Executive Summary

Industrial organizations must be good citizens when it comes to the safety and reliability of their operations. They are challenged with ensuring regulatory compliance and maintaining reliable and continuous plant processes—while still keeping operating costs down.

Plants require optimal safety instrumented system (SIS) performance in order to protect personnel, the environment and production assets, and at the same time, maximize uptime and minimize operational disruptions.

Recent accidents at industrial facilities have focused attention on the international IEC 61511/ISA-84.01 standard, which addresses the threat of hazardous plant operating conditions. However, not all process manufacturers fully understand the implications of today’s functional safety regulations—or have taken action to ensure compliance at their facilities. This is particularly true of large companies with dispersed global operations, as well as smaller firms with limited engineering resources.

Additionally, ongoing updates to the ISA/IEC standard, coupled with government requirements for recurring safety system certifications and hazardous operations studies, complicate a regulatory compliance strategy.

Honeywell’s Safety System Services can help process industry sites maximize uptime and productivity while avoiding compliance issues, meeting safety standards and solving problems faster. Our approach is based on a comprehensive Safety Lifecycle Management program, which develops the complete set of activities needed to determine safety requirements and implement effective solutions.
# Table of Contents

**Introduction** .................................................................................................................. 3

**Background** .................................................................................................................... 3

  - Growth of Regulatory Standard ......................................................................................... 3
  - Need for Compliance ........................................................................................................... 4

**Plant Safety Requirements** ................................................................................................. 4

  - Industry Guidelines ........................................................................................................... 5
  - Cost of Conformance ........................................................................................................ 5

**Effective Compliance Strategy** ............................................................................................. 6

  - Layers of Protection .......................................................................................................... 6
  - Segregated Systems ............................................................................................................ 6
  - Operational Integration ....................................................................................................... 6

**Safety System Lifecycle** ....................................................................................................... 7

  - Analysis .............................................................................................................................. 8
  - Implementation ................................................................................................................... 9
  - Operation ........................................................................................................................... 10

**Benefits of Safety Services** .................................................................................................. 11

  - Role of the Service Provider ............................................................................................ 11
  - Specific Service Offering .................................................................................................. 12
  - Lifecycle Management Program ....................................................................................... 13

**Conclusion** ......................................................................................................................... 13

**References** .......................................................................................................................... 13
Introduction

Risks prevail wherever people store, process or handle hazardous or toxic materials. In the process industries, these risks are compounded because of their potential to impact numerous people. A spill of a toxic agent or explosion could be hazardous to a population within a plant or the surrounding area.

In recent years, there has been an increased focus on industrial safety across the globe. The need for improved understanding and harmonization of risk reduction approaches became evident with the occurrence of such major catastrophes as Seveso (Italy), Bhopal (India), Flixborough (U.K.), Piper Alpha (U.K.) and Chernobyl (Ukraine).

Compliance with legislation to safeguard personnel, communities and the environment is a priority for both legal and ethical reasons, as well as reducing lifecycle costs. An effective safety solution is needed to enable proactive protection versus responsive mitigation, help stop events before they happen, prevent injuries, and save lives (See Fig. 1).

Industrial plants employ many types of control systems that continuously manage process parameters such as temperature, flow and pressure. Such processes can create hazardous situations when they are out of control, and the Basic Process Control System (BPCS) may not be able to maintain safe operation in the event of a failure. This is where the safety instrumented system (SIS) comes into play. The purpose of the SIS is to perform safety instrumented functions (SIFs), and if necessary, shut down the process in an orderly manner. In other words, the SIS trips the process when it detects an out-of-limit condition. Common types of safety systems include emergency shutdown, fire and gas monitoring, critical process control, burner management, and turbo machinery control.

Based on a cost-benefit analysis, it makes sense to invest in and maintain an effective SIS compared to the implications of a potential hazardous event. Plant safety systems require careful planning, design, implementation and maintenance to ensure the expected level of safety is realized and maintained, and spurious trips are minimized. To stay competitive and to retain regulatory compliance, plant operators seek solutions to ensure they operate as required and at peak efficiency.

