White Paper

Honeywell

Honeywell Process Solutions

An Integrated Approach to Safety: Defense in Depth

Executive Summary

Ensuring safety requires reducing the risk of incidents, faults and failures that can disrupt normal operations. This effort goes far beyond simply installing fail-safe controllers or a safety instrumented system. In fact, to mitigate the risk of serious incidents that can cause injury to personnel, equipment and the environment, it is important to consider safety from all aspects of a plant's operation.

Honeywell's integrated approach to plant safety helps customers improve their business performance and peace of mind. This solution includes independent yet interrelated layers of protection to deter, prevent, detect and mitigate potential threats.

Table of Contents

Executive Overview

Why is safety important? From the perspective of the plant manager, safety is important because protecting personnel, equipment and the environment are their top priorities. Safety is maintained when the risks of serious incidents are mitigated.

A question that is constantly in the mind of the plant manager is “Are we safe enough?” And this is not an unreasonable question when one considers that safety-related incidents can cause injury to personnel, equipment and the environment, as well as interrupt production capability.

The media has been instrumental in bringing attention to the magnitude of safety-related incidents. Recently reported was an explosion that ripped through a major oil refinery, killing 15 workers and injuring more than 170 others. Pointing to mistakes made during the unit startup, the regional president called the incident “an extraordinary tragedy.” The human loss this company experienced is practically unbearable. And to add to this staggering report, this particular blast was the plant’s third accident in a year, seriously affecting product from a refinery that processes 433,000 barrels of crude oil per day, representing approximately 3 percent of the nation’s gasoline.

Other companies are more fortunate. Their safety incidents do not result in such tragedy, but they do impact production. For them, safety risks cost money.

In a paper published in the U.K., the author states that:

> *There are three commonly accepted reasons for reducing accidents at work i.e. legislation, humanistic and moral considerations, and economic considerations. Very often though the last one, economic considerations, tends to be forgotten. It is, however, accepted in industry that "good safety is good business."* [1]

So, why is safety important? It comes down to this . . . it is just the right thing to do.

To meet these growing safety needs, Honeywell offers a systematic, multi-phased engagement aimed at reducing the risks involved with unsafe or potentially unsafe conditions at a processing facility. With over two decades of Honeywell process safety management expertise in integrating process safety data, applications, system diagnostics and critical control strategies, Honeywell approaches safety in an integrated and comprehensive way.

1 Safety and the Bottom Line: Proving the Financial Benefits of Your Safety Initiatives. Mr ‘Fats’ Van Den Raad. Presented at the Proactive Accident and Incident Reporting & Investigation Conference. IIR Ltd, Stakis St. Ermins Hotel, London, 7-8 Dec 1999.

An Integrated Approach to Safety

Ensuring safety means reducing the risk of incidents, faults and failures that cost money. This effort goes far beyond simply installing fail-safe controllers or a safety instrumented system. In fact, to mitigate the risk of serious incidents that can cause injury to personnel, equipment, and the environment, as well as disruption of production capability, it is important to consider safety from all aspects of a plant's operation. This goes right back to the heart of the question, "Are we safe enough?"

Plant safety today requires a comprehensive approach including managing operator effectiveness, constant monitoring of distress indicators, personnel tracking and mustering applications, and ongoing asset monitoring and maintenance for asset health. This integrated approach demands not only understanding safety's relationship to human error, but also the inter-relationships among root causes and interventions by plant systems and plant personnel.

Honeywell's approach to plant safety helps customers improve their business performance and peace of mind. This solution includes independent yet interrelated layers of protection to deter, prevent, detect, and mitigate potential threats. Woven throughout these layers are features that offer ongoing assessment, as well as design, implementation, and assessment plans that directly improve work, people, and technology processes.

Creating Layers of Protection

The concept of layers of protection is widely recognized by the process industry, and the term is clearly defined in industry safety standards such as IEC 61508 and IEC 61511. 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 and gas protective systems or plant emergency response systems). Other layers of protection can deter incidents in the first place (e.g. plant and physical asset protection, constraint and boundary management, operator training, and asset management); while others can provide detection and alerting, and associated guidance (e.g. operator alarms, early event detection, and integrated operator procedures).

Layers can either be automated, such as emergency shutdown (ESD) equipment, or require human interaction such as operator responses to process alarms. Some layers offer easily quantifiable risk-reduction benefits, but require that the risks all be identified before. And still others are less tangible and offer softer benefits.

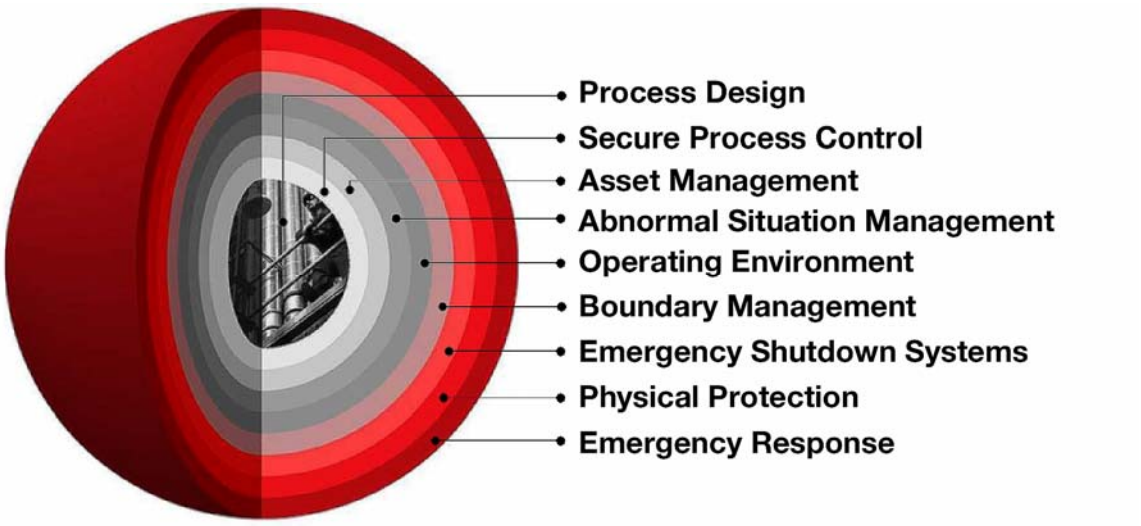


Figure 1. Integrated layers of protection

As shown in Figure 1, at the core of the layered architecture is a well-designed and implemented process design that is the embodiment of the business, safety, and production considerations necessary for effective operations. The process must be controlled

by a secure process control network that extends across the entire plant and business networks. Managing the plant's assets ensures that the process design continues to function as intended, all while protecting the plant from pending incidents with an early indication of failing assets.

