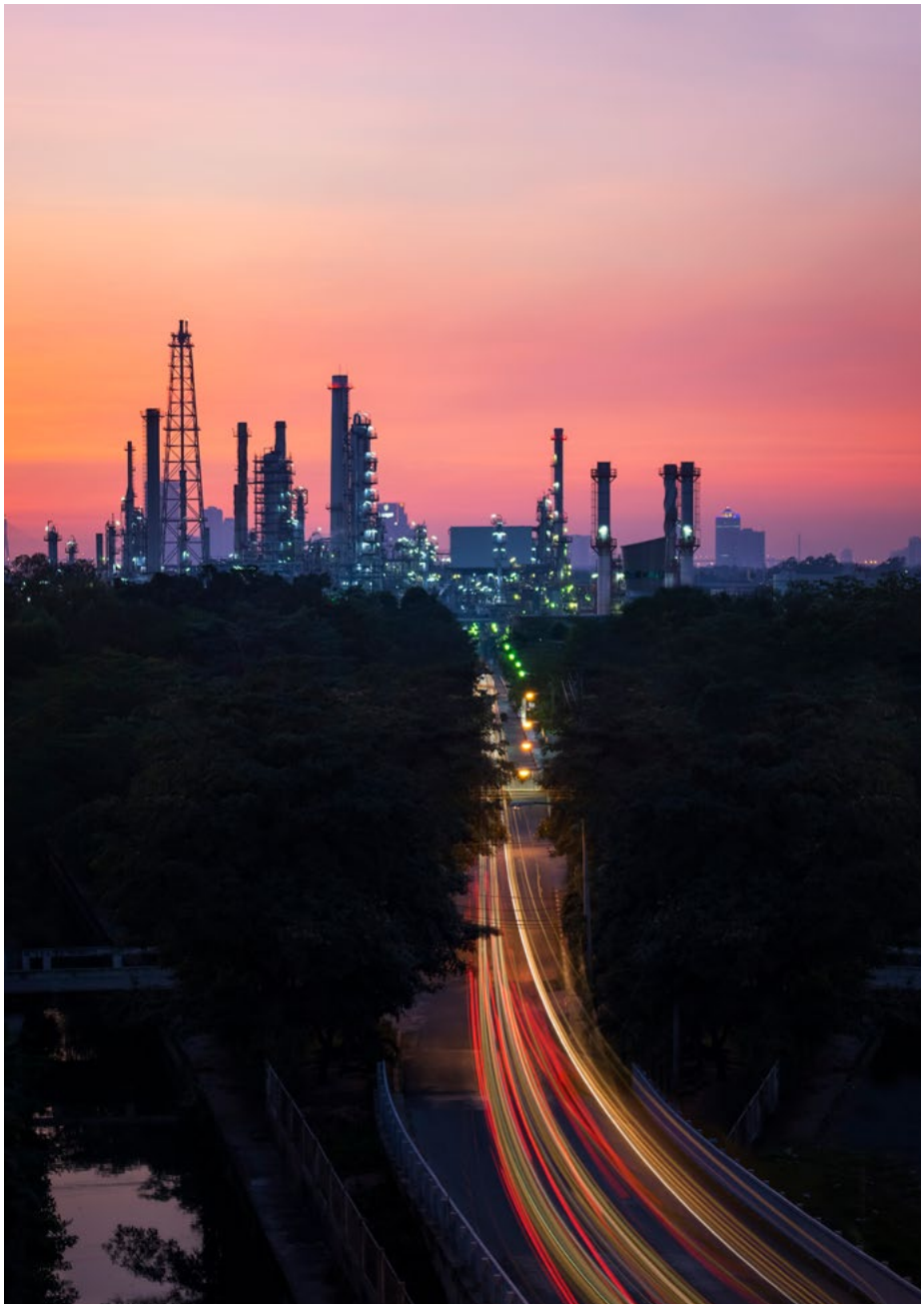
BENEFITS OF A COMBINED CONTROL AND SAFETY PAC

Honeywell

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This white paper discusses the different Safety Integrity Levels (SILs) that are commonly applied to critical processes;the SIL2 certified ControlEdge HC900 Programmable Automation Controller; the benefits of having a process control system that provides a solution for both process control and SIL2 safety-related applications; and the specific advantages that it provides over conventional safety PLCs. These benefits include faster start-up time, reduced training, simplified maintenance, and a low cost of ownership.



CURRENT CHALLENGES IN THE PROCESS INDUSTRY

Whatever the application, the process industry faces a number of major challenges. These include the need to keep processes up and running with maximum uptime. At the same time, the performance and profitability of processes need to be maximized. And ultimately, processes need to produce products that are of a higher quality than those of their competitors. Plant reliability, employee safety and environmental compliance are also crucial to a smoothly operating process. Accidents must be reduced to as few as possible, with zero being the goal. Emissions need to be controlled. And should an emergency scenario occur, the plant or specific process needs to be shut down in a timely and safe manner.

