** – Experion Safety Manager delivers best-in-class integration developed with Honeywell's unparalleled experience in providing integrated safety systems.
- **Defense-in-Depth** – SafeNet and remote distributed Safety Manager provide the ability to design defense-in-depth safety strategies that maximize safety and security while minimizing risk and scope-of-loss concerns that come with traditional remote I/O technologies.

Built on QMR Technology

Safety Manager is based on the unique and field-proven QMR diagnostic-based technology with a 2oo4D architecture. QMR enhances system flexibility, increases diagnostic messaging capabilities and improves system fault tolerance for critical applications. It enables the handling of multiple system faults within Safety Manager, matching the needs of critical control applications.

In addition, Safety Manager provides the basis for integrating Safety Integrity Level (SIL) rated field sensors and valve actuators, ensuring that safety functions are well established to protect complex and hazardous processes. Safety Manager integrates SIL 1-3 safety transmitters (such as Honeywell ST3000 and STT250) or safety valve positioners for improved safety and field asset management.

Compliance to Safety Standards

A major requirement for compliance to IEC 61511 and IEC 61508 is the availability of a change history of applications. With Safety Builder, change history is efficiently tracked with the Safety Audit Tracker through an automatically enabled audit trail. It tracks all changes performed on an application. Difficult procedures or extensive loggings are not required. The Safety Audit Tracker, together with the Application Verification Tool, are the only tools required.

Safety Manager complies with the following international standards:

- For burner management: NFPA 85, 86, VDE 0116
- For emergency shutdown: IEC 61508, ISA S84.01, DIN V 19250, UL, FM, ATEX
- For fire and gas: EN54-2, NFPA 72, Lloyd's Register and offshore installations ABS

With all SIL-3 safety compliance tools, hardware and software, Honeywell's Safety Manager provides excellent protection for safety applications across multiple industries throughout the entire life of an installation. Together with Experion or any other process control system, Safety Manager provides the basis for critical control and safety unification, reducing risks and installed costs, and improving plant safety while increasing plant uptime.

Improved Engineering Environment

The Safety Builder software improves engineering and design efficiency. With simple drag and drop functionality, a complete and complex network can be designed within minutes without programming, saving valuable engineering and testing time. The complete network design is available as a one-page view without requiring additional documentation.

An integrated editor facilitates fast and effective application design, allowing clear and distinct views of all logic with full compliance to IEC 61131 standards. Logic inputs, outputs and symbols are placed with drag and drop functionality from the toolbar and are easily configurable.

The UniSim[®] simulation environment for Safety Manager supports offline simulation. In the early implementation phase of a project, the design of the safety functions can be validated against the safety requirements without the actual hardware being present. It supports step by step simulation, freezing the application and building snapshots. This simulation is integrated into the overall UniSim architecture supporting plant-wide simulation.

Improved Process Availability

Applying QMR technology in Safety Manager delivers unlimited runtime for a single channel operation. This increases process availability up to 20 percent, allowing uninterrupted process operation in the event of any system degradation. With the redesigned and simplified online system modification procedures, a plant benefits from significantly improved application and system upgrades during plant startups and throughout the life of the process operation.

Improved Operation and Maintenance Performance

Safety Manager unifies critical safety process data with process control information, providing single-window access for operation and maintenance. When connected to the Honeywell Fault Tolerant Ethernet (FTE) network through TUV SIL-3 approved Universal Safety Interfaces, multiple Safety Managers are unified into one safety system architecture.

Safety Manager integration delivers fast, safe and reliable data exchange with Experion, enhancing operator and maintenance performance. In addition, Safety Manager extends the system proof test interval with inherent, extensive system self-testing and diagnostic capability, reducing operational and maintenance costs. Integrated sequence of events (SOE) functionality for all process and safety-related activities supports analysis at a glance.

Safeguards are built into Safety Manager to eliminate the possibility of systematic failures in automation system design. Systematic failures are caused by errors made during the design, planning, construction, operation and decommissioning of the system. A systematic failure in the design of a common tool can result in an unsafe reaction of both the safety and control systems.

Safety Through Separation

Safety and control systems must be integrated to allow for a smooth and safe plant operation, while still maintaining a safe separation where appropriate. Dedicated safety-related functions such as the actual application (either the application during design or the application running on the dedicated safety hardware) must stay segregated and must be subject to high safety integrity.

Secure Separated Databases

Within Honeywell's unique solution, separate databases store the safety and control strategies, and separate software modules are available for safety and control through dedicated tools such as Safety Builder and Control Builder. Maintaining separate tools with separate databases prevents unauthorized changes or corruptions, decreases safety risks and prevents common cause failures.

Database Integrity and Security

All Safety Builder modules are protected from viruses and harmful hacking by a built-in protection mechanism that checks the integrity of the software before installation, after installation and during run time. The integrity of all data accessed through Safety Builder, as well as the integrity of an application loaded into Safety Manager, is protected against unwanted changes to protect the entire safety application.