Background

There is a compelling business case for operations across the process industries to invest in solutions helping to maintain standards of health, safety and environmental (HSE) protection. Indeed, industrial organizations have a responsibility to their key stakeholders and the public to comply with all industry and government regulations, and maintain reliable and continuous processes — while still keeping operating costs down.

Growth of Regulatory Standards

In response to rising safety concerns, the U.S. Occupational Safety and Health Administration (OSHA) developed and published OSHA 29 CFR, 1910.119-1992, Process Safety Management of Highly Hazardous Chemicals, Explosives, and Blasting Agents; and the Environmental Protection Agency (EPA) enacted EPA 40 CFR Part 68, Accidental Release Prevention Requirements: Risk Management Programs under the Clean Air Act. These regulations helped define areas that must be addressed in order to achieve a mandated level of functional safety performance in industry.

The International Society of Automation (ISA) also recognized the need for improved process sector functional safety. Its Standards Project 84 committee accepted the IEC standard as a U.S. national standard replacing ANSI/ISA-84.01–1996. The only modification to IEC 61511 for adoption in the U.S. (i.e., ANSI/ISA-84.00.01-2004) concerned the handling of legacy systems (i.e., the “grandfather clause”). The European standards body, CENELEC, subsequently implemented the IEC/ISA standard as EN 61511. This means in each of the member states of the European Union, the standard is published as a national standard (See Fig. 2).

More recently, in 2007, a number of major control system end users and manufacturers, along with ISA, formed the ISA Security Compliance Institute (ISCI) to establish standards, tests, and conformance processes supporting the integration of control system products. The organization’s work recognizes that SIS and distributed control systems (DCSs) are interconnected with common Human-Machine Interfaces (HMIs) and servers, and the SIS should be designed to protect itself from cyber threats coming from any of these interfaces.

Need for Compliance
The underlying need for the IEC/ISA standard arises from processes involving major hazards, with significant potential to cause losses and harm. The risk of these undesirable outcomes is a function of both their severity—for example, how many people injured or killed, and how much damage and lost production—and their frequency, that is, how often such an event can be expected to occur.

The following aspects must be considered by plant management seeking to comply with international safety standards:

• What are the potential hazardous events and their associated risks, and what risk reduction is required to achieve tolerable safe process installation?
• How can it be established and confirmed that the chosen safeguarding measures/equipment realize the required risk reduction?
• What activities must be carried out to guarantee adequate safety is maintained during the entire lifetime of the safeguarded process installation?
• How can it be proven, by proper documentation, that safety requirements are met?

Despite the growing awareness of plant safety issues, not all process manufacturers fully understand the implications of today’s functional safety requirements—or have taken action to ensure compliance at their facilities. This is particularly true of large companies with dispersed global operations, as well as smaller firms with limited engineering resources. Additionally, ongoing updates to the IEC/ISA standard, coupled with government requirements for recurring safety system certifications and hazardous operations studies, underscore the need for an effective compliance strategy.

Plant Safety Requirements
Recognized safety standards such as IEC 61508, IEC 61511 and ANSI/ISA-84.00.01 now represent generally accepted best engineering practices for industrial organizations worldwide. In the U.S, for example, OSHA has endorsed IEC 61511/ISA-84 as a "national consensus standard" for the application of SIS in plant operations. It states that employers may be in violation of the General Duty Clause of the Occupational Safety and Health (OSH) Act of 1970 if plant safety systems do not conform to IEC 61511/ISA-84, and hazards exist related to the SIS, which could cause serious harm to employees.
Industry Guidelines
The IEC 61511/ISA-84 international standard addresses:

- Management of functional safety
- Safety lifecycle requirements
- Process hazard and risk assessment
- Allocation of safety functions and determining the SIL value of these functions
- SIL verification
- SIS safety requirements specification
- SIS design and engineering
- Requirements for application software
- Factory acceptance testing (FAT)
- SIS installation and commissioning
- SIS safety validation
- SIS operation and maintenance
- SIS modification
- SIS decommissioning
- Information and documentation

For end-users, SIS designers and system integrators, IEC 61511 defines the safety standard they should follow when implementing certified safety equipment. It applies when equipment meets the requirements of IEC 61508, or if Section 11.5 of IEC 615111 (prior-use or proven-in-use) is integrated into an overall system used for process sector applications. The standard clearly states that manufacturers of equipment used on SIS must follow the requirements of IEC 61508 Section 2 and 3 unless the end user is in compliance with Section 11.5 “Prior-Use.” As such, equipment certified for safety loops with an adequate Safety Integrity Level (SIL) is recommended. A reasonable level of SIS must be used based on the studies (See Fig. 3).

