Honeywell

Product Information Note

Safety Manager

Honeywell's Safety Manager, part of the Experion® Process Knowledge System (PKS), enhances the safety, reliability and efficiency of critical processes. Experion® PKS – The Knowledge to Make it Possible.

Safety Manager combines Honeywell's proven Quadruple Modular Redundancy (QMR®) 2oo4D technology with 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 TÜV 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 operationally integrated 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

- **Safe and Secure** – Safety Manager is designed to be securely integrated into customer systems and has passed very rigorous security testing as defined by ISA Security Compliance Institute (ISCI).

  Safety Manager was the first safety system to achieve Embedded Device Security Assurance (EDSA) certification. ISCI developed this certification within the framework of the ISA Industrial Automation and Control Systems security standards (ISA 99). Because of the built in protection mechanisms, the Experion Safety Manager is protected 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. The optional Safety Manager A.R.T. (Advanced Redundancy Technique) provides additional benefits for locations where timely maintenance is not available.

- **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. TÜV-approved, menu-driven online modifications prevent errors while maintaining and optimizing the safety application.

- **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.

- **Safety Networking** - The networking capabilities of Safety Manager are unsurpassed. Up to 1024 redundant nodes can be included in one safety network, acting as one integrated safety solution. 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 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, is possible when the plant is in operation, and data and programs are automatically copied from the running processor. 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** – Safety Manager has been optimized to manage large applications with over 1,000 I/O as well as high-speed applications with fast processing requirements of cycle times well below 100 milliseconds.
- **Universal Safety I/O** – Safety Manager Universal Safety I/O enables maximum architectural flexibility and lowest cost of

ownership when safety is required at distributed locations. It has the unique feature that each channel can be configured individually to a different I/O type. Every Universal Safety I/O module has a capacity of 32 freely configurable channels, enabling savings on both installation and operational costs. By using soft-marshalling, the Universal Safety I/O module can be mounted close to the process unit, eliminating the need for marshalling panels, homerun cables and reducing or eliminating field auxiliary rooms. This approach is ideally suited to highly distributed applications such as oil and gas upstream applications, and reduces cost while increasing availability and efficiency. This reduces overall capital expenditure, as well as maintenance costs.

- **Localized Safeguarding** - With Universal Safety Logic Solver, the safety application can be distributed into the field close to the process unit while maintaining a transparent overview of the overall safety application. The unique feature of this Universal Safety IO module is the fact that besides being an IO module to Safety Manager, it can execute the safety application locally. Safeguarding the process even in the event communications to the Safety Manager are interrupted.
- **Standardized Solutions** - Universal Channel Technology enables Universal Cabinet designs to be standardized, significantly reducing engineering cost and schedule when applied broadly across a project.
- **Advanced Experion Integration** – Supports Safety Manager integration in Experion, providing an integrated safety and control solution. It enables, for example, transmitter data sharing between the CEE (Control Execution Environment) controllers and Safety Manager, via direct peer to peer communication, to save installed and operational costs. Peer to peer communication further allows for alarm suppression, automatic bypassing and interlocks between shutdown and control functions as well as “soft landing” in case of process upset. It also provides easy operator access and full Console Station support. As part of the “enter data only once” philosophy, the Experion-related properties are configured from the Safety Builder tool simplifying maintenance and reducing total cost of ownership.
- **Built on QMR Technology** – 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.

- **Optimized field maintenance** - Without the need for extra infrastructure or engineering, HART devices are integrated within Honeywell's Field Device Manager. This provides all required data for field asset management. To prevent inadvertent device changes, the safety manager prevents FDM from writing parameter changes unless the device safety lock has been disabled from Safety Builder.

Compliance to Safety Standards

A major requirement for compliance with 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. 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, EN50156
- 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 safety while increasing uptime.

Optimized Engineering Environment

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.

Through the Safety Manager simulation mode any application can be loaded and tested on a minimum size system, a tool that facilitates easy application design and testing. The simulation mode also allows execution of online modifications and testing of all communication interfaces.

In absence of a Safety Manager system the Honeywell's UniSim® simulation environment for Safety Manager supports offline simulation as well. It can help in the early implementation phase of a project or as part of a plant-wide system simulation. It supports step by step simulation, freezing the application and building snapshots.

Optimal Process Availability

Applying QMR technology to Safety Manager delivers unlimited runtime for single channel operation. This increases process availability, allowing uninterrupted process operation in the event of any system degradation. Without incurring any process downtime, the system can be kept up to date with the latest system software as well as application changes or additions through a four-step online system modification procedure The on-process modification to the application can be carried out remotely without physical presence to the system.

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 increases system robustness.

Integrated Operation and Maintenance

Safety Manager unifies critical safety process data with process control information, providing single-window access for operation and maintenance. When connected to the Honeywell FTE network through TÜV 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 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.

- **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 in accordance with 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 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** - It is crucial that critical control and SIS are protected from intentional or accidental cyber threats. In general, functional security in combination with functional safety is critical to assessing the overall integrity of a SIS.

  Safety Manager architecture is secure by design and is certified to the Embedded Device Security Assurance program as defined by the ISA Security Compliance Institute. Adherence to this standard provides assurance of safety, security and robustness, meeting stringent industry best practices and performance benchmarks.

  In addition, Safety Manager is protected from outside threats by an embedded certified hardware firewall. This firewall isolates the safety application during runtime execution from external devices so they can never jeopardize the safety or availability of the application. With this firewall and the use of a SIL 4 certified proprietary protocol between safety managers, 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 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 application. This customized safety level is a manual process and requires fundamental knowledge of the safety system to establish safety functions without jeopardizing the integrity of the application.

  Honeywell's integrated control and safety solution is driven by the separation principle—hardware and software diversification, integrated operator interface, integrated data processing and 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. This allows for a wide range of applications to be monitored plant-wide from any operator console. A complete overview of all information needed from the operator's point of view is available through Experion Station or Experion Console Station. This communication architecture, supplied by Honeywell, delivers a scalable solution, from small control and safety networks to huge plant architectures with over 100,000 monitored I/O points. Interoperability of Safety Manager 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.

Engineering Excellence

Honeywell's Global Safety Discipline program enables consistent project execution excellence across Honeywell engineering locations. TÜV certified procedures and resources guarantee a global and transparent safety project execution by using certified standard builds, including templates, guidelines solution libraries, checklists, methodologies and tools.

Safety Manager HMIWeb Solution Pack shapes and faceplates provide all projects with a highly flexible and functional library, enabling maximum advantage of the principles of safe and effective operations as described by the Abnormal Situation Management (ASM) Consortium.

Honeywell Safety Services

Honeywell's 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, including:

- Safety system audits
- Process hazard and risk assessment
- SIL classification
- IEC61508 and IEC61511 CFSE training
- Safety requirement specification development
- 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

For More Information
To learn more about Honeywell's Safety manager, visit our website www.honeywellprocess.com or contact your Honeywell account manager.

Honeywell Process Solutions
Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB UK

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com

PN-12-25-ENG
March 2013

Honeywell