As one moves through the layers of protection further away from the core of process design, mitigating risk due to human error is the key to ensuring safety. Implementing tools and procedures (such as boundary and alarm management and early event detection) for the purpose of managing abnormal situations reduces incidents and prevents escalation. Appropriate operating windows need to be defined and managed, and properly designed emergency shutdown systems must be in place as preventative measures in the event that an incident escalates beyond the inner layers of the sphere of protection.

Working across the various layers of protection, a plant or facility must operate in a secure and protected atmosphere, including protection of the perimeter, facility, people, and assets. With the correct work practices and technology in place, in the event that an abnormal situation does occur disrupting safe operations, an emergency response plan can be executed, controlled and monitored to minimize the impact of the incident.

In order to maximize plant effectiveness and to ensure that the question "Am I safe enough?" can be answered, a systematic approach to safety is required. This approach must minimize risks to safety and security, and it requires independent but interrelated layers of protection be in place across an organization.

Understanding Factors Affecting Safety

The Relationship to Human Error

One of the founding activities of the Abnormal Situation Management® (ASM) Consortium in the early 1990s was having a concept team review the commonality between five sites relating to abnormal situations. The team was established to address the current limitations facing industrial plant operations during abnormal conditions. Their objective was to recommend changes in methodologies, practices, and operations in order to establish best practices and to identify prioritized products and services which could be implemented over a three- to five-year period.

> The ASM Consortium convened informally in 1992 and was formally chartered in 1994 to enable and empower operating teams to proactively manage their plants, maximize safety, and minimize environmental impact—all while allowing the processes to be pushed to their optimal limits. Original ASM Consortium members included Honeywell, Chevron, Exxon, Shell, BP, Mobil, Nova Chemicals, and Texaco.
> www.asmconsortium.com

This ASM concept team reported on a serious upset at a petrochemical plant resulting in a flood of 60 alarms, assaulting plant personnel in one instance. During the next 15 minutes, operators, supervisors, board operators, and field operators frantically prioritized alarms, stabilized the process and diagnosed the cause of the upset. This high adrenalin period required the efficient use of intense communication, diagnostic tools (both manual and automatic), and an intentional collaboration between all involved.

Unfortunately, studies show that human error is a significant factor in almost all accidents, and that intense moments as described above either result in or exasperate these errors. A practical definition of human error is any human action (or lack thereof) that exceeds the tolerances defined by the system with which the human interacts. Human error in processing plants, although not intended, does happen. This is not to say that plant employees are unskilled and error prone. Most managers agree that their employees are skilled, careful, and productive, yet they do make mistakes. Why?

Further studies conducted by the ASM Consortium have shown that 42 percent of abnormal situations or upsets that occur in modern-day processing plants are due to people or their work context. Additionally, 36 percent of these are from equipment problems, and of those, one-half are a direct result of operating the equipment or process unit outside the operating envelope.

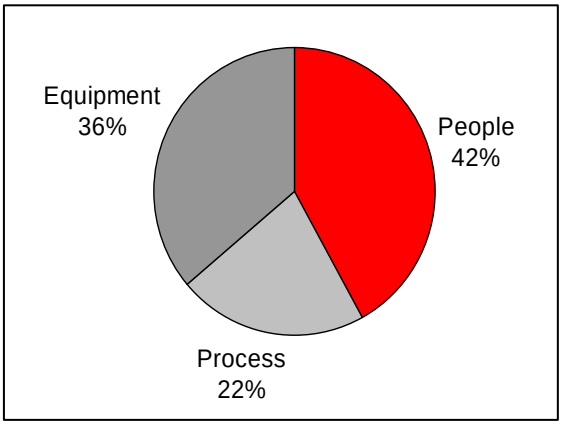


Figure 2. Causes of Abnormal Situations

These examples result in safety accidents with serious consequences. The American Petroleum Institute and the American Chemistry Council agree that in recent history the largest accidents in chemical and hydrocarbon processing facilities have severely injured or killed hundreds of people, contaminated the environment—resulting in greater than $8 billion in property damage losses. However, the actual cost of these accidents is certainly much higher if associated business interruption costs, cleanup costs, legal fees, fines, losses of market share, and so forth are also considered.

In order to improve operational reliability and to avoid some of these incidents, it is necessary to examine the work processes of the control room operators. Facilities need to decide what tools operators need so that they can be successful in their jobs and contribute to safe and profitable operations.

The Anatomy of a Disaster

Before considering the tools required to mitigate the issues relating to an incident, or the layers of protection that are required in a particular facility, one must have an understanding of how a disaster may propagate. The inter-relationships among root causes and interventions by plant systems and plant personnel are an important aspect of understanding the management of abnormal situations. Figure 3 illustrates the anatomy of a disaster.

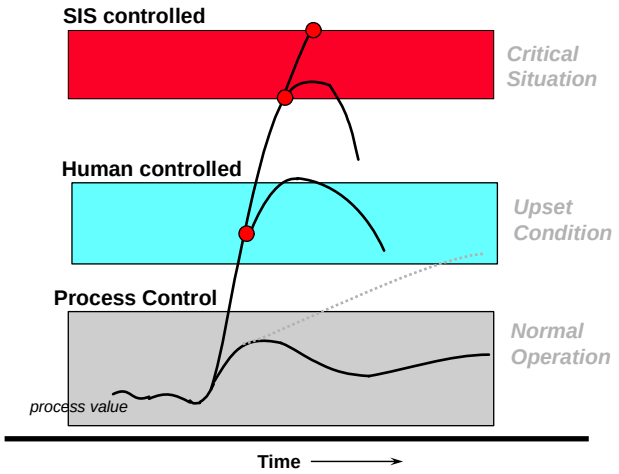


Figure 3. The Anatomy of Disaster

A typical process plant operates in the region labeled process control. The control system is tasked with keeping the process in this region of operation; and in most cases, it does. However, outside forces or disturbances can cause a process to deviate or drift from normal operation into the upset condition. If not mitigated, this abnormal situation continues into the critical situation zone. Figure 3 depicts the evolution of an abnormal situation from some initial cause that produces an operations upset to a catastrophic disaster involving serious destruction and harm to the plant and/or the surrounding community. The dotted line depicts an insidious problem that develops slowly over time.