Cost of Conformance
For new projects, conformance to the IEC 61511 safety standard typically has minimal impact on total project costs. It requires project and operations leaders to follow a structured safety lifecycle approach through the design, installation, and operation of the SIS.

For existing SIS installations, engineering and hardware costs are impacted by the regulatory guidelines. Engineering cost will vary based on the quality of the existing process hazards analysis (PHA). If the PHA has established a tolerable risk for the events under review and determined the target risk reduction for the SIF, then little additional engineering is required beyond normal instrument and control design. The probability of failure on demand (PFD) of the SIF at the current test frequency can be calculated and compared to the required SIL. If the existing PHA has not adequately defined the need for risk reduction (e.g., SIF design, SIL requirements), considerable engineering effort may be required to conform to the standard. The PHA must be updated to define these requirements for each identified SIF. The target SIL for the SIF will then be determined to obtain the risk reduction required to reach tolerable risk for the event. The PFD of the SIF can then be calculated to determine if the tolerable risk for the event is achieved. If the SIF cannot meet the target SIL, the test interval may have to be decreased or redundant equipment added. The plant may also have to look at other processes, which are inherently safer.
Effective Compliance Strategy

Efforts to ensure plant safety and regulatory compliance must go far beyond simply installing fail-safe controllers or advanced SIS technology. In fact, to mitigate the risk of serious incidents, it is important to consider safety from all aspects of an operation. Furthermore, plant owners need access to the right resources, with the right skills, at the right time to restore productivity in the event of safety system failure.

Industrial facilities should take a holistic approach to safety and security, addressing critical requirements from the process control network to the perimeter of the plant. This approach is intended to increase situational awareness of production processes and improve response to emergency situations arising from safety-related incidents. When properly implemented, it will help protect people, assets and the environment while sustaining a high level of operational and business performance.

Layers of Protection

At the core of best practices for integrated safety and security is “defense in depth” with independent layers of protection. This strategy is included in the IEC 61511 standard, which stipulates that every layer of protection, including both control and safety systems, should be unambiguously independent. Some of the reasons for this basic requirement are to avoid common cause faults, minimize systematic errors, and provide security against unintentional access.

With a layered safety solution, some layers of protection are preventative in nature (e.g., emergency shutdown), and some are there to mitigate the impact of an incident once it occurs (e.g., fire & gas protective systems or emergency response systems). Other layers of protection can deter incidents in the first place, or provide detection, alerting and associated guidance. The core is an “inherently safe design,” and as such, the load on all other layers is lessened to meet the “tolerable risk” criteria. (See Fig. 4).

A layered safety strategy unifies all plant protection layers (i.e., basic control, prevention and mitigation as outlined in IEC 61511) required for achieving a high level of functional safety. Plus, it provides the required functional safety with a high SIL. This includes superior visualization and logging facilities enabling optimal operator response and accurate evaluations. By integrating basic control, prevention and mitigation components, overall project costs and ongoing maintenance expenses can be vastly reduced.

Segregated Systems

As prescribed by IEC 61511, safety systems should be dedicated to safety-critical assets only. Most DCSs are not sufficiently robust and fail-safe to operate safety-critical instruments at all times. The IEC standard also urges caution if non-safety and safety functions are implemented in the same safety-related system, since this may lead to greater complexity and increase the difficulty of carrying out lifecycle activities such as design, validation, functional safety assessment and maintenance.

Apart from segregation of control and safety equipment, there should be a separation of responsibilities between the personnel who manage these assets. The safety engineer is focused on safe operation, whereas the process engineer wants to maximize plant availability and profits.