UNDERSTANDING RISK

Risk is inherent in all industrial processes, and it's simply impossible to eliminate risk completely and bring about a state of absolute safety. Safety standards exist to reduce risk, and the role of a modern safety system is to reduce risk to an acceptable or tolerable level. Risk can be minimized initially by inherently safe process design, by the Basic Process Control System (BPCS), and finally by a safety shutdown system.

SAFETY AS A PROTECTION LAYER

Providing a protective layer around industrial process systems is the role of a Safety Instrumented System (SIS), examples of which include a safety interlock, a safety shutdown system, or an emergency shutdown system. The objective of a SIS is to prevent any unforeseen incidents happening that the BPCS cannot handle, and take a process to a safe state when safe operating conditions have been transgressed.

A SIS is comprised of Safety Instrumented Functions. A Safety Instrumented Function (SIF) is a safety function with a specified Safety Integrity Level (SIL) that is implemented by a SIS to achieve or maintain a safe state. A SIF's sensors, logic solver, and final elements act in concert to detect a hazard and bring the process to a safe state.

Layer of protection analysis (LOPA) is a risk management technique commonly used in critical process industry such as refineries, chemicals etc. that can provide a more detailed assessment of the risks and layers of protection associated with hazard scenarios. By using the LOPA method, the user is able to ascertain the level of risk that is associated with hazardous events in the workplace.

DESCRIPTION

1. **Process Design**
   Good process design provides a system that is robust and can prevent or tolerate deviations in operating conditions.

2. **Basic Process Control System**
   BPCS is the control system used during normal operation and sometimes denoted as the process control system (PCS). Input signals from the process and / or from the operator are generated into output which make the process operate in a desired manner. If the system discovers that the process is out of control (e.g. high pressure) it may initiate actions to stabilize the process.

3. **Alarms and Operator Intervention**
   Alarms monitoring certain parameters (e.g. pressure and temperature) are considered another protection layer. When the alarm is tripped, the operator may intervene to stop the hazardous event.

4. **Safety Instrumented System**
   SIS implements the wanted safety function SIF (Safety Instrumented Function) to bring the process to a safe state. In LOPA, SIFs are considered as critical protection layers.

5. **Physical Protection (Relief Devices)**
   Physical protection include equipment like pressure relief devices. E.g. in a separator this may be a rupture disc which blows-off if the pressure is too high protecting the underlying equipment.

6. **Physical Containment (Bunds)**
   Post release protection is physical containment such as dikes, blast walls etc. These have their function after the release or explosion has occurred to prevent spread of damage.

7. **Emergency Response Layer**
   Plant and community emergency response, are considered the final protection layer. If an accident occurs, procedures, evacuation plans, equipment and medical treatment help the exposed personnel to escape, or to mitigate damage / injury.

WHICH SAFETY INTEGRITY LEVEL (SIL)?

Safety Integrity Levels are defined in accordance with IEC 61511, and indicate the tolerable failure rate of a particular safety function. The Safety Integrity Level corresponds to a range of values from 1 to 4 measured in terms of the average probability of failure to perform a safety function on demand and in terms of the safe failure fraction. The higher the SIL, the greater the impact of a failure, and the lower the failure rate that is acceptable.

SIL4 is the highest level of risk reduction that can be obtained through a Safety Instrumented System. However, in the process industry this is not a realistic level and currently there are few, if any, products/systems that support this Safety Integrity Level. SIL4 systems are typically so complex and costly that they are not economically beneficial to implement. Additionally, if a process includes so much risk that a SIL4 system is required to bring it to a safe state, then fundamentally there is a problem in the process design which needs to be addressed by a process change or other non-instrumented method.

When determining whether a SIL1, SIL2, or SIL3 system is needed, the first step is to conduct a Process Hazard Analysis to determine the functional safety need and identify the tolerable risk level. After all the risk reduction and mitigation impacts from the Basic Process Control System (BPCS) and other layers of protection are taken into account, a user must compare the residual risk against their risk tolerance. If there is still an unacceptably high level of risk, a risk reduction factor (RRF) is determined, and a SIS/SIL requirement is calculated. The RRF is the inverse of the Probability of Failure on Demand for the SIF/SIS (see table below)

SAFETY INTEGRITY LEVEL (SIL)	RISK REDUCTION FACTOR (RRF)
SIL4	100,000 to 10,000
SIL3	10,000 to 1,000
SIL2	1,000 to 100
SIL1	100 to 10

Selecting the appropriate SIL level must be done carefully. Costs increase considerably to achieve higher SIL levels. Typically in the process industry, companies accept SIS designs up to SIL2/SIL3. If a Process Hazard Analysis indicates a requirement for a SIL4 SIS, owners will usually require the engineering company to re-design the process to lower the intrinsic process risk. The Honeywell HC900 process control system has recently been certified as a SIL2 device.