Managed and Protected Database Environment

A unique, secure login scheme protects Safety Manager from off- and on-process changes. This login scheme uses a dedicated protection mechanism with several access levels for the engineering application, loading of the application in the controller and forcing points in Safety Manager. A user expiration mechanism downgrades the access level after a user-defined period of time elapses to protect the application from changes when Safety Builder is unmanned over a specified period.

Dedicated Software and Hardware

Using dedicated and specifically developed hardware and software, according to the IEC61508 safety standard, reduces the risk of a common cause failure. Using dedicated hardware and software for both safety and control protects the safety system from any defects in the control-related operations. In addition, the safety and control strategies are developed by different groups using dedicated methods.

Conversely, using the same hardware or software for both safety and control increases the possibility of systematic controller failures, including those that result from design errors. A clear separation reduces the effort for testing and designing safety systems.

Secure Environment

As the usage of Ethernet networking and commercial-off-the-shelf (COTS) software increases, it becomes more important to keep safety and control separate. These COTS technologies are not subject to a dedicated protection method, such as IEC61508.

Personal computers, servers, mobile phones and other electronic equipment connected to the Internet are vulnerable to harmful actions, such as viruses or denial-of-service attacks. Maintaining separate control and safety systems provides a secure environment with additional layers of protection.

In addition, Honeywell's Safety Manager is protected from the outside world by a hardware firewall. This firewall isolates the safety application during runtime execution from external devices. Those devices can never jeopardize the safety or availability of the application. By using a unique proprietary protocol, the data integrity between control and safety is protected and guaranteed.

Dedicated Firmware

Using dedicated firmware for safety and control ensures that safety is embedded into the safety system—no additional programming is needed to establish the required safety level. Strategies with a common platform for safety and control require that safety be built into the system. This customized safety level is a manual process, prone to errors and requires fundamental knowledge of the safety system to establish the required safety functions without jeopardizing the safety integrity of the application.

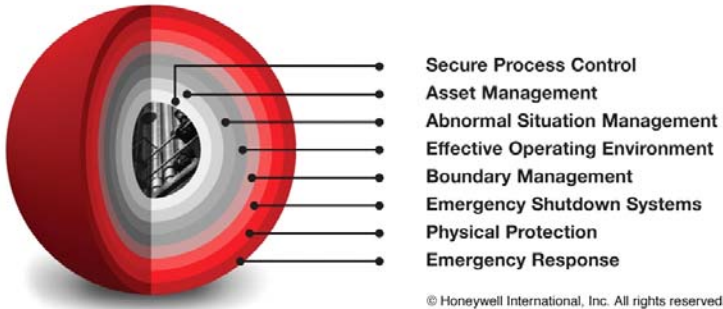
Honeywell's unique integrated safety and control offerings have always held true to the separation principles. As long ago as 1996, Honeywell offered an integrated control and safety solution driven by the separation principle—hardware and software diversification, integrated operator interface, integrated data processing, integrated analysis and integrated alarm management.

The operational integration provided with Experion and Safety Manager allows plant personnel to have a seamless interface to the process, while maintaining safe separation. It makes no difference whether the actual strategy is running in the process controller, Safety Manager or on a higher level—all required information is available on the operational level. This allows for a wide range of applications to be monitored plant-wide from any operator console, from rotating equipment and compressor protective systems to emergency shutdown systems and large fire and gas applications.

A complete overview of all information needed from the operator's point of view is available on the operator stations through Safety Manager and Experion operational integration. This communication architecture, supplied by Honeywell, delivers

a scalable solution, from a small control and safety network to huge plant architectures with over 100,000 monitored I/O points, through one integrated solution. Safety Manager interoperability with the SafeNet protocol extends the functionality of one Safety Manager and allows for plant-wide implementation, binding the separate functionalities into one safety application with different protection layers.

Honeywell's Layered Approach to Plant Safety



Safety Services

Honeywell's service offerings go beyond supplying hardware and software, establishing a unique safety knowledge community located in our expertise centers around the world in Europe, South Africa, Asia, India, Australia and the U.S. More than 200 safety engineers employed in these centers offer a wide range of consulting, project and lifecycle support services. Honeywell's consulting and lifecycle management services include:

- Process hazards and risk assessment
- Safety Integrity Levels classification

More Information

For more information on Experion and Safety Manager, visit www.honeywell.com/ps or contact your Honeywell account manager.

Automation & Control Solutions

Process Solutions

Honeywell

2500 W. Union Hills Dr.

Phoenix, AZ 85027

Tel: +1-602-313-6665 or 877-466-3993

www.honeywell.com/ps

- IEC61508 and IEC61511 training
- Safety requirement specifications development
- Front-end feed studies with customers to jointly develop their requirements
- IEC61508, IEC61511 and ISA S84 compliant solutions development
- Safety Instrumented Systems implementation
- Live, hot cut-over implementation and execution of revamp projects
- Installation and commissioning
- SIL verification
- SIL validation
- Periodic proof-testing
- System maintenance
- Solution Enhancement Support Program (SESP)
- Parts management

Experion®, QMR® and UniSim® are registered trademarks of Honeywell International Inc. Safety Manager™ is a trademark of Honeywell International Inc.