White Paper

Honeywell

Honeywell Process Solutions

# Integrating Control and Safety with Secure System Segregation

**Table of Contents**



## Table of Figures

## Introduction

Honeywell delivers operational integration with critical system segregation. With secure integration at the control data and operator levels, Honeywell provides a common operational interface to the process and equipment for both control and safety. And, with integrated simulation tools, we're able to verify and optimize hazard identification, train operators and verify the responses. A truly integrated system delivers:

- Integrated operational interface
- Integrated peer control
- Integrated diagnostics
- Integrated postmortem analysis
- Integrated fire and gas system
- Integrated power supplies
- Integrated modifications
- Integrated simulation and optimization

Safety Manager integrates with the Experion PKS process controller to unify Honeywell's safety controller with its equally reliable Experion platform. This integration provides plant-wide Safety Manager point data, diagnostics and system information, alarms and events, operator displays and sequence of event information to any Experion Station. The result delivers:

- Fast, high speed and bi-directional data exchange
- Direct communication with no Experion server or other equipment required
- The ability to use currently available infrastructure with no additional or new hardware needed
- Built-in physical and logical redundancy
- Flexibility with multiple C300 controllers that can connect to multiple Safety Manager controllers
- Fault reaction configuration per point
- Safety Manager point data is instantly available for C300 control functions

Integrating safety with control provides multiple benefits to end-users:

- Minimize intervention and shutdowns and recover more easily from process upsets
- Reduce hardware and installation cost
- Easy configuration with preconfigured function block selections

Honeywell's approach to integration avoids adding extra equipment, such as serial interface hardware, which adds cost for:

- Serial interface licenses
- Serial interface configuration software
- Power supplies
- Racks
- Switches
- Ethernet cabling
- Cabinet square footage
- Spare parts
- Engineering hours to configure
- Engineering hours to maintain

## A Full Range of Solutions

Honeywell offers products and services that map against the entire the 61511 lifecycle, from a pre-assessment that provides a quick overview of the safety status of the facility to decomissioning services. A full range of safety consultancy services help customers manage all their safety and risk management needs. Honeywell safety experts have the experience to guide and assist end users in the implementation of international safety standards such as IEC 61508 / IEC61511 and ANSI/ISA S84.01.

Honeywell can help customers:

- Formulate and manage their safety lifecycle model
- Carry out hazard and risk analysis and definition of safety functions
- Define safety requirements
- Provide expertise on failure rate assessments
- Perform safety and availability calculations
- Provide advice on optimal proof test intervals

## Foundation for the Integration: Safety Manager

Honeywell's Safety Manager is a robust, safe, high availability controller for Safety Instrumented Systems (SIS) applications that delivers enhanced safety assurance for industrial plant operators. Safety Manager helps lower the cost of safety and improves plant performance by reducing the risk of safety incidents, maximizing production uptime, reducing the cost of compliance and providing productivity tools that help manage safety in your plant.

Using innovative and field proven QMR (2oo4D) diagnostic based technology, Safety Manager is a key component in delivering a layered approach to plant safety, providing applications such as emergency shutdown, process shutdown, fire and gas detection, burner management, compressor control, pipeline management or any critical safeguarding in the process industry. End-users can achieve 2oo4D (2 out of 4 with integrated diagnostic to a > 99.9% coverage) even without the second CPU, providing a fully SIL 3 certified solution which allows continuous production.

Safety Manager is a user-programmable, modular, microprocessor-based safety system which can perform a wide range of critical process control and safety instrumented functions, including:

- High-integrity process control
- Burner/boiler management systems
- Process safeguarding and emergency shutdown
- Turbine and compressor control and safeguarding
- Fire and gas detection systems
- Pipeline monitoring

## Building the Integration

Honeywell's unique integrated safety and control offerings have always held true to the separation principles. Since 1996, Honeywell has 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.

Operational integration 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 plant-wide 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 delivers a scalable solution, from a small control and safety network to large plant architectures with over 100,000 monitored I/O points through one integrated solution. Safety Manager interoperability with the SafeNet communication network 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 Manager integrates the sequence-of-event (SOE) features as supported by Safety Manager into the Experion Server. Safety Manager supports SOE for digital inputs and outputs, analog inputs and outputs and marker points. Each tag name that has been SOE-enabled is time-stamped by the Safety Manager controller and reported to the Experion Server, where it is incorporated into the standard SOE list which allows for improved search, filter and automated archive functionality. Standard SOE displays are available to view the events as they are reported.

In addition, peer-to-peer communication through the Peer Control Data Interface (PCDI) between Safety Manager and C300 controllers can easily be established. This allows for a fully redundant, robust, fast and cost-effective communication between process safety and process control without jeopardizing the IEC 61508 segregations requirements. PCDI communicates over the existing redundant FTE network for peer-to-peer communication between Safety Manager and C300 controllers without the need of any additional equipment.

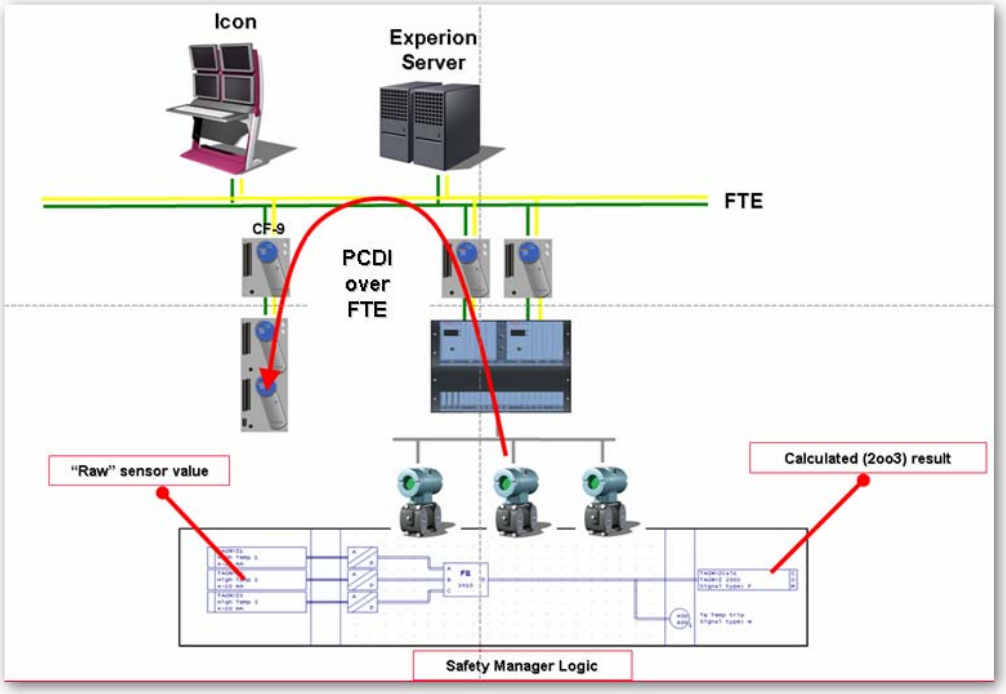


**Figure 1**

Using PCDI to connect to Safety Manager allows for a seamless peer-to-peer communication between the process safety and process control and benefits from the existing redundant FTE infrastructure. Point data from the Safety Manager can be used in any C300 controller on the same FTE community.

Sharing data between Safety Manager and C300 controllers supports the following scenarios:

- Safety Manager point data is instantly available at the process control level. This supports using field sensor data originating from the safety layer in the process control layer to reduce the installed field sensor equipment by 30%, thus saving over US$750,000.00 on an average process unit. Reducing the installed field equipment further reduces maintenance costs.
- A Safety Manager-managed process upset supports a “soft landing” of the downstream process with the C300 Controller. This avoids the downstream ESD demand, manages the downstream process shutdown and provides an easier process restart after an process upset. This principle will increase process uptime and decrease the consequence of a process trip. This can result in a cost reduction of US$100,000 a year for a process unit.
- Automatic process interlock from shutdown valve to control valves will keep the PID from winding up and the control valve from ramping wide open to prevent a surge when the shutdown valve is subsequently opened.
- Automatically bypassing a low flow or pressure trip on a pump discharge based on the running status of the pump.
- Automatic suppression of alarms in either the C300 Controller or Safety Manager when some process units are out of service or a trip is in bypass. For example, when the Safety Manager trips a pump, it will suppress any process control system un-commanded change alarms.
- Automatic opening and closing of shutdown valves during a compressor purge sequence.

## Communication Networking

Safety Manager networks provide the means to decentralize process safeguarding with central process monitoring and control capabilities. In a network, multiple Safety Managers are interconnected through dedicated Ethernet (or serial) communication links. This communication is based on the Honeywell proprietary, TÜV-approved SIL 4 SafeNet communication protocol. SafeNet is the only SIL4 certified protocol available in the process industry today. The SafeNet protocol includes a high level of error detection and recovery, and built-in redundancy which makes it suitable for exchanging safety-related information while maintaining optimum availability.

Communication within Safety Manager networks is based on the peer-to-peer concept. With this concept, data communication with any connected Safety Manager in a SafeNet topology is possible.

The SafeNet concept supports safety solutions in line with the plant design, with every independent process unit being safeguarded by a separate Safety Manager. This minimizes the risk of nuisance plant trips during unit maintenance.

Although SafeNet can run on any medium, including FTE, Honeywell recommends using a separate physical medium. A dedicated safety network provides the right level of architectural communications segregation. To ensure continued availability:

- All safety functions will continue even if a complete process control collapse occurs
- A dedicated network for safety guarantees availability of redundant safety functions in case of communication problems on FTE network (no nuisance alarms)
- Complete segregation of process control from process safety
- No common cause network failures

## Mitigate Risk with a Layered Approach

Honeywell employs a layered approach to safety and security. 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.

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 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 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. Wit this embedded firewall and the use of a SIL 4 certified proprietary protocol, the data integrity between control and safety is protected and guaranteed.

## Integrated Diagnostics Reduce Intervention and Shutdowns

Honeywell's safety system provides integrated diagnostics. With Safety Manager, the diagnostics that monitor the health of the circuitry runs continuously as an integrated part of the Safety Manager firmware.

The next best alternative is far from attractive. If the diagnostics are only run at startup, periodic intervention on the part of an application engineer called proof-testing, always a non-value add activity, is required. In order to maintain a SIL 3 installation, each safety controller must be taken off line, shut down and restarted every time the proof test interval expires. Depending on the application, this could be once every quarter in order that the non-integrated diagnostics are run. For a single controller this means that the plant must shutdown, For a redundant controller, a manual switchover from primary to hot stand-by must be initiated, which can cause a nuisance trip. Also will the switchover result in nuisance alarms to the operators. Initiating the proof-test and evaluating the result is the responsibility of the user. This is an incremental costs incurred every year. This can get up to $350,000 for an average refinery.

But that cost is likely small as compared to the potential cost of a plant shutdown. While this proof-testing is being conducted, the safety system is not ensuring the safety of the plant; the operator is. Also, in case of a redundant controller, a manual switch must be made to stop the primary controller and switch over to the secondary controller. This can result in a plant shutdown often costing at least $500,000 per occurrence.

For Safety Manager, the proof-test interval is greater than 15 years.

## Integrated Fire and Gas Solutions Reduce Installed Cost

One of the main tasks of a fire and gas system is to alert personnel of potential safety hazards and to initiate the evacuation of buildings and areas through annunciation devices. While most safety system outputs are normally energized outputs, these annunciation devices are of the "energize-for-action" type.  What this means is that the safety system must have purpose-built field-monitoring output modules in order to properly integrate with a fire and gas system. Those field-monitoring output modules will actively check the wiring from the SIS output channel to the fire and gas field equipment such that malfunction of the connected device, lead breakage or short circuit in the wiring can be detected.

## Integrated Power Simplifies Project Implementation and Cost

Honeywell's Safety Manager goes a step further than the competition by providing power for field devices. This makes project implementation easier. A separate sourcing of double over-voltage protection power supplies is avoided. Appropriate power supplies are difficult to find and add unneeded cost to the project. If you need to source external power supplies, you can plan on an additional cost of $10 per device. For an average refinery this could add up to $140,000.

## Integrated Modifications Eliminate Offline Changes

Safety Manager delivers a fully tested and TUV-approved infrastructure for implementing online modifications to the safety controller configuration. It's not realistic to expect that once a safety system is commissioned, it doesn't change. In fact, in the months just following a project implementation, it is not unusual for hundreds of modifications to be made.

Some safety systems do not allow for integrated modifications. Instead, the system must be taken offline, modifications installed and then full functional testing needs to occur before the system (and process) can be started. If online changes are supported, some are limited to set-point modifications only.

Some claim that changes can be made, but have huge disadvantages and even safety risks from the moment a change is initiated until the complete functional test has completed, the process operators are fully responsible for the safety of the unit. This could take up to a couple of hours. One of the reasons safety systems have been developed and implemented is to remove the "human factor" from the

safety layer of dangerous processes. A faulty decision by an operator can result in a plant shutdown often costing at least $500,000 per occurrence. If an operator does not judge correctly once a safety critical situation occurs, the safety of a plant is at stake.

Honeywell's Safety Manager provides TUV approved on-process migration that has no limitations on points, modules, chassis or complete systems.

## Integrated Simulation

By using a fully integrated simulated system (process, control and safety) you can verify and optimize hazard identification, train operators and verify if the response are correct. This helps

- Improve hazard identification and response planning
- Improve execution quality and productivity
- Analyze impact of changes on plant safety

Safety Manager is integrated with Honeywell's UniSim simulation package to:

- Provide offline development platform with configuration and runtime debugging environment
- Allow Safety Manager application to be evaluated before it is commissioned in the plant
- Support flexibility by functioning on an Experion Station without requiring Safety Manager controller hardware
- Reduce engineering costs with intuitive displays and integration under Experion Configuration Studio to provide a common development platform

This integration also supports logic debugging with visualization displays. Safety Manager I/O can be integrated with a UniSim process model or forced from open-ended connections. Support is provided for the complete control device library in Safety Builder as of R110, custom function-blocks are supported, and drawings extracted from Safety Builder and regenerated in HMIWeb I/O lists, browsing for quick links.

The Safety Manager database is automatically imported within Honeywell's UniSim simulation technology with a look and feel identical to the configuration tool. All features like function blocks, forces and other operational features are supported in the simulator.

In addtion, Experion Station software can be embedded in Unisim to see the same displays, alarms, detail displays and trends. This allows users to integrate control and safety simulation in the same environmnent. The HMI requires no modifications and all standard displays are supported in the simulation environment.

## Applying Open Concepts to Safety Services

Usually the concept of open systems is applied to hardware and software, but it applies just as well to services, both project implementation services and aftermarket support services.

Some suppliers require that only their project engineers can install, configure and commission the safety system. That is, the hours required to implement the system are proprietary. The automation world has shunned proprietary offerings at every turn citing cost and quality as the downside of being locked into just one offering. A robust safety system that is thoroughly documented and free from an intimidating safety manual can be implemented by any qualified engineer.

With Honeywell's Safety Manager, end-users can hire Honeywell, hire a third-party or select their own in-house resources to implement the system. They can assemble an optimized project team that not only gets the original project completed correctly, but also provides the learnings that make on-going system maintenance efficient and affordable.

Just as Honeywell supports open project services, we go well beyond traditional project services with a unique set of technology services designed to help industrial professionals monitor the health and reliability of safety instrumented systems (SIS). By precisely monitoring system status, Honeywell's SIS-Health Monitoring reduces unnecessary maintenance and engineering and minimizes failures that might lead to safety incidents and unexpected plant downtime. These services can be universally applied to any type or brand of safety instrumentation.

Studies show that companies can save up to $100,000 to $1 million per year if their SIS and associated safety instrumented functions (SIFs) are properly engineered and maintained. SIS-Health Monitoring was co-developed with industry professionals in the maintenance, instrumentation and test engineering fields to address these specific issues. SIS-Health Monitoring also enables better work practices that can lead to 20-30 percent savings on installation and operating costs.

SIS typically include sensors, controllers and actuators that help bring processes to a safe state when dangerous conditions develop. Reports suggest that more than 20 percent of plant incidents are caused by SIS maintenance and testing errors. Often, SIS maintenance and testing are performed too frequently because system status cannot be accurately monitored. This unnecessarily opens the door to human errors that can cause the system to fail. Additionally, the lack of reliability data has lead to unnecessary SIS engineering, which can also lead to system failure.

Honeywell's SIS-Health Monitoring can be customized for specific plant requirements, conditions and process demands. The current release includes two modules:

- The SIS-Health Monitoring Local Reliability Database can be applied to any SIS and stores all inventory information regarding a site's safety instrumentation. Based on the failure behavior of the site's instrumentation, SIS-Health Monitoring can help determine reliability and safety performance characteristics such as trends, demand rates and time-dependent failure rates.
- The SIS-Health Monitoring Analysis Toolset enables operators to analyze, validate and optimize the SIF reliability and its Safety Integrity Level (SIL), which is a statistical representation of reliability.

These modules can operate as standalone units or together as an integrated system. They can be universally applied to any type or brand of safety instrumentation.

Safety instrumented systems are vital assets because they protect lives, processes and equipment. However, the systems themselves also need protection through performance monitoring. Many existing tools, however, are not capable of automatically monitoring the actual performance of an SIS. Honeywell's SIS-Health Monitoring solution addresses that weakness by collecting necessary, meaningful data and giving engineers the tools they need to act on it.

**For More Information**

For more information about Honeywell's integrated approach to safety, visit our website at 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

WP-08-20-ENG
June 2008


Honeywell