Operational Integration

Today, improved solutions for operational integration allow plant personnel to have a seamless interface to the process under control, and at the same time, maintain safe separation. From an operational perspective, it makes no difference where the application is running. All required information is available to the operator. Applications ranging from rotating equipment and compressor protective systems, to emergency shutdown systems and large plant-wide fire and gas applications can be monitored from any operator console.
This truly integrated system architecture unifies:

- Operational interfaces
- Peer control
- Diagnostics
- Postmortem analysis
- Fire and gas systems
- Power supplies
- System modifications
- Simulation and optimization

An integrated approach provides multiple operational and business benefits to process plants. For instance, it helps operators to minimize intervention and shutdowns and recover more easily from process upsets. It also allows facilities to reduce hardware and installation cost, and ensure easier system configuration with preconfigured function block selections.

**Safety System Lifecycle**

Some plant owners may still be wondering, "Are international safety standards relevant to my operation?" Since there is a growing awareness in process industries of the IEC/ISA standards, and because of the association with some regulatory authorities, the answer is "yes."

However, the operation in question may already have the appropriate safeguards or layers of protection in place, alleviating the need to implement a SIS solution. This can only be determined through the implementation of the "safety lifecycle," which is a sequential approach to developing a SIS (references to a safety lifecycle can be found in ANSI/ISA-84.00.01 Parts 1-3 and IEC 61511 Parts 1-3).

**Figure 5.** IEC 61511 divides the safety lifecycle into a series of key phases.

In general, the implementation of the safety lifecycle can follow the IEC/ISA standard in a suggested manner or can be customized to suit the company or corporation’s management style. It is not necessary to develop an extra tier of paperwork to manage this process; integrating the lifecycle requirements into existing procedures for planning, design, construction and maintenance is perfectly acceptable.

In either case, the safety lifecycle is the foundation to build on—with no beginning or end. This gives the flexibility of implementing some or all of the phases based on current requirements.

In the first safety lifecycle phase, the objective is to analyze the risks involved in running the plant. This involves deciding how much safety risk the operation can tolerate; optionally, the user can also consider other types of harm such as environmental damage, downtime, equipment damage and loss of reputation. In the next period, the SIS is designed to meet the specification. Hardware is selected; calculations are performed to ensure the hardware can achieve the specification; software and maintenance procedures are written; and extensive tests and checks are conducted, both before and after the safety equipment is installed and commissioned. And in the final lifecycle phase, the plant is operated with the SIS in place. Documentation is prepared on the performance of the system and the demands made on it by the plant. Maintenance of the SIS is carried out as planned, with every change to its design carefully controlled through a management of change procedure.
The safety lifecycle phases can be categorized as follows:

**Analysis**

**Process Design**
Process design is an essential task, which must be completed before conclusions can be drawn on whether or not a project will require a safety system. The contributions of process design to a project are most intense in the earliest part of the project lifecycle. This includes conceptual review, process flow diagrams with heat and material balances, and piping and instrument diagrams (P&IDs).

**Site Assessment**
A site assessment is conducted to determine the risk associated with operation of process units, and to evaluate the design, operation and maintenance of either an existing or potential SIS. Based on the results, plants have a detailed roadmap for installing new equipment or updating obsolete infrastructure to an optimal level of safety. They can also pinpoint necessary maintenance and updates, avoid costly downtime, improve plant performance and extend the operating life of the SIS.

**Safety System Audit**
Safety system audits determine if a site has harnessed its respective technology appropriately in providing a truly effective operating environment, and whether the SIS is operating in a safe and reliable manner. This is accomplished by answering the following questions:

- Is the SIS designed in a correct way? For instance, does the system match the current as-build documentation?
- Is the environment affecting the SIS? Possible factors include corrosion, loose cables, climate conditions, etc.
- Did modifications impact the safety and reliability of the SIS? It is important to study the status of the system configuration, applications and hardware.
- Are diagnostics showing a hidden issue? The system's on-line characteristics should be carefully analyzed.

Finally, the audit indicates whether preventive maintenance is scheduled and implemented in a suitable way.

**Competency Assessment**
Competency assessment ascertains the level of competency of individuals involved in the safety lifecycle. All persons performing any safety tasks, including management activities, must have appropriate training, technical knowledge, experience and qualifications relevant to their duties.

**Hazard Identification**
Process safety starts with the initial concept of the project, where hazards are identified even as the process is synthesized. This process typically begins during preliminary PHA, which uses simpler "What If?" and "Checklist" analysis techniques. A team that includes expertise in the technology and operation of the process, as well as the PHA methodology should conduct the analysis.

**Risk Assessment**
Risk assessment processes defined by the IEC/ISA standard typically take a lifecycle approach in stipulating how to implement an effective process to identify hazards. This is where the Hazard and Operability (HAZOP) analysis often plays an important role in the process design. Every process plant per OSHA regulations must perform a HAZOP study every five years. Rigorous adherence to this requirement can have a significant impact on an operation’s insurance premium.

Central to the HAZOP is assessing the risk associated with the hazard. Unlike machinery assessments, risk assessments in process applications employ a more comprehensive focus due to the potential for accidents to impact a much wider area, such as an entire facility or community.

The HAZOP analysis also investigates and considers how the plant might deviate from the design intent. This helps to ensure that proper safeguards against accidents are in place. A risk analysis is integral to quantifying the level of risk in terms of severity of consequence, frequency of exposure, and probability of avoidance. It quantifies the risk into one of four possible SILs, which represent the amount of safety that must be available to mitigate the risk.

Once the different hazards have been identified, the next step is to determine a way to reduce the risk within those hazards to a tolerable level. IEC 61511 specifies a number of techniques to accomplish this task. One example is a layers of protection analysis.
(LOPA), which starts with data developed in the HAZOP and accounts for each identified hazard by documenting the initiating cause and the protection layers that prevent or mitigate the threat.

**SIL Determination**
A SIL assessment is performed to establish a "fit for purpose" design for instrumented safety measures, which are able to mitigate hazards with respect to safety, environmental consequences and economic loss. The design is also fit for purpose in that the robustness (i.e., redundancy of sensing and/or final elements) of the safety measure is validated against operational losses caused by spurious trips. A multi-disciplinary team typically performs the SIL assessment.

**SIF Definition**
Definition of safety functions, whether instrumented or non-instrumented, moves them beyond allocation to conceptual design. For a SIS, the process involves the preparation of a SIF list containing causes and effects as well as the required SIL of each SIF. This is determined by a comparison of assessed risk with tolerable risk.

**SIL Verification**
SIL verification is a critical step in the conceptual design process for SIFs. After the preparation of a safety requirement specification (SRS) based on the SIL assessment, the SIF subsystem technology is chosen and its redundancy is decided. Test methods for all equipment are also determined. Finally, the SIF design is verified to determine whether or not it meets functional and integrity requirements.

**SIL Validation**
SIL validation is used to verify, through inspection and testing, that the installed and commissioned SIS and its associated SIFs meet the requirements as stated in the SRS. Common steps include: verifying the SIS performs under normal and abnormal operating modes; confirming adverse interaction between the BPCS and other connected systems does not affect the SIS; confirming sensors, logic solvers and final elements perform as defined in the SRS; and verifying proof test intervals are documented in maintenance procedures.

**Implementation**

**Detailed Design**
During mechanical/electrical/structural detailed design, the engineering design team takes the process and SIS designs and translates them into construction documents from which skids can be built and facilities constructed.

**Software Configuration**
Software configuration translates control strategies implied in the P&IDs and safety strategies described in the SRS into computer programs that actually control the process.

**Equipment Build**
Equipment build tasks can range from fabricating equipment modules, to building control cabinets and configuring other skid-mounted components.

**Factory Acceptance Testing (FAT)**
The time to catch issues with equipment modules, control cabinets and other skid-mounted components is before they ship to the construction site. FAT allows the end-user to be confident that equipment is fully functional and assembled from standard parts before it arrives for installation.

**Construction/Installation**
Construction and installation of a project can fall anywhere in the spectrum from totally "stick-built" to totally modular construction. Totally modular construction consists of receiving everything on skids, flanging them up, bolting them together, and plugging them in, whereas totally stick-built construction relies on craftsmen in the field to put everything together from basic components.
Site Acceptance Testing
On almost any project, it is important to test how the entire process functions and how all of the component pieces of equipment and instrumentation interact with one another. Each SAT is unique to each project, and is typically carried out by a team assembled from the construction contractor, equipment vendor representatives, and plant operations and maintenance.

Validation
Validation ensures the SIS and each of its SIFs perform in the intended manner as detailed in the SRS. It combines field tests, calibration, and simulations. Validation should be carried out after the process and control systems have been installed, but prior to the introduction of any process or utility hazards.

Pre-Startup Review
The pre-startup safety review is a best practice for starting any process in an industrial facility.

Operation
Training
A safe operating facility depends on operations and maintenance personnel understanding their process and its safety features prior to startup, and on ongoing training in variety of topics.

Proof Testing
Similar to validation, proof testing is the defined procedure of confirming that the SIS and its SIFs are functioning correctly and as they were designed. Each SIF must be tested in its entirety, either as a complete loop or component-by-component. When proof testing is done by component, separate components of the same control loop may be tested at different times and at different intervals. Recent advances allow proof testing to be done online so as to minimize disruptions to plant personnel and expedite the final results.

Inspection
It is also a good practice to observe whether components in the plant, particularly elements of an SIS, are in good shape. They may be still working and able to pass a proof test, but suffering from fatigue, corrosion, loose or missing parts, or other conditions that compromise the integrity of the process. Inspection alerts the plant to problems without waiting for an actual failure.

Maintenance
One important cost factor that may be overlooked in a plant safety strategy is the ongoing cost to maintain the SIS installation. Maintenance should never be neglected when cost cutting takes place. If maintenance is disregarded, the plant’s SIL-rated safety functions will diminish to less than their designed value, or worse yet, have no actual SIL rating at all. This will give plant management a false sense of security in their safety system and create a less safe process while increasing the company’s liability if a hazardous incident occurs.

Management of Change (MOC)
MOC is the process of identifying, analyzing, and tracking any adjustments to the process or equipment. OSHA standards require plants to monitor any change to the process that is not "a replacement in kind" and how it affects the hazards, production, operations, and safety of the process. Once these effects are identified, the standard also requires the plant to update any procedures, safety functions, hazard analyses, or other documents as appropriate.

Decommissioning
Decommissioning is the final element of safe process management. It is crucial that decommissioning activities not interfere with or inadvertently impact other processes remaining active. Careful consideration must be taken to ensure utilities or safety equipment for processes still in use are not damaged or removed with the decommissioned process.
Benefits of Safety Services

In parallel with all the phases of the safety lifecycle, IEC 61511 demands proper management of every activity undertaken, from first concept to final disposal of the safety equipment. There are many aspects to this process: competency requirements, planning, and documentation control, to name a few.

The only way to ensure a SIS is installed and works properly is having a comprehensive safety management system in place. This includes a continuous monitoring and verification process following the plan-do-check-act (PDCA) concept, as well as a consistent modification procedure covering all the interferences of a possible SIF modification.

Experience has shown that industrial operations of all sizes can significantly improve their safety management by employing the assistance of a qualified safety services provider. Many facilities currently have no maintenance service contract for their safety systems, or rely on a service agreement that provides a technician rather than a safety systems specialist (See Fig. 6).

Figure 6. Industrial operations can improve their safety management by employing a qualified safety services provider.

The objective of a third-party safety services solution is to help industrial firms be good citizens when it comes to the safety and reliability of their plants. The services are also intended to maximize process uptime and productivity while avoiding compliance issues, meeting regulatory requirements and solving problems faster. This includes proactive system health analysis and documentation that meets compliance requirements, as well as emergency services with a guaranteed timely response by a safety system expert.

Role of the Service Provider

Leading automation suppliers and engineering firms have some combination of capabilities that go beyond simply supplying hardware and software. To realize maximum production and optimal safety levels, they help customers implement automation and safety systems, and offer services and expertise to assess hazards and risks; define safety requirements; and deliver tools to measure, analyze and optimize these systems.

Honeywell’s safety systems services provide a complete lifecycle solution that helps ensure compliance with all applicable industry safety standards. It encompasses safety and compliance, reliability, technical risk management, access to experts, disaster recovery and cost reduction. The suite of safety system services includes hazards and risks analysis, SIL validation and verification studies, documenting safety system specifications, on-line SIS proof testing, maintenance services and part management programs.

Honeywell safety system services can help process plants:
- 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

In addition, Honeywell has established a unique safety knowledge community located in expertise centers around the world. Certified safety engineers in these centers perform a wide range of consulting, project, and lifecycle support services. They deliver sound safety solutions in all phases of the lifecycle—from the definition and conceptual design phase, throughout implementation, and during plant operation and automation.
Specific Service Offering
Honeywell’s safety system services portfolio include:

Assessment and Documentation
A pre-assessment determines the current status of process facilities, people and organization. Service technicians also conduct expert reliability calculations and deliver a report of the findings, as well as written test procedures.

IEC 61511 Safety System Lifecycle Services
• Hazard and risk analysis
• Allocation of safety functions to protection layers
• Safety requirements specification for SIS
• Design and engineering of SIS
• Installation, commissioning and validation
• Operation and maintenance
• Emergency services
• Modification
• Decommissioning

Complementary Services Related to IEC 61511
• Management and organization of functional safety
• Verification services
• Functional safety audits
• Functional safety assessments

Shutdown Optimization Services
Expert review of the event log, including results of previous test findings evaluated against initial testing recommendations (the intent is to minimize unnecessary shutdowns for testing).

TÜV Certification
Many companies would like to have an independent confirmation from an officially accredited body that compliance is achieved with IEC 61511. TÜV is recognized as the “best-in-class” organization in this area.

Training Services on Functional Safety and SIS
• TÜV functional safety program, provided by Honeywell
• TÜV functional safety engineer exam

Honeywell’s in-depth safety system health checks enable plants to minimize the risk of equipment failure and address a wide range of potential operational issues. Its service staff also responds much faster than the typical service organization to expedite problem resolution. With on-demand services, getting a safety system expert on-site can involve lengthy delays — potentially impacting in-house productivity or even production by days.

In addition, Honeywell’s optional parts assessment, holding and replacement services provide assurance that the right parts are available to get the SIS up and running as soon as possible. Professional troubleshooting and immediate access to parts speeds the time to resume operations, and saves potentially millions in production impact.
**Lifecycle Management Program**

Key to Honeywell’s safety systems services solution is its the Safety Lifecycle Management Program (SLMP), a tool that employs a series of steps to develop the complete set of activities needed to determine safety requirements and implement effective solutions. The SLMP’s robust data management model transforms input information into safety requirements. In combination with a reliability database and a number of calculation algorithms, this model is used to validate safeguarding measures. The required information is entered step by step, and then transformed and calculated (See Fig. 7).

Upon completion of the step process, the SLMP tool produces all documentation required to prove the process is safeguarded in a compliant manner.

**Conclusion**

For today’s process manufacturers, the safety of their facilities, personnel, production operations and the environment is essential to achieving on-time delivery and minimizing any potential losses. Plants must meet their critical infrastructure protection needs while ensuring operational and business readiness. Faced with this reality, they are seeking the lowest risk, and highest value protection, from their safety system technology.

The IEC 61511 approach to functional safety has proven to be effective at process industry sites around the world. Thorough attention to design integrity provides the only viable way to eliminate systematic failures, which can otherwise take out an entire safety system. Detailed management of the design process ensures costly errors are eliminated. Plus, the rigorous discipline of planned, appropriate maintenance procedures and scrupulous management of change pays for itself in reduced downtime and enhanced safety.

By utilizing expert safety services to help optimize SIS lifecycle performance, process safety and availability, plants can reduce interruptions and upsets to increase process uptime, maximize effective and efficient utilization of safety assets while improving SIS integrity and availability, and decrease testing and maintenance requirements. They can also empower operators with actionable and reliable data and safety knowledge to drive greater productivity.

References


For More Information

Learn more about how Honeywell’s safety system services help plants realize maximum production and optimal safety levels, 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

Shanghai City Centre, 100 Junyi Road
Shanghai, China 200051

www.honeywellprocess.com