

## Safety Manager



**Honeywell's Safety Manager, part of the Experion Process Knowledge System (PKS), enhances the safety, reliability and efficiency of critical processes.**

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

Honeywell's IEC 61511 and IEC 61508 SIL 3 TUV certified solution provides the optimal level of safety and process integration while still maintaining functional safety separation as mandated by those standards. Through Experion operational integration, all systems are unified into one architecture, providing a unique opportunity to improve safety, process availability and efficiency

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.

### Benefits

Safety Manager delivers the following benefits:

- **Safe and Secure** – Every Experion 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 safe architecture. Applying QMR technology allows uninterrupted process operation in the event of any system degradation or on-process modification without jeopardizing the SIL 3 level.
- **Easy and Intuitive Engineering and Modifications** – Safety Builder, an intuitive and comprehensive configuration tool, provides plant-wide management

of safety-critical databases and application programming for easy network design. TUV-approved, menu-driven online modifications prevent errors while maintaining and optimizing the safety application.

- **Operational Integration** – 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 that are not protected properly.
- **Safety Networking** - The networking capabilities of Safety Manager are unsurpassed. Up to 1024 redundant nodes can be included in one safety network, allowing small remote I/O solutions as well as large integrated safety applications. The SIL 4 certified SafeNet communication protocol guarantees fast and safe communication over any media and distance. The remote management capabilities support centralized management of all connected safety systems.



- **SafeNet Flexibility** - SafeNet can run over any network, such as on a dedicated separated safety network as well as the Honeywell Fault Tolerant Ethernet (FTE) network infrastructure. SafeNet is the only SIL 4 certified communication protocol available in process networks today.
- **Self-learning** – Replacing any module, including the safety processor (QPP), is possible when the plant is in operation and data and programs are automatically copied from the running processor. This is applicable for application configuration as well as embedded system software. There is no manual loading required which simplifies handling and avoids problems. The total system will continue to meet the stringent SIL 3 requirements.
- **High Performance** – The Experion Safety Manager has been optimized to manage large applications such as fire and gas with over 1,000 I/O as well as high-speed applications with fast processing requirements of cycle times well below 100 millisecond.
- **Robust Integration Interface** – The Peer Control Data Interface (PCDI) supports peer-to-peer communication between the Safety Manager and the C300 controller over a redundant FTE infrastructure. This supports integrated safety and control, including sharing transmitter data between the C300 controller and Safety Manager to save installed and operational costs. Multiple C300 controllers can be connected to multiple Safety Managers with a fault reaction configuration per point. PCDI allows for alarm suppression, automatic bypassing and interlocks between shutdown and control functions as well as “soft landing” in case of process upset.

### Built on QMR Technology

Experion Safety Manager is based on the unique and field-proven QMR diagnostic-based technology with 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 Experion Safety Manager, matching the needs of critical control applications.

In addition, Safety Manager provides the basis for integrating SIL-rated field sensors and valve actuators, ensuring that safety functions are well established to

protect complex and hazardous processes. It 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 automated embedded Application Verification mechanism is all that is required.

Safety Manager complies with the following international standards:

- For burner management: NFPA 85, 86, VDE 0116
- For emergency shutdown and other critical applications: IEC 61508, IEC61511, 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 hardware and software compliance tools, Safety Manager provides excellent protection for safety applications across multiple industries throughout the entire life of an installation. 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 on 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.

Honeywell's UniSim<sup>®</sup> 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 to Safety Manager delivers unlimited runtime for a single channel operation. This increases process availability, allowing uninterrupted process operation in the event of any system degradation. The redundancy built into Safety Manager is for availability only. With a four-step online system modification procedure, a plant benefits from significantly improved application and system upgrades during plant startups and throughout the life of the process operation. Any on-process modification to the software can be carried out remotely without physical presence to the system. Those changes will not affect the running process

I/O faults are detected and isolated on a per channel basis and immediately reported to the appropriate level. This minimizes the time to repair and further increase the robustness.

### **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 can be 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 smooth and safe plant operation, while still maintaining a safe separation where appropriate. Dedicated safety-related functions such as the actual safety 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 during the entire lifecycle.

### **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 accidental or unauthorized 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, as prescribed by the IEC61508.

Personal computers, servers, mobile phones and other electronic equipment connected to the Internet are vulnerable to risks, 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, Safety Manager is protected from outside threats by an embedded 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. With this embedded firewall and the use of a SIL 4 certified proprietary protocol, the data integrity between control and safety is protected and guaranteed.

### **Safety Inside**

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. Since 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 that is under control, while maintaining safe separation. From an operational perspective, it makes no difference where the application is running. All required information is available to the operator. This allows for a wide range of applications running in Honeywell equipment to be monitored plant-wide from any operator console, from rotating equipment and compressor protective systems through emergency shutdown systems to 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 Experion Station. 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.

## 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 North America, Europe, South Africa, Asia and Australia. Over 200 certified 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
- IEC61508 and IEC61511 CFSE 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 cutover 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.

## For More Information

To learn more about Safety Manager, visit [www.honeywell.com/ps](http://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: 877.466.3993 or 602.313.6665

[www.honeywell.com/ps](http://www.honeywell.com/ps)

PN-08-15-ENG  
May 2008  
© 2008 Honeywell International Inc.

**Honeywell**