KNOW YOUR SIF, SIL AND SIS

- **SIF: Safety Integrated Function:** A safety function with a specified Safety Integrity Level which is necessary to achieve functional safety. Can also be defined as a single set of actions that protects against a single specific hazard. So can refer to the equipment that carries out the actions in response to the hazard, or to the particular set of actions itself.
- **SIL: Safety Integrity Level:** The amount of defined risk reduction to be provided by the Safety Integrated Function; also can be seen as the level of dependability of the Safety Integrated Function.
- **SIS: Safety Instrumented System:** A system made up of one or more Safety Integrated Functions.

INTRODUCING THE CONTROLEDGE HC900 PROCESS AND SAFETY SYSTEM

The ControlEdge HC900 Process and Safety System is an advanced process and logic controller with a modular, scalable design that is built to work with a wide range of process equipment in a cost-effective way.

The system comes with a touch-screen operator interface which makes it very easy to operate. HC900 possesses a flexible architecture that can accommodate the most demanding application. With its advanced features and versatile connectivity, it is capable of customized pinpoint control. HC900 also simplifies the documentation process and eliminates filing errors.

HC900 is available in two versions, depending on whether it is SIL2 compliant or not.

THE CONTROLEDGE HC900 SIL2 CONTROL SYSTEM

- Is targeted at SIL2 safety applications and critical control applications
- Delivers high availability, safety and reliability for process control and SIL2 safety applications
- Provides easy engineering and development capabilities with a common set of hardware/software tools for process and safety applications
- Provides the lowest total cost of ownership
- Is proven to be reliable and trustworthy in the field for a number of years
- Is highly flexible and scalable with a modular design

HC900 offers the capability and flexibility of hosting both safety and process control applications on a single hardware platform or separate platforms depending on the need of the application or the end-user. A common hardware platform allows separation

between the process control and safety environments within the designer software, which is totally non-interfering and easy to configure using function block methodology.

If separate hardware platforms are chosen, then communication between the process control system and safety system becomes very easy and flexible because of easier data exchange and similar communication protocols. Safety critical data is exchanged between safety systems using a SIL2 certified peer protocol.

Similar hardware for process control and safety allows for easy training of engineering and safety personnel. This leads to development and training cost savings because the same function block software is used for safety and process. Training costs are reduced because training on using the tools needs to be conducted only once, although proper design procedures must be followed to ensure there is no common cause of failure between BPCS and SIS when shared components are used between the safety and process control system.

The operators can have the same HMI or operator interface with enhanced diagnostics to view the process and safety control operations. The use of a similar kind of system for process control and safety reduces the system complexity and number of systems from different manufacturers used.

Features of HC900 include a SIL certified operating system with TÜV SIL2 certified function blocks with input voting and output validation features. It also includes a SIL2 certified Universal IO module with all Safety features built-in. Advanced features include the use of external watchdog time, independent clock, additional RAM and flash memory, and ECC memory circuitry for safety and process controllers.









WHERE IS THE SIL2 CERTIFIED HC900 USED?

Process industries currently using the SIL2 certified HC900 system include:

- Chemicals, including specialty and fine chemicals, plastics & rubber
- Pharmaceuticals & Cosmetics
- Power (excluding nuclear)
- Cement & Glass
- Pulp & Paper
- Mining & Metals
- Water & Waste Water
- Food & Beverage
- Heat Treatment

APPLICATIONS IN WHICH THE SYSTEM IS PROVING INVALUABLE INCLUDE THE FOLLOWING:

Safety:

- Burner Management Systems (e.g., furnaces, boilers, pre-heaters, kilns, ovens, reactors, calciners, dryers, thermal oxidizers, melters, incinerators, process heaters, vaporizers).
- Combustion control
- Pipeline monitoring
- Spill prevention
- Transportation - tunnel ventilation
- Terminal automation
- Emergency shutdown
- Fire & gas monitoring and protection

UNIQUE BENEFITS OF THE SIL2 CERTIFIED CONTROLEDGE HC900 SYSTEM

PROVEN TRACK RECORD

ControlEdge HC900 SIL2 is proven in the field with over 15000 installations globally across process control and critical applications. The system complies with most major standards and regulations such as CSA Class1, Div 2, ATEX, ABS, UL, CE Conformity.

The system is also certified by TÜV for use in a SIL2 environment. External certification from a recognized agency like TÜV further validates the capability of the system to perform its safety tasks.

The system is ideal for a process/safety software environment. Its non-interfering software environment means that the HC900 system is capable of hosting process control and safety applications, providing control, monitoring, password protection for configuration, alarm processing and data acquisition for process applications.

High reliability and availability is ensured by redundant CPU, rack power supply, communications and networking, as well as by features such as removal and insertion under power, online monitoring, edits and hardware maintenance during running operation. Its hardware, communications and sensor level diagnostics are robust, and the system provides early warning notification of pending sensor failure.

EASY TO USE AND ENGINEER

Process-specific function blocks, including I/O validation safety function blocks suited to individual application needs, reduce configuration time.

The system is quick to start up thanks to its HC Designer intuitive software. Powerful Accutune III auto-tuning algorithms enable control loops to be quickly and easily tuned to reduce start-up time and lessen the impact of process upsets.

Advanced monitoring and debugging tools are easy to use and engineer, and the system provides an integrated operator interface and open Ethernet communications as well as central and remote I/O capability.

The system is fully scalable, allowing a customer to purchase only what the process currently needs, while enabling future expansion as the process expands. The ControlEdge HC900 system supports up to 12 racks, and 4608 IO's.

ACCURATE AND OPTIMAL PERFORMANCE

ControlEdge HC900 enables accurate process control which translates into benefits such as increased throughput, reduced scrap, reduced energy utilization, and minimized energy costs.

The SIL2 certified CPU displays a digital throughput of only 10 ms. Its External Watchdog Timer with an independent clock provides a safeguard for detecting and correcting spurious CPU lock-ups. Internal faults are monitored and add to the robustness and performance of the system. The external watchdog timer is advantageous over internal watchdog timers as internal watchdog can be damaged if CPU is damaged.

The system provides RAM and Flash memory enhancements, while its ECC memory circuitry corrects single faults and detects double faults, thus adjusting memory corruption conditions. This ensures robustness, performance and reliability of data transmission.

The system also offers a SIL2 certified Universal IO, which can be soft configured as AI, AO, DI or DO. The Universal IO has safety features such as line monitoring, short circuit protection, per channel safety shutdown, current limiting and user specified failsafe value to allow predictable operation in the event of a communication loss between controller and IO module.

TOTAL SOLUTION WITH LOW COST OF OWNERSHIP

ControlEdge HC900 provides similar hardware/software for process control and safety-related applications. An option is to have a separate or a common logic solver for process control and safety applications. The system integrates easily and smoothly with the HMI (HC900 Control Station), Experion HS (SCADA solution), and Matrikon OPC (third-party solutions).

A low total cost of ownership is ensured by:

- Universal IO module to minimize hardware buy and inventory, while reducing the configuration time and effort
- One time license purchase with no annual fee
- Software web-based downloads for upgrades
- Reduced training costs with common tools for process and safety applications
- One Vendor for Safety/Process solutions – integration with a portfolio of Honeywell products

SPECIFIC ADVANTAGES OVER SAFETY PLCS

The HC900 offers additional advantages over safety PLCs:

- Provides redundancy and I/O checking
- Redundancy of CPU, power supply IO module and communication is easily achieved
- First SIL2 certified Universal IO in the market for Safety PLC with safety features built-in, HART-IP, redundancy, and Sequence of Event (SOE) support
- Flexibility in programming allows the program to be developed by experts thus helping exceed the NFPA codes
- Program security and protection through password protection
- Affordable SIL2 solution can be achieved right out-of-the-box, thus helping achieve compliance to industry standards
- System flexibility allows it to be used with any fired equipment such as ovens, furnaces, boilers etc.
- Communicates easily with other third-party PLCs
- Integrated HMI and a global database easily reduce operator errors
- Multiple burners, multiple scanners can be used for burner related applications (as compared to microprocessor based BMS systems)
- Critical information and advanced diagnostics for improved operations

CONCLUSION

The SIL2 certified ControlEdge HC900 is a single flexible system for process control and safety with faster start-up time, common engineering tools, reduced training, simplified maintenance, and lowest cost of ownership. Its engineering tools and hardware can easily integrate with Honeywell system and other third-party applications. This leads to increased throughput, less rework, secure accurate process records, improved safety and reliability, reduced human error, and loss prevention through a TUV certified SIL2 system.

For more information

To learn more about combined control and safety PAC, visit our website www.honeywellprocess.com or contact your Honeywell account manager.

Honeywell Process Solutions

2101 CityWest Blvd, Houston, TX 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road
Zhangjiang Hi-Tech Industrial Park
Pudong New Area, Shanghai 201203

WP-13-04-ENG | Rev 1 | 07/21

THE FUTURE IS WHAT WE MAKE IT

Honeywell