

A LAYERED APPROACH TO RISK

Peter Jofriet and Scott Hillman, Honeywell, explain why using layers of protection is the best way to ensure plant safety.

Safety means reducing risk, both the risk of incidents, faults and failures that cost money, and those that can cause injury to personnel, equipment and the environment. This goes far beyond simply installing failsafe controllers or a safety instrumented system. In fact, to mitigate the most serious risks of injury, as well as the disruption of production capability, it is important to consider safety from all aspects of a plant's operation.

Plant safety therefore includes areas such as operator training, constant monitoring of distress indicators, personnel tracking and mustering applications, and ongoing asset monitoring and maintenance to manage the health of assets.

CREATING LAYERS OF PROTECTION

The concept of 'layers of protection' is widely recognized by the process industries and 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, and plant emergency response systems). Some can deter incidents in the first place (e.g. plant security, constraint and boundary management, operator training and asset reliability management). Others can provide detection, alerting people to dangers and issuing associated guidance (e.g. operator alarms, early event detection and integrated operator procedures).

Layers can also be either automated, as in the case of emergency shutdown, or require human interaction, as process alarms do. Some layers offer easily quantifiable risk reduction benefits but require that all the risks be identified before the implementation; others are less tangible and offer softer benefits.

To maximize the effectiveness of a plant's efforts and to ensure you can answer the question, 'Am I safe enough?' a systematic approach to safety is required. Such an approach ensures that the layers of protection are properly designed with a strategy that makes use of integrated, multiple, independent yet interactive layers of protection.

A HOLISTIC APPROACH TO SAFETY

In this way plant safety measures are much the same as those used for driving. Safety equipment such as the air bag and the seat belt of a car are analogous to the fire and gas and other emergency response systems. These mitigate adverse affects of an incident in the case that it does occur, while the next layer of protection, the brake pedal and antilock brakes, can be seen as analogous to the safety shutdown system in the plant.

However, those systems are merely the worst case measures that come into play once an incident has begun; before the driver gets to the point of a collision there are several basic design features of the car to help prevent an incident occurring in the first place. Rear view mirrors and well placed

controls on the dashboard, for example, help to maximise visibility and provide the least amount of distraction.

However, probably the most important measure used to reduce the risk of accidents is education. After all, people will not be turned loose with a car before spending a significant amount of time learning how to be safe and responsible drivers.

Therefore, just as in the plant, driver safety is made up of standards and layers of protection. Safety does not consist of one or two tools, but rather is the result of the layered combination of numerous things: education, best practice, proper maintenance and, of course, hardware. Each is designed to protect against needing the next, but all of them aid in the prevention or mitigation of a potential incident.

THE RELATIONSHIP TO HUMAN ERROR

The Abnormal Situation Management Consortium(r) (ASM) met informally first in 1992 and formally chartered in 1994 to empower operating teams to proactively manage their plants, maximise safety and minimise environmental impact while allowing processes to be pushed to their optimal limits. Original members included Honeywell, Chevron, Exxon, Shell, BP, Mobil, Nova Chemicals and Texaco.

One of its first activities in the early 1990s was to create a concept team to review the commonality between five sites with respect to abnormal situations. This team addressed the concerns of limitations facing industrial plant operations during abnormal conditions. Its objective was to recommend changes in methodologies, practices, operations and technical solutions to achieve best practice. It was also asked to identify solutions in the form of prioritised products, applications and services that could be implemented over a three to five year period, with intermediate results as appropriate.

What follows is an excerpt from the concept team's report that brings to life the human factor in safety systems: 'The plant operations team is monitoring a petrochemical process that has been operating smoothly and without incident. Suddenly without warning, there is a serious upset. A flood of 60 high priority, emergency, and low priority alarms assaults the eyes and ears of the plant personnel. Within seconds, the operations team must prioritise the alarms and decide together how to stabilize the process and diagnose the cause of the upset. Operators work frantically together on a single console and co-ordinate their responses to try to stabilise the process. Supervisors, board operators, and field operators speak to each other as they try to isolate the problem and verify and adjust the state of the equipment. After a period of minutes the causal chain of events begins to unravel through a process of deduction and verification across plant units. After the problem has been isolated upstream, appropriate compensatory action is taken. As the process begins to return to normal operations, a 15 minute

segment of the workday has come to a close.'

According to the American Petroleum Institute and the American Chemistry Council, during the past 30 years, the 100 largest accidents in chemical and hydrocarbon processing facilities have severely injured or killed hundreds of people, contaminated the environment, and caused more than US\$ 8 billion in property damage losses.¹ The actual cost of these accidents was in fact much higher when taking into account the associated business interruption costs, cleanup costs, legal fees, fines, losses of market share, etc.

Unfortunately, studies also show that human error is a

significant factor in most of these accidents.

Studies done by the ASM Consortium have shown that 42% of abnormal situations or upsets that occur in modern day processing plants are due to people or their work context. Additionally, 36% of these result from equipment problems, and of these half are a direct result of operating the equipment or process unit outside the 'operating envelope'. To improve operational reliability and to avoid some of these incidents it is necessary to examine the work processes of the control room operator; what tools need to be provided so that they can be successful in their jobs, ensuring a safe and profitable production or operation?

ANATOMY OF A DISASTER

An important aspect of understanding the management of abnormal situations is the interrelationships among root causes and interventions by plant systems and plant personnel. Figure 1 illustrates the anatomy of a disaster.

A typical process plant operates in the green region labelled 'process control'. The job of the control system is to keep the process in this region of operation. However, due to outside forces or disturbances, a process occasionally deviates from normal operation into the 'yellow' or upset condition. If not mitigated, this disturbance or abnormal situation will then continue into the 'critical situation' zone. The dotted line in Figure 1 depicts an insidious problem; a problem or upset that develops slowly over time, potentially evolving into a catastrophic disaster.

Figure 2 illustrates the progression of an abnormal situation and the interaction with failures that need to occur to bring the situation back to normal. The difference in slope here from the dotted line in Figure 1 is evident. 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 different zones requires a different intervention, ranging from normal control action to mechanical shutdown by a safety instrumented shutdown (SIS) system. Each intervention is independent: the process system, the protective applications, shutdown system and the safety containment system are designed to safeguard the plant from catastrophic events. Moreover, the event sequence illustrates the role of plant personnel in intervening 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 minimise the impact of a disaster on the plant and surrounding community.

DEALING WITH DISASTER

'Operator action' refers to the activities of a typical operations crew comprising console operators, lead operators, supervisors and field operators.

This would also include coordination between the operations crews responsible for different areas within the plant and any technical support engineers. In most cases it is generally assumed that the console operator is the only one available to respond to abnormal situations due to the speed at which most abnormal situations evolve. In fact, if time permits, the technical support team can

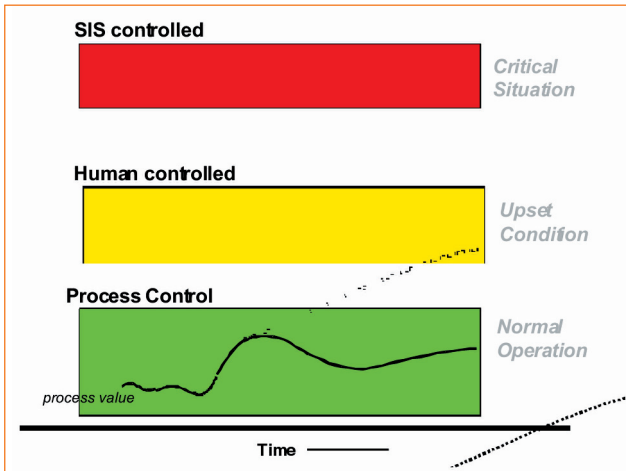


Figure 1. The anatomy of disaster.

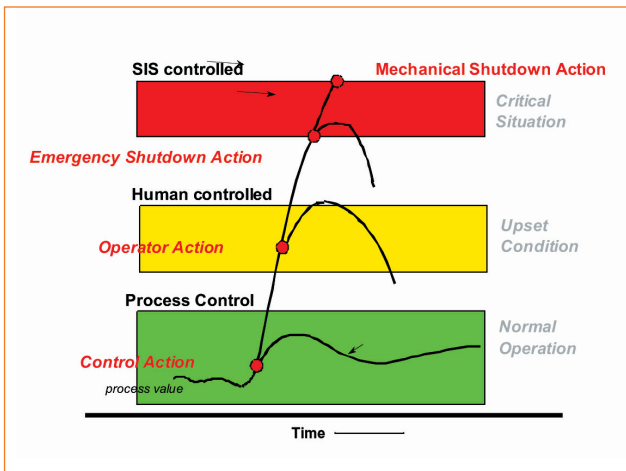


Figure 2. Intervention points.

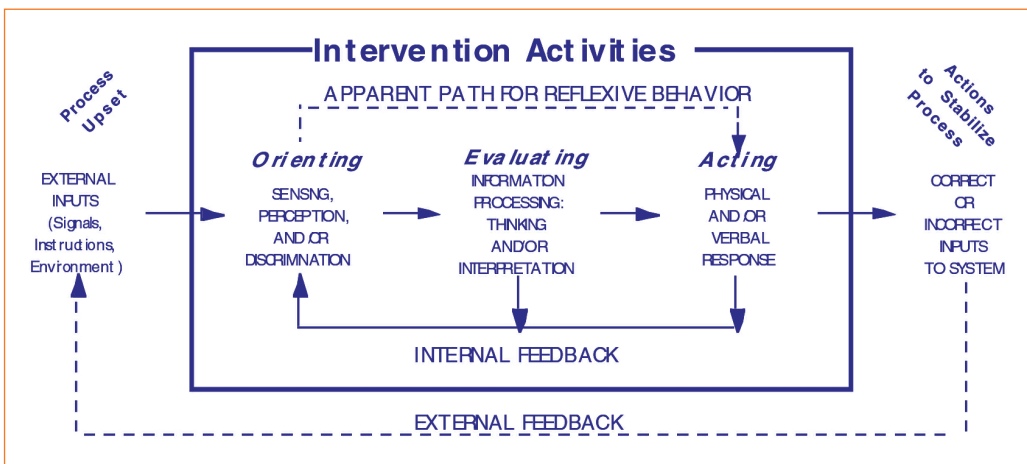


Figure 3. Cognitive behaviour underlying intervention activities.

sometimes provide additional intervention at the initial stages of an abnormal situation to prevent its escalation. Nevertheless, the ability to support the console operator in real time is paramount, and mitigation of process upsets is dependent on integration and timely communication throughout the information and communication systems.

A number of authors have developed models to describe the cognitive behaviour underlying intervention activities. Figure 3 (based on a model proposed by the Chemical Manufacturers Association) is a simple loop diagram that describes three stages of processing within the operations team. The framework in Figure 4, meanwhile, outlines distinct intervention activities that occur during an abnormal situation. The left side of the Figure represents the occurrence of an external event that initiates a process upset. The operations team and/or technical team, represented by the grey shaded box, then will act to stabilise the process.

The three stages of operations team processing are:

- Orienting: sensing, perceiving and/or discriminating.
- Evaluating: information processing (thinking and/or interpretation).
- Acting: physical and/or verbal response.

The first stage involves discerning an anomaly in the process. This can happen by a number of means. Typically, an alarm in the process control system, or an alarm or trip in the safety shutdown system may direct the operations team's attention to a specific point in the process. Alternatively, the operations team may be monitoring the process using schematics (with value readouts) or trends, and determine that an anomalous condition exists. Finally, an indicator, such as size of flame in the flare or sound of an emergency relief valve, may alert the plant personnel to a problem.

In the information processing stage, the operations and/or technical support team develops hypotheses regarding the cause of any anomalous operating conditions. However, as denoted by the dashed line labelled 'apparent path of reflexive behaviour', which goes directly from the first to the third stages of processing, an individual may be so well rehearsed for certain response conditions that it appears that this intermediate stage of processing is skipped.

Finally, the team must take some form of compensatory or corrective action. This might entail the use of the automated control system or the assistance of plant maintenance personnel. Not all action taken is corrective (e.g. re-establishing a stable process by manipulating process parameters). Sometimes the operations team may perform actions to test their hypothesis and determine if the supposed problem genuinely exists.

The iterative nature of active control (action, observe, action, observe) is represented by the internal feedback loop connecting the blocks at the bottom of the diagram. When operations and/or technical support are satisfied that the process has stabilised, the operator can resume supervisory control. However, additional analysis and evaluation may continue to try to restore the system to normal production levels and prevent future occurrences.

DESIGN FOR DISASTER

With a clear understanding of how abnormal situations develop and the tools available to help mitigate them, it is possible to

design for the inevitable. Figure 4 illustrates the various levels of protection available to mitigate an abnormal situation as the upset escalates beyond a preceding layer.

The intent of the asset monitoring layer is to provide an early warning of pending failures, before they become operational concerns. The alarm system is the operator's first warning that the control system cannot cope with a pending condition. When properly designed, it 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 come system interlocks, perhaps triggered by field switches or stored boundaries or constraints. Typically these interlocks are built into the control logic to prevent equipment damage or worse. Within this category of interlocks is a work process to establish limits and to set standard or automated procedures where prudent. In operations management, the critical, standard and target boundary of a system's variables or processes must be clearly understood and defined. This requires supporting information including the purpose of the measurement, P&ID 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 vari-

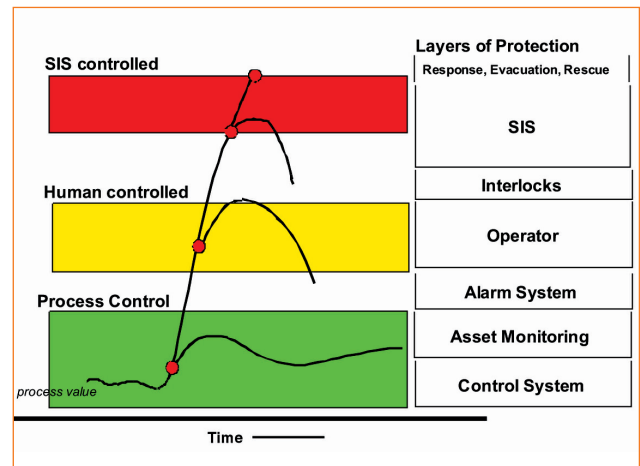


Figure 4. Layers of protection available to mitigate an abnormal situation.

