

To improve the safety of the operating environment, a holistic method for defining and evaluating the systems that aid an operator with the safe operation of a process unit is required. This approach starts with an audit of the site's work practices and approach to safety as well as an analysis of the "as-built" condition of the site's layers of protection.

Stepping back and considering or defining a "safety system" as the many levels of protection used at a site allows the plant operator to better use each of these independent yet interrelated layers.

The concept of "layers of protection" is widely recognized in the process industry but is not always recognized as being implemented as interrelated systems. The term is clearly defined in industry safety standards such as the International Electrotechnical Commission's (IEC) standard 61508 and IEC 61511.

Some layers of protection are preventive like emergency shutdowns, and some are there to mitigate the effect of an incident once it occurs, such as fire and gas protective systems or plant emergency response systems. The layers that are often missed are those that deter incidents in the first place (e.g., plant and physical asset protection, constraint and boundary management, operator training, and asset management); and those that can provide detection and alerting, and associated guidance (e.g., operator alarms, early event detection, and integrated operator procedures).

Fig. 1 shows that 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 the while protecting the plant from pending incidents with an early indication of failing or poorly performing assets.

As one moves through the layers of protection further away from the core

## Holistic approach to safety systems produces improvement methodology

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) to manage abnormal situations reduces incidents and prevents escalation.

Appropriate operating windows must be defined and managed, and properly designed emergency shutdown systems must be in place as preventive measures in case an incident escalates beyond the inner layers of the sphere of protection.

To maximize plant effectiveness and to ensure the best safety level, 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 are in place across an organization.

Peter Jofriet  
Honeywell Process Solutions  
Cincinnati

### LAYERED APPROACH TO PLANT SAFETY

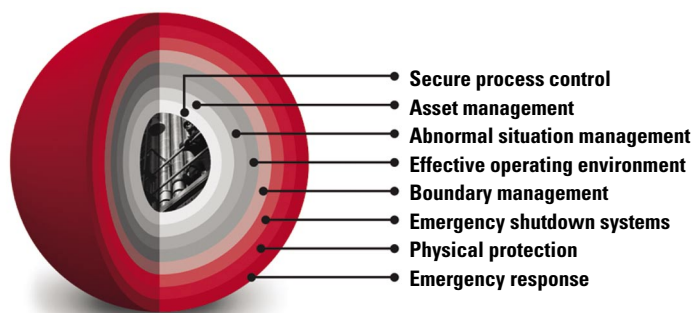


Fig. 1

Based on a presentation to the National Petrochemical & Refiners Association Annual Meeting, Salt Lake City, Mar. 19-21, 2006.

Although every site is different, there are some common or basic components needed in an analysis of the “as-built” condition of the site’s layers of protection. The overall intent is to assess the areas of risk and potential areas for improvement.

The areas that should be considered are:

- Regulatory compliance.
- Instrumentation and control.
- Asset and abnormal situation management.
- Physical and system security.
- Work practices and policies.

## Regulatory compliance

At the highest level, a safety program for any refinery in the US should conform to the Occupational Safety and Health Administration (OSHA) standard. These regulations require that programs are developed and implemented including these provisions: written procedures, training for process maintenance activities, inspection and testing, equipment deficiencies, and quality assurance.

OSHA and EPA regulations are performance based, allowing the owner-operator of the facility a great degree of latitude to implement a program that is most suitable for the organization and site, as long as it meets the general requirements listed in the standard.

Industry has been supportive of the goals promulgated in these standards and has supported their implementation by providing standards, recommended practices, and technical reports that provide guidelines for these regulations. Industry groups for areas where their membership has particular expertise publish this additional guidance.

Although 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, they provide an excellent benchmark for the practices of industry. If a site’s programs do not conform to these guidelines, there should be a solid

explanation why the industry guidance is inappropriate and why the site’s alternative is superior.

## Instrumentation, control

Fig. 1 shows that a secure process control system is one of the base layers upon which everything else is built. As part of any holistic look at safety, one must verify that the relevant programs are in place for verification of relevance of instrumentation and control systems, and that these systems are performing adequately.

There are several general guiding principles or benchmarks against which one can judge these types of systems.

## Classification

All instrumentation and control equipment should be classified. EPA and OSHA regulations and many industry standards are risk-based, allowing maintenance and testing resources to be disproportionately spent in areas where higher risk is perceived.

In addition, different standards are applied to different kinds of instrumentation. A good classification process is a necessary first step in implementation of a mechanical integrity program.

An appropriate industry standard that can be used as a guideline for this task is ISA 91.01, “Identification of Emergency Shutdown Systems and Controls that are Critical to Maintaining Safety in Process Industries.”

## Identify programs

The body of instrumentation and control equipment should be subdivided into categories. These are at the discretion of the plant operator to some degree but typically include:

- Regulatory control systems. These are not protective and include instrument categories not listed hereafter.
- Safety instrumented systems.
- Alarm systems.
- Fire and gas systems.
- Burner management systems.
- Compressor, turbine monitoring systems.

- Simple manually activated protective systems (e.g., remote isolation valves).

- Complex manually activated protective systems (e.g., HF alkylation water curtains and cannons).

For each type of system, a program should be in place that includes provisions for the frequency of inspection and testing and procedures by which those inspection and testing tasks are performed.

These programs should consider both recommendations of the vendor and criticality of the instrument. The program should also describe methods by which proper equipment selected and installation is ensured.

## Safety instrumented systems

Programs for safety-instrumented systems are generally performed in accordance with ISA 84.00.01, “Functional Safety: Safety Instrumented Systems for the Process Industry Sector.”

This standard requires that all safety-instrumented functions be classified with a safety integrity level of 1, 2, or 3. The equipment selection and test plan is developed in concert with a quantitative reliability assessment showing that the probability of failure of demand estimated for the system is in accordance with the safety integrity level selected.

## Regulatory controls

A program for integrity of regulatory controls is generally considered less critical than the program for protective functions; however, without good regulatory control the likelihood of an upset increases, as does a resulting escalation to process incident.

Considering that most business decisions made in a plant are ultimately carried out by the control loop (arguably, the heart of any automation system), it is alarming that two thirds of all control loops perform in a disruptive or ineffective manner.

With some manner of control-performance monitoring service, closed loop operating data can be used to identify areas where maintenance and

engineering actions are required to resolve the worst-performing loop problems.

### *System performance review*

A review of the control system network's performance is essential for identifying any loading problems or bottlenecks. The reliability and performance of a control system can directly affect the effectiveness of an operator and, ultimately, the plant's safety. On a regular basis the health and status of a control system network must be quantified.

Taking a system-wide approach to control system management and developing baseline statistics for control system benchmarking allows ensures the

tion and connection processes, testing frequency, and testing procedures.

- Burner-management systems are a subset of safety-instrumented systems and should comply with ISA 84.01. In addition, they should also comply with prescriptive requirements from other standards bodies that are a function of the specific type of fire device upon which the system is installed.

- Compressor, turbine-monitoring systems are also a subset of safety instrumented systems and should comply with ISA 84.01. In addition, they should also comply with prescriptive requirements from other standards bodies that are a function of the specific type of compressor or turbine that they are monitoring. These standards include

### *Asset management, ASM*

The role of the operator is currently in a state of evolution partially brought on by the use of new technologies, downsizing of operating departments, and increased competitiveness in the industry. This evolution is significantly affecting the role and responsibilities of the "traditional" operator as well as the support elements required to make the operator successful in this environment.

To stay competitive and continue to advance abnormal situation management (ASM) practices in the future, companies must align their operations personnel to these necessary roles and responsibilities.

Any safety audit should consider the operating environment to assess whether a site has harnessed its respective technology appropriately in providing a truly effective operating environment. It should consider:

- Operator interface.
- Alarm system performance.
- Boundary and constraint management.
- Procedural automation.
- Asset effectiveness.

### *Operator interface*

Using generally accepted industry guidelines, one should examine the process-operating environment. For example, using the evaluation methods developed by the ASM consortium (see box on this page) in conjunction with basic human factor design principles, one might consider operator task analysis, ease of access to information, alarm handling, and navigation.

In addition, the display-based operator interface can be reviewed for consistency with known standards. The intent is to review the following, looking for areas for improvement:

- Display organization and navigation.
- Context-sensitive access to information.
- Integration of auxiliary information (operating procedures, operator help, etc.).

## ASM consortium

The abnormal situation management (ASM) consortium ([www.asmconsortium.com](http://www.asmconsortium.com)) was informally started in 1992 and formally chartered in 1994 to enable and empower operating teams to proactively manage their plants, maximize safety, and minimize environmental impacts while allowing the processes to be pushed to their optimal limits. Original ASM consortium members included Honeywell, Chevron Corp., Exxon Corp., Royal Dutch Shell PLC, BP PLC, Mobil Corp., Nova Chemicals Co., and Texaco Corp.

reliable operation of the control system. Establishing clear system performance criteria and an analysis of the effect of any changes that may have been made to the existing control system in the past is the key to success.

### *Auxiliary systems*

Other systems in the refinery may be left out of the standard safety audit. They are typically handled by other departments but play an integral part in a plant's safety. Consider, for example:

- Fire and gas systems are typically designed in accordance with NFPA 72, "National Fire Alarm Code." This guideline provides prescriptive requirements for equipment selection, installa-

tion and connection processes, testing frequency, and testing procedures.

- Simple manually activated protective functions are typically designed in accordance with the "emergency stop" provisions on the NFPA 79 standard. In addition, they are generally designed to operate as an "independent protection layer" in conformance with AIChE guidelines.

- Complex manually activated functions. Some manually activated functions are so complex and situation-specific that general industry guidance is either unavailable or unacceptable. In these cases special extra care should be taken in their design and testing.

- Display design standards.
- Utilization of operator tools.

## *Alarm system performance*

Alarm system programs are generally developed in accordance with EEMUA 191, “Alarm Systems – A Guide to Design, Management, and Procurement.” This guideline recommends that alarms be rationalized and prioritized to ensure that the quantity of alarms and their display is appropriate for operations staff.

Alarm equipment selection, testing, and maintenance are typically tied to the priority that has been assigned to the alarm. Unlike safety-instrumented systems, the alarm system standards have no predefined alarm priorities. They are typically assigned at the discretion of each site and are typically a function of the type of control system hardware used at the plant.

Development programs for alarm systems are typically based on judgment and the concept of an “independent protection layer” as defined in AIChE guidelines from the Center for Chemical Process Safety. Performance of an alarm that is critical to safety is typically designed so it can meet the criteria for an independent protection layer.

In addition to quantifying the frequency and priority of alarms, one should review the site’s overall alarm management strategy. Consideration must be given to current work practices relating to alarm system management:

- Existence and content of overarching alarm philosophy.
- Alarm annunciation and indication conventions.
- Situation-based alarm design.
- Automatic alarm cutout strategies.
- Alarm change management design.
- Use of alerts to notify the operator of prealarm anomalies.
- Alarm reporting standards and conventions.

## *Boundaries, constraints*

All of the considerations noted for alarms can be extended to operating envelopes or constraints. One should

consider whether work processes exist that are targeted at establishing operating limits for plant processes. This should be extended to include validation that operating targets are within specified limits, ensuring that the process is monitored and controlled to these targets, and reporting done in a consistent manner to promote continuous improvement.

Additionally, one should ensure that the operating envelope exercise is done in unison with alarm management efforts; these are two highly interrelated layers that are often considered independently.

## *Procedural automation*

Every day operations staff must execute common, repeatable tasks that often combine manual and semi-automated processes. When key processes require an operator to manually control or activate specific components, such as a shutdown and start-up, execution can be inconsistent.

When that happens—whether because of varying levels of operator expertise, less-than-explicit instructions, out-of-date or missing data or unregulated input—the consequences can range from lost time and revenue to unnecessary safety hazards. These consequences are likely to be repeated time and again.

Recent ASM consortium-sponsored studies indicate sites that believe their manual procedures are sufficient still may have unknown problems. Questions one should ask include:

- Are procedure-related incidents recorded and tracked properly?
- Is there a measurable improvement system for critical procedures?
- How are “golden” procedures measured and compared to non-golden procedures?
- Can a small change be measured for reliability and efficiency?
- Are these procedures executed the same across shifts and personnel?
- How does a known decrease in execution time reflect on production dollars?

The current operator procedures and workflow used on site should be considered. An evaluation of the procedure workflow, as well as an assessment of the availability of data and standard tools and capabilities aimed at improving workflows and procedures may help to answer these questions.

## *Asset effectiveness*

Directly related to the prevention of abnormal situations is the maintenance of a plant’s assets. According to the ASM consortium, at least one-third of abnormal situations occurring in a typical processing plant are due to equipment problems.

Because operators must ultimately deal with these failures when they occur and given the possibility of the operator incorrectly recognizing the problem, it is important to consider asset management as a layer of protection. Proper procedures and work practices in the area of asset management can prevent an operator from ever needing to deal with the issue in the first place.

For a particular asset, no matter how big or small, an increase in availability is directly related to reliability. Reliability is the probability of equipment or systems functioning without failure for a stated period of time.

The achievement of availability is supported by a range of frequently talked about operation-based initiatives, including reliability, asset management, and ASM—an intense focus on the root causes of unplanned shutdowns and the procedures and technical tools that can help operators deal with upsets when they occur or prevent them from happening in the first place.

## *Physical, system security*

Although perhaps not obvious in the context of a safety discussion, plant and process security is integral to ensuring plant safety. Not all upsets or incidents come from within.

An audit would be remiss if it did not consider the layers relating to plant and process security. An effective ap-

proach for protecting an industrial facility uses 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 of a plant.
- Identifying and controlling who enters and leaves the plant.
- Controlling access to restricted areas.
- Determining the location of people in the event of an emergency.
- Targeted and faster emergency response.
- Protecting process automation networks and systems from cyber threats.

### *Physical, electronic security*

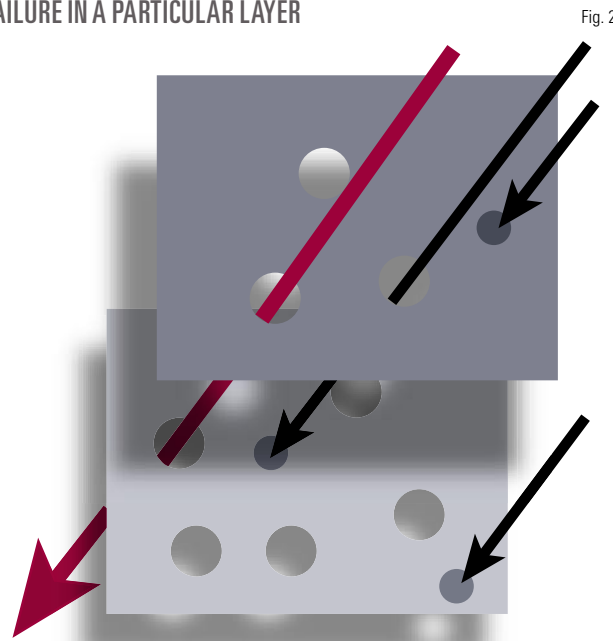
The physical perimeter is protected by those technologies that have more visible, tactile characteristics—including fences, barricades, guards, and other assets used to prevent entry by unauthorized personnel.

An electronic security layer uses technologies such as video cameras, access cards, and motion-detection equipment. State-of-the-art systems use wireless and microwave closed-circuit television 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

## FAILURE IN A PARTICULAR LAYER



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.

TV 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.

Furthermore, 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. A comprehensive cyber-security strategy must therefore 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.

### *Work practices, policies*

In “The Human Factor,” Kim Vicente points out the way humans and technology interact at the physical (ergonomic), psychological (individual), team, organization, and political levels. In the case of safety, the marrying of technology with humans is key to preventing serious if not fatal incidents.

One of the main barriers to adoption of a safe working environment occurs at the organizational-political level. There are many examples of instances of excellence at the physical, psychological, and team level. To solidify the future of safety at a plant, organization and political issues must be considered.

In order to complete a safety audit, one must examine the plant's leadership involvement in HSE self-assessment and audit processes, executive audits, recordable incident reviews, and risk assessment process.

## *Layers of protection*

In many discussions of hazard assessment, the layers-of-protection concept is described as multiple layers of Swiss cheese (Fig. 2). In this model, the process has multiple layers of protection and that protective systems have "holes" that represent failures of a particular layer.

The holes may represent errors or lapses of attentions or perhaps poor maintenance or design, and the size of the holes simply represent the fraction of time that the system fails due to component failures. The bigger the holes and the fewer the layers the better the chance of a failure passing through.

The intent of any methodology aimed at ensuring a holistic approach to safety is to reduce the size of holes in the layers, and to ensure that multiple layers of protection indeed do exist. ♦

## **The author**

Peter Jofriet (Peter.Jofriet@Honeywell.com) is the global business director of refining for Honeywell Process Solutions, Cincinnati. He joined Honeywell almost 5 years ago as an industry consultant, working in the areas of operator effectiveness, abnormal situation management, asset effectiveness, and mobile technologies. Jofriet has worked as a production supervisor, a control engineer, and a senior process engineer before joining Honeywell, working on supervisory control, advanced control, performance monitoring issues, and systems upgrades. He holds a masters in process control from Queen's University, Kingston, Ont., specializing in model-based fault diagnosis, expert systems, and neural networks.