Figure 4 illustrates the progression of an abnormal situation and the actions that bring the situation back to normal. Notice the difference in slope in this figure from the dotted line in Figure 3. One of the defining elements for an abnormal situation is the time it takes to develop and the urgency with which a response is required. Each of the zones requires a different intervention, ranging from normal control action to mechanical shutdown by a safety instrumented shutdown system. Each of these interventions is independent— the process system, the protective applications and shutdown system, and the safety containment system are designed to safeguard the plant from catastrophic events.

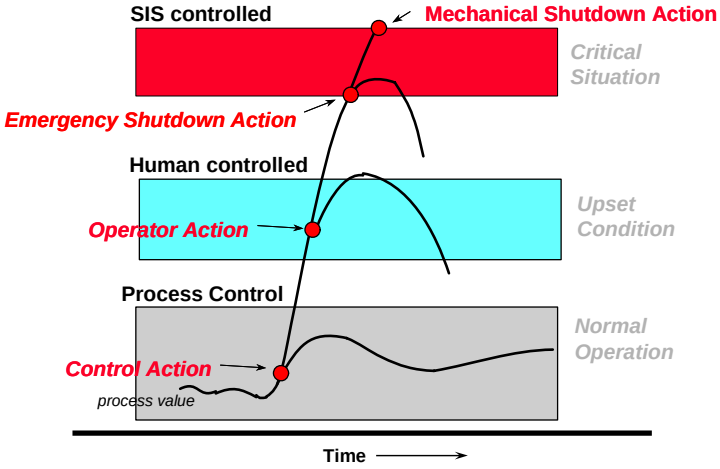


Figure 4. The Anatomy of Disaster—Intervention Points

The event sequence illustrates the intervening role of plant personnel to prevent a process upset from escalating to a plant shutdown. In the event of a loss of control, the plant personnel must intervene to minimize the impact of a disaster. Failing that, it is up to the safety instrumented shutdown system to take action.

There are a number of factors that can contribute to the onset and escalation of an abnormal situation. In Figure 4, ‘operator action’ refers to activities performed by a typical operations crew comprised of console operators, lead operators, supervisors, and field operators. This also includes coordination among operations crews responsible for different areas within the plant and any technical support engineers. In most situations, when we refer to abnormal situations we think of the console operator as the only person available to respond because of the speed at which most abnormal situations evolve. Although this is not always the case, the ability to support the console operator in real-time is essential for mitigating process upsets and requires integrated and timely communication.

A number of authors have developed models to describe cognitive behavior when dealing with a disaster. One model proposed by the Chemical Manufacturers Association is a simple loop process that describes three stages of processing within the operations team:

Process Stage	Description
Orienting	**Sensing, perceiving, and/or discriminating an anomaly** The team perceptually discriminates an anomaly in the process. This can happen by a number of means: An alarm in the process control system, or an alarm or trip in the safety shutdown system may direct the operations team to a specific point in the process. The operations team may be monitoring the process using schematics (with value readouts) or trends, and determine that an anomalous condition exists. An extensible indicator, such as the size of flame in the flare or the sound of an emergency relief valve, alerts the plant personnel to a problem.
Evaluating	**Information processing (thinking and/or interpretation)** The operations and/or technical support team develops hypotheses regarding the cause of any anomalies. An individual may be so well-rehearsed for certain response conditions that it may appear that this intermediate stage of processing is skipped.
Acting	**Responding** The operations and/or technical support team must take compensatory or corrective action. This may include using an automated control system or the assistance of plant maintenance personnel. Not all actions will be corrective (e.g., reestablishing a stable process by manipulating process parameters). The operations team may perform hypothesis testing actions to determine if the supposed problem is, in fact, real.

Design for Disaster

With a clear understanding of how abnormal situations develop, and with many tools available to help mitigate these situations, one can design for the inevitable.

Figure 5 illustrates the various levels of protection available to mitigate an abnormal situation as the upset escalates beyond a preceding layer.

As described earlier, the control system is composed of instrumentation and a distributed control system designed to maintain the process in the normal operating region. Inefficiencies can occur in a process, equipment can fail, and a process can drift beyond the optimal. The intent of the asset monitoring layer is to provide an early warning of pending failures before they become operational concerns.

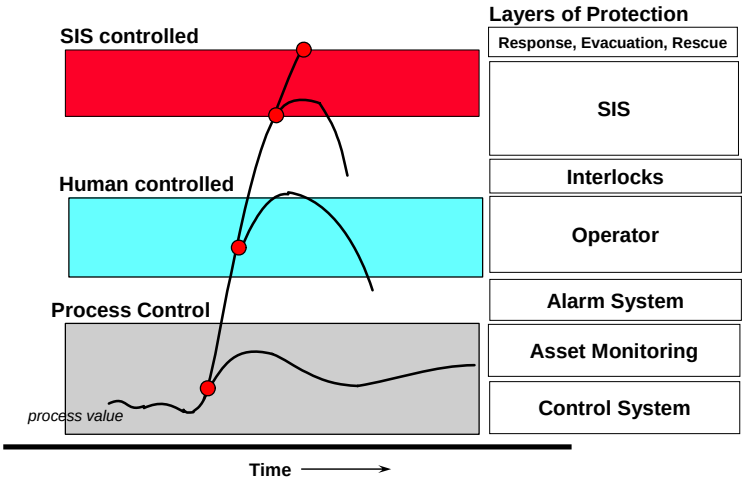


Figure 5. Layers of Protection

The alarm system is the operator's first warning that the control system cannot cope with a pending condition. When properly engineered, the alarm system warns the operator that an action is required. From here, the operator needs to interact with the system to bring the process back to the normal zone of operation.

Next, system interlocks, triggered by field switches or stored boundaries or constraints, may intervene. Typically these interlocks are built into the control logic or procedures to prevent equipment damage or worse. Within this category of interlocks is a work process to establish limits. In operations management, the critical, standard, and target boundaries of system variables or processes must be clearly understood and defined. This requires supporting information including the purpose of the measurement, a piping and instrumentation diagram reference, equipment constraints, corrosion control limit, safety limit, and environmental limit—all stored or referenced so that the database is a complete repository of the information associated with both the variable and boundary.

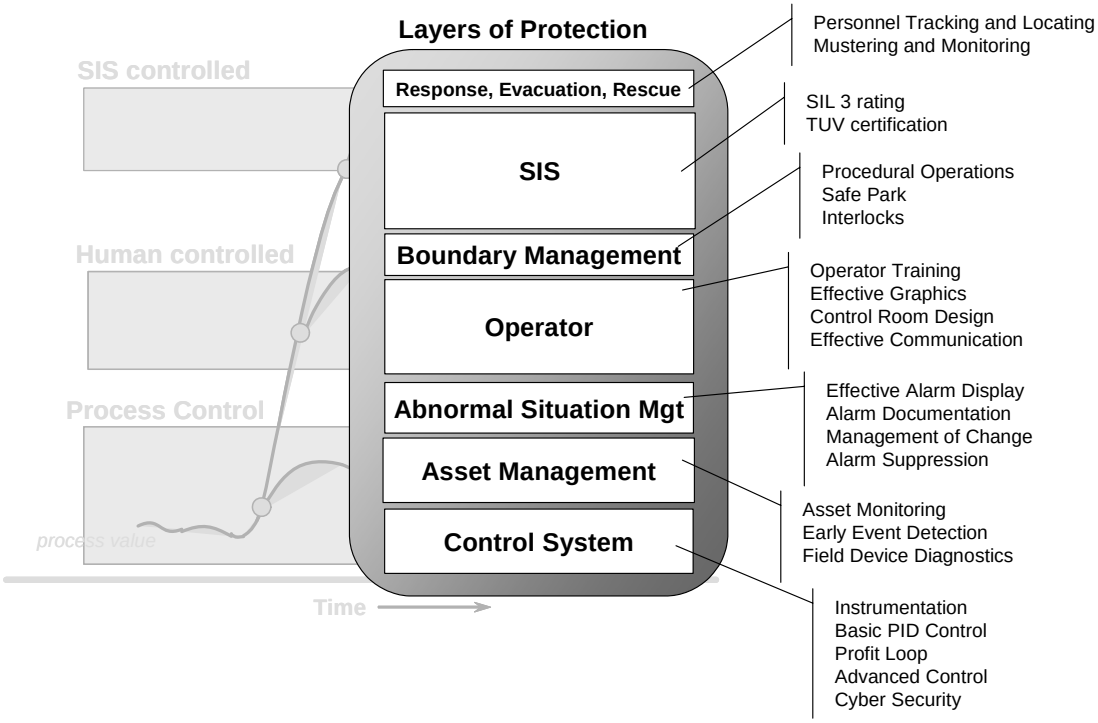


Figure 6. Components of the Layers of Protection

The final two layers play an integral part in the protection of life and plant assets, although everyone hopes that a situation never requires these levels. The safety system provides a redundant and final layer of protection that brings the plant to a safe condition. Failing all else, a layer that demands consideration is the one that contains the applications that aid in tracking personnel and mustering those that are evacuated in the case of an emergency. Figure 6 details some of the applications associated with each of the layers. The following sections of this paper are devoted to the examination of these layers in more detail.

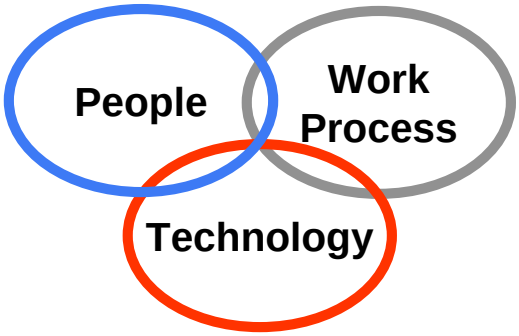
Implementing Layers of Protection

Integrate Discipline Throughout the Layers of Protection

Safety is more than just installing a fail-safe controller. Since disruption can occur at every level and from seemingly simple issues, every layer must be part of the improvement process targeted at safety. Therefore, in order to mitigate the risk of threats, it is extremely important to consider safety in all aspects of operation.

For modern-day processing plants, safety standards are a crucial layer of protection. It is important that when we consider safety, we consider all the layers of protection in an integrated fashion. Since the lower layers protect against ever needing the upper layers of protection and help mitigate some of the costs involved with such incidents, each layer clearly has its own unique importance for ensuring plant-wide safety.

With the complexity of process units today, and given the current pressures on the business environment, mitigating risk involves more than just the proper application of hardware and software. A plant must consider an integrated approach to managing the total enterprise when designing for risk management that maintains a safe operating environment. This plan must also include a goal of achieving operational excellence through best-in-class work practices and a commitment to achieving a world class safety record.



Safety success requires a structured approach that includes an integrated look at the process and system **technology** that is used at a site, the **work process and practices** that make use of and maintain this technology, and the **people** and their collective abilities that interact with both technology and work practices.

Technology—All plants have access to available technologies and the expertise required to benefit from this technology. The challenge is applying the right technology in the right context. Capital investments must be made wisely, especially when it comes to safety.

Work Process and Practices—The traditional safety study focuses on physical hazards and process-related issues. However, true improvement requires crossing functional lines and recognizing the way people interact with the process and the assets. .

People—Operational excellence is achieved by continuously striving to operate at peak performance with no tolerance for upsets, product giveaway, or unplanned downtime. This means minimizing human error, ensuring plant integrity, and remaining agile to meet rapidly changing marketing conditions.

The most successful companies utilize this integrated approach as the basis for improving safety and productivity. Optimizing work practices has implications beyond the realm of safety. For example, true enterprise management comes from seamless integration of functional lines such as crude purchasing, operations, maintenance, and marketing in order to achieve optimal results.

Regulations and Standards

Any improvement program starts with understanding the regulations and standards that affect every layer of protection. At the same time, a discussion of the appropriate use of control system and safety instrumented systems spans several of the layers of protection.

At the highest level, a safety program for any refinery in the United States should be in conformance with the Occupational Safety and Health Administration (OSHA) Standard 29 CFR 1910.119 and the Environmental Protection Agency (EPA) Regulation 40 CFR Part 68. The regulations set requirements for mechanical integrity programs; and the standards apply to a number of equipment items, including “(iv) emergency shutdown systems (v) controls (including monitoring devices and sensors, alarms, and interlocks).”

The regulations also require that programs be developed and implemented for the above systems with the following provisions:

- Written procedures
- Training for process maintenance activities
- Inspection and testing
- Equipment deficiencies
- Quality assurance

The OSHA and EPA regulations are performance based, allowing the owner/operator of the facility to implement a program that is most suitable for the organization and site, as long as it meets the general requirements. The industry has been very supportive of the goals promulgated in these standards, has supported their implementation by providing standards, and has recommended practices and technical reports that provide guidelines for how these regulations are implemented. This additional guidance is published by industry groups where their membership has particular expertise. Some of the organizations that have published relevant guidance include:

- American Petroleum Institute (API)
- National Fire Protection Association (NFPA)
- Instrumentation, Systems, and Automation Society (ISA)
- International Electrotechnical Commissions (IEC)
- Engineering Equipment and Materials Users Association (EEMUA)
- Abnormal Situation Management (ASM) Consortium
- American Institute of Chemical Engineers (AIChE)
- American Chemistry Council (CIDX best practices)

The program that an owner/operator implements at a specific site is not required to be identical to the standards, recommended practices, and technical reports provided by these bodies. However, these resources do provide an excellent benchmark. If programs are not in conformance with these guidelines, there should be solid explanation of why the industry guidance is inappropriate and why the site's alternative is superior.

Honeywell programs follow OSHA's Program, Quality, and Verification (PQV) auditing method. First, the program for the audited element must be identified. Then, the program quality is judged in comparison to OSHA/EPA regulatory compliance and industry guidance and benchmarks. Finally, verification of implementation of that program is performed through documentation searches and staff interviews.

Safety Instrumented Systems Integration

The process industries have employed a long and successful practice of applying redundant process control and safety systems to operate their profitable critical processes. Redundant process control systems and safety systems have achieved superior reliability and high availability by applying a very important architectural principle entitled the separation principle. The design criteria behind this principle calls for separate safety and control.

This separation principle is not new. It was recognized in the earlier days of plant automation and later consolidated in the IEC 61508 standard, the umbrella safety standard for all automated process applications.

Some statements from the IEC 61508 standard are very clear about this principle:

> *"Where an E/E/PE safety-related system is to implement both safety and non-safety functions, then all the hardware and software shall be treated as safety-related."*
>
> *"Whenever practicable, the safety-related functions should be separated from the non-safety-related functions."*
>
> *"Caution should be exercised if non-safety functions and safety functions are implemented in the same E/E/PE safety-related system. It may lead to greater complexity and increase the difficulty in carrying out E/E/PES safety lifecycle activities (for example design, validation, functional safety assessment and maintenance)."*

The safety and control systems must be integrated to allow a smooth and safe plant operation, but only to a certain level. Dedicated safety-related parts, such as the actual safety-related application (during application design and the application as running on the dedicated safety hardware) must stay segregated, as they may not be changed without authorization and must be subject to high safety integrity.

Four levels of integration are essential from a usability point of view.

- First, the operational integration must allow the plant personnel to have a seamless, transparent interface to the process under control. Whether the actual strategy is running in the process controller, the safety system, or on a higher level makes no difference. All required information will be available on the operational level.
- Second, peer-to-peer communication between safety controllers and process controllers is the key to integration. Information from one controller needs to be communicated to peers quickly in order to anticipate process startup or abnormal situations in a controlled manner.
- Next, all data that is available in the lowest level of process and safety I/O can be transferred to the higher level of operations and turned into information that is usable for various higher level applications.
- Finally, builder tool integration only has added value if the point information is interchangeable. This means that the user has a single point of data entry and all information entered into the database can be replicated to other databases. The information is available for use in all levels of the safety and control topology.

Honeywell's integrated safety and control offerings have always held true to these principles. As far back as 1996, Honeywell offered an integrated control and safety solution that was driven by the separation principle—hardware and software diversification, integrated operator interface, integrated data processing, integrated post mortem analysis, and integrated alarm management.

Operator Effectiveness

The layer of protection often missed is the one requiring human intervention. It is essential to equip the operations group with technology and work practices to manage abnormal situations or the eventuality of an incident. In addition, as an experienced workforce transitions and domain knowledge is potentially lost, it becomes increasingly important to transform that knowledge into institutional procedures and practices.

The ASM Consortium has dedicated itself to pursuing methodologies specifically designed at reducing upsets and preventing them from escalating. With a primary goal of ensuring the operator is properly equipped to recognize an event, as well as capable of properly evaluating the situation and responding accordingly, their focus has been in several areas of advanced research and development. The primary areas of emphasis include:

- alarm management
- operator environment
- field operator communications and work practices (recognizing that the field operator is also a key part of the operations group)
- early event detection

Alarm Management
Every process plant of any significant size has an alarm system. In most existing plants there are several thousand alarms configured. Most alarm systems are DCS-based, with some critical alarms hard-wired. Some alarm activations are too frequent, with many plants having rates between 20 and 60 alarms per hour during normal operation. Operators are effectively responding to the alarm system on nearly a full-time basis. When discussed in the context of safety and dealing with an escalating incident, this prospect is very concerning.

During an upset condition, alarm activation rates often exceed 30 alarms per minute. This condition (known as alarm flood) often continues for prolonged periods. Operators cannot possibly respond to such a high alarm rate. The end result is that some genuinely important alarms are missed in this flood of information, possibly covering up the incident that is causing the flood.

The situation described above is not universal. There are some plants where alarm activation rates are much lower. This isn’t due to the size or type of plant, but is due to the engineering and operations work practices instituted to ensure a safe operation. Many plants lack the systematic design and operations practices required for improved alarm management. In many long-established plants, the alarm system has received little critical attention during 20 years or more of plant operation.

Focusing specifically on alarm management, we see:

- Industry bodies, such as the ASM Consortium and EEMUA, have identified many shortcomings in existing alarm systems.
- A number of serious incidents have been attributed, in part, to poor alarm management.
- Alarm activation rates varying widely, even on similar plants; it is clear that it is not a lack of technology that prevents improvement.
- Regulatory bodies such as HES have started to focus on improvements in alarm management as a means of improving safety.
- The IEC 61508 standard also impacts the way in which safety-related alarms are implemented.
- The EEMUA guidance document is based on the advice of experienced industry representatives and provides a documented methodology for improvement.

The Seveso II Directive requires EC member states to use the Safety Case framework as a means of reducing risks at major hazard installations. In the U.K., the HSE is strongly encouraging compliance with both IEC 61508 and EEMUA recommendations as part of the Safety Case.

In summary, alarm system improvements are essential and regulators are requesting changes that will impact alarm system design, and will make available the tools needed for improvement.

The Operating Environment

The operators' work environment consists of more than just alarms. Other factors must be considered to provide an optimized operations work environment. For example, ASM Consortium research has proven that ergonomic elements such as lighting, noise levels, seating position, and traffic flow can have a tremendous impact on the safe and effective operation of a process plant.

By providing an environment that is highly integrated, interactive, and participatory, one can minimize the potential for process error, provide an environment conducive to reducing the number of incidents, and improve overall operator ownership of the control center.

The ASM Consortium has identified several basic human factors as critical in control center operation, for both abnormal and normal conditions. The following components must come together to provide a control environment best suited to managing abnormal situations:

- Positioning the right number of operator work areas and consoles
- Optimum communication between console operators and other operations and production personnel
- Ergonomically correct equipment and user interface design
- Effective and efficient work practices
- Critical factors for areas that impact operators' work environment in the control room as they pertain to each operation including competency levels across operations teams
- Effectiveness of communication (situational awareness) and collaboration of the operations team
- Effectiveness of the console operators' user interfaces
- Environmental stressors in the control building
- Effective and appropriate allocation of tasks and workload under normal and abnormal conditions
- Communication flow between management, production, and operations

The work environment must be conducive to readying the operator to deal with average and peak workloads during both normal and process upset situations.

Field Operator Communication and Work Practices

The third element of the operator effectiveness layer of protection covers field operator communication and work practices. The field operator is a key part of the operations group. Mobile technology is maturing quickly as the market demands accelerated deployment of enterprise applications to the field workforce. Further, the process manufacturing industry is beginning to adopt and deploy mobile computing applications with an emphasis on operational excellence and operator-driven reliability programs. In many cases, executive management is placing emphasis on reliability improvement initiatives that require plant operators to uncover hidden opportunities to improve efficiencies and reduce operating costs.

The focus thus far has centered on the board operator. Unfortunately (or perhaps not), not all measurements made in a modern-day processing complex are instrument based. In fact some studies show that the typical control system only captures approximately 50 percent of a plant's data points. This leaves out field data, field operator observations, and the exceptions captured by those not wired to the I/O racks. Wireless mobile computing technologies allow field operators to get connected, thereby accurately transferring the remaining 50 percent of the plant's data points to the myriad of people and plant applications required to run the plant safely and productively.

Combining software applications and hardware with a handheld wireless computer and integrating it into the existing plant computing infrastructure brings together field operators, supervisors, console operators, and other plant personnel indirectly through connectivity to other plant applications.

Armed with mobile productivity tools, the field operators become central to a workflow that encompasses everything from work order creation to historical data trending. Information that is gathered in the field flows from the field operator to the supervisor and from there to the console operator. Supervisors can be in the loop to review the data from the field and ensure the correct inputs from the field. The console operator can then use the field-based inputs as a positive feedback mechanism for field operating conditions.

The same non-instrumented data can be distributed to the plant historian and work order system in such a way that the field operator's entries can be historized, or they can be used to initiate a work order notification. Similarly, work orders can be provided on the handheld, along with details of faults or failures, from the asset management system. The end result is a technology that brings an extended set of data from the field while at the same time empowering the field operator with greater connectivity to the plant-wide automation system.

Early Event Detection

Another current area of research for the ASM Consortium is early event detection (EED). This is the next layer of protection in the category of operator effectiveness.

Although beyond the initial scope of many initial automation or asset management projects, it is worth wondering what else a site might do to detect process problems. As a site builds an infrastructure for application for control and asset management, it becomes obvious that the possibilities range from the very simple diagnostics, to multivariate statistical analysis tools for building empirical process models to detect process changes. Regardless of the technique used for detection, the intent is to predict a drift or deviation from normal conditions in a process before an alarm is heard on the control panel.

In process industries, it is a significant advantage to be able to detect a change of state in a process before it becomes an abnormal situation. This analysis or a prior knowledge of a fault allows for preemptive action. If a situation is detected using traditional operator-based methods of fault detection and diagnosis, it is often too late.

Detecting performance changes in a process can be achieved using multivariate statistical analysis methods. Studies by the ASM Consortium found that principal component analysis (PCA) can effectively predict abnormal situations before operators discovered them. Consequently, the basis of Honeywell's process state estimation efforts, and consequently Honeywell's EED Toolkit, is based on this technology.

Asset and Process Reliability

Not unlike the previous discussion on early event detection, asset management tools and technologies help prevent abnormal situations from escalating beyond control. With online tools, assets can be monitored and pending conditions sent to the appropriate personnel for early mitigation. Similarly, with proper maintenance and work practices, it is possible to remove the root cause of an incident.

As shown in Figure 2, the ASM Consortium has reported 36 percent of abnormal situations are equipment based. Situations arise when these equipment problems escalate beyond the control of human intervention and require a safety shutdown system. With a layer of protection focused on the assets themselves, subsequent layers, in some cases, may not be required.

Asset management solutions should follow these specific principles:

- **Freedom of choice** – Support multiple protocols, multiple suppliers, and multiple methods. "One size fits all" approach will not work. For example, Honeywell's Asset Manager enables multi-supplier and multi-protocol support integrated into an overall asset effectiveness strategy
- **Software-enabled** – Wherever possible, solutions should utilize information already existing within the SIS/DCS/historian, and should not force the end-user to buy new hardware to get the value of monitoring the SIS health. Honeywell's Safety Valve Scout is one example of this philosophy.
- **Process-centric** – Focused on the Safety Instrumented Function (SIF) and its effect on the process – not focused on the individual devices. The SIS Health Monitoring solution recently developed by HPS in conjunction with one of our key customers analyzes the reliability of the SIF and its effects on the process with data taken from actual system performance.

An asset management solution must include a comprehensive package for monitoring all types of assets, from field device to process unit. Asset management starts with the control system with field device configuration, calibration management, and diagnostics. In this raw form, the data is made available for asset management through a process knowledge system (PKS). From here, the data can be further processed simply by the operator in a console detail display or in more detail by a maintenance technician on the asset management node.

Asset monitoring functionality can be further split into several sub-areas, given that a PKS not only diagnoses control system and field device problems, but also process-related issues. The diagnostic component of Experion PKS comes from the ability to monitor the cause-and-effect relationships using Asset Manager.

Most asset management offerings are instrument-centric, focusing only on field devices and not on the impact of these and other assets on overall operational and process effectiveness. The complete asset effectiveness solution connects once-isolated silos of knowledge and delivers this information to the right people at the right time, thereby improving decision-making and reducing incidents.

To put the potential of an integrated control system, such as Experion PKS, infrastructure in place to monitor more than just field devices, consider the definition of reliability-centered maintenance (RCM). RCM is defined as "a process used to determine what must be done to ensure that any physical asset continues to do what its users want it to do in its present operating context."

Traditionally, the science of reliability-centered maintenance was focused on rotating equipment. However, the Marshall Institute reports that, "most of the dollars lost from unreliability come from fixed equipment like piping, vessels, and heaters." Thus, the focus on reliability and availability should not only include the most obvious assets such as the field devices but should include all plant assets.

Work practices for improving reliability should also extend past the maintenance department and become best practices in operations. With access to non-instrumented data input, the synergy between maintenance and operations for improved operations and reliability can be captured. This forms the basis of a process-centric solution.

Plant and Process Security

Raising the Bar on Safety and Security Accountability

Pacesetting organizations are recognizing that the bar for security accountability is rising. Whether the pressure comes from the insurance industry, regulators, or internally driven safety programs, manufacturing executives must consider technical services and solutions in step with the advances in automation and computer capabilities. In light of the high risks associated with abnormal situations and the high cost of preventing them, no process manufacturer can afford to ignore them.

In March 2003, the U.S. Department of Homeland Security (DHS) indicated that chemical and petrochemical plants are attractive terrorist targets. Additionally, the EPA concluded there are more than 7,700 chemical plants in the U.S. in locations where, if there were a terrorist attack, a thousand or more people could be injured. There are 100 facilities where a terrorist attack could place at least one million people at risk. The new reality of terrorist threats has given momentum to industry and government initiatives aimed at enhancing the security of industrial facilities to meet non-traditional threat scenarios.

Security in the chemical and petrochemical community prior to September 11, 2001 was primarily in place to protect against thefts and accidents. Post 9/11, the attention has expanded to ensure business continuity and minimize environmental and safety impacts in the event of an attack.

In addition to the risk of traditional attacks against physical assets, modern process control and safety systems using open systems technologies are exposed to new attacks directly against the cyber network. To address this growing threat to cyber security, the U.S. DHS has funded the establishment of the Process Control Systems Forum (PCSF). The PCSF accelerates the technology development to enhance the security, safety, and reliability of process and supervisory control (SCADA) systems.

An American Chemistry Council Chemical Industry Data Exchange (CIDX) document titled “The Case for Taking Action on Cyber Security” identifies the following concerns associated with security, particularly for those facilities that are deemed high risk:

Release, diversion, or theft of hazardous materials	Loss of production capacity
Employee and public fatalities, injuries and health effects	Interruption of production
Violation of regulatory requirements	Fire and significant explosions
Loss of proprietary or confidential information	Equipment damage
Process upsets/process shutdown	Societal impacts
Product quality problems	Loss of public confidence
Contamination of products	Impact on national security

Plant and process security is integral to improving safety for two reasons. First, applying comprehensive security in a defense-in-depth approach can dramatically reduce the likelihood of a successful security incident. A defense-in-depth approach will include elements of physical, electronic, and cyber security.

Physical, Electroni, and Cyber Security Layers

Woven into the layers of protection shown in Figure 1 are a series of layers relating to plant and process security. An effective approach for protecting an industrial facility employs not only elements as previously discussed, but also elements protecting against a variety of threats, including threats to physical and cyber security. This includes:

- Monitoring and protecting the perimeter
- Identifying and controlling who enters and exits a facility
- Tracking movements of building occupants and assets
- Controlling access to restricted areas
- Quickly locating equipment, products, and other resources
- Improving emergency response time
- Preventing theft
- Integrating systems for greater speed and efficiency
- Protecting process automation networks and systems from cyber threats
- Implementing policies, procedures, and education

The integration between building automation, security, and process control systems at plants plays a crucial role in rapid, efficient, and coordinated mitigation steps during a security incident. A close linkage between security and process systems ensures that a process control system operator is immediately made aware of a security breach so they may take preventative action to protect the safety of individuals in and around the facility.

Physical and Electronic Security Layers

Viewing a facility from the outside perimeter inward, the physical perimeter is addressed by those technologies that have more visible, tactile characteristics—including fences, barricades, guards, and other assets used to prevent entry by unauthorized personnel.

An electronic security layer employs technology such as video cameras, access cards, and motion detection equipment. State-of-the-art systems use wireless and microwave closed-circuit television (CCTV) technology to monitor the perimeter. Digital video technologies can substantially optimize the monitoring regime by employing sophisticated pattern recognition to detect unusual movements. Access control systems track everyone who enters and exits a facility, allowing operators to know who enters and departs, as well as where they are located while on the premises. Both video and access records can be stored electronically for simplified retrieval and review.

Access control technology plays an important role during incident mitigation. In the event of an incident, it may be important to muster individuals in a safe location. An electronic mustering station allows security or operations personnel to quickly identify which individuals are in the safe location. For those who have not reported to the muster location, access control records may be searched to determine the last known whereabouts of individuals. The use of CCTV cameras can be used to determine the location of individuals requiring emergency assistance.

Cyber Security Layer

A dramatic transformation from proprietary to open control systems has been underway within the process control industry. This trend, coupled with the connectivity between open control systems and enterprise networks, has introduced unprecedented cyber vulnerabilities in process control systems.

Further, safety systems that are designed to bring a process to a safe state in the event of a failure are being integrated with open process control systems. This integration introduces the risk of a common cause cyber fault which not only disrupts the process, but also prevents the safety systems from responding to such disruptions. Without an effective cyber security strategy, the fundamental mission of process control—to ensure safe and reliable operations—can be compromised by an ordinary cyber threat such as a virus or worm. Therefore, a comprehensive cyber security strategy must be an essential element of every process control and safety system implementation and should include the following:

- Regular risk and vulnerability assessments
- Hierarchical architecture with cyber security access restrictions at each network level
- High security model deployed on PCs and servers
- Physically separated process control and enterprise networks with limited access points
- Physically separated process control and process safety systems with limited access points
- Security hotfix and antivirus deployment strategy
- Disaster recovery
- Best practices, policies, procedures, and change management
- Dedicated service team responsible for cyber security

A Systematic Safety Improvement Process

Typically, a safety and security improvement effort is a systematic, multi-phased engagement aimed at reducing the risks involved with unsafe or potentially unsafe conditions at a processing facility. As shown in the figure below, the initial phase of this engagement includes an assessment and provides benchmarks of current safety work practices and competencies, while at the same time identifies and prioritizes opportunities for improvement. The effort can be focused plant-wide, but initially can be primarily focused within a particular process unit.

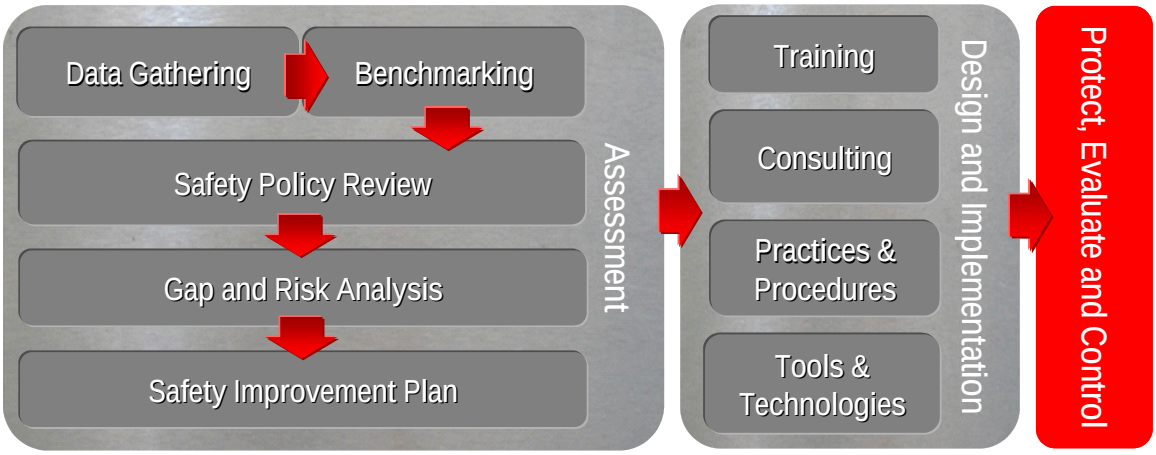


Figure 7. Comprehensive approach to improving safety

Assessment, the first phase of improvement, identifies the unit's safety and security performance, and provides recommendations for improvement with a structured methodology and technical expertise at the core of the assessment. The assessment output is an overall plan for future implementation. Throughout the engagement, the methodology is executed as a collaborative effort, thus promoting active participation from all those involved at every step.

The second phase of improvement is typically a design and implementation phase. Depending upon the outcome of the assessment, this may include activities such as developing personnel, facilitating organizational and procedural changes, implementing a metrics system for monitoring progress, and installing technology required to accomplish the job.

The final phase, and arguably the most important, of any improvement program focuses on retaining and sustaining the benefits of each improvement. With periodic performance monitoring and reporting, reassessment as necessary, and ongoing training, coaching, and facilitating as required, your investment in the improvements and work done in the previous two phases is protected.

Intermingled in these three phases are five key elements. Any sustainable and successful program of improvement must include:

- a structured improvement process
- systematic benchmarking
- an integrated approach focusing on people, technology and work process
- a cross-functional team approach that includes industry-specific domain knowledge
- tools that enable and sustain work practice improvements

Summary

The processing industry is facing real challenges as technology is forever advancing, seasoned industry professionals are retiring, and the business environment of the new global economy pressures managers in different directions. At the same time, moral, regulatory, and insurance requirements must be met in terms of maintaining a safe and secure workplace.

Research has shown that abnormal situations cost many millions of dollars. Manufacturers pay dearly for these catastrophes. There are numerous catastrophes that can be cited, but they all indicate the need for focusing on layers of protection to provide a safer work environment, while at the same time increasing process availability and reducing total cost.

Reducing the number of incidents and potentially decreasing the severity of such incidents when they occur, offers benefits to the operating companies, their personnel, the community, and insurers.

In what is an increasingly competitive marketplace, the players in every sector of industry have access to the same technologies. Implementing technology-driven solutions may provide some relief to the pending safety pressures. However, not until a site considers independent yet interrelated layers of protection to deter, prevent, detect, and mitigate potential threats will there be a satisfactory answer to the question “Are you safe enough?”

For More Information
To learn more about Honeywell’s integrated safety solutions, visit 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-05-003-ENG
November 2005
Printed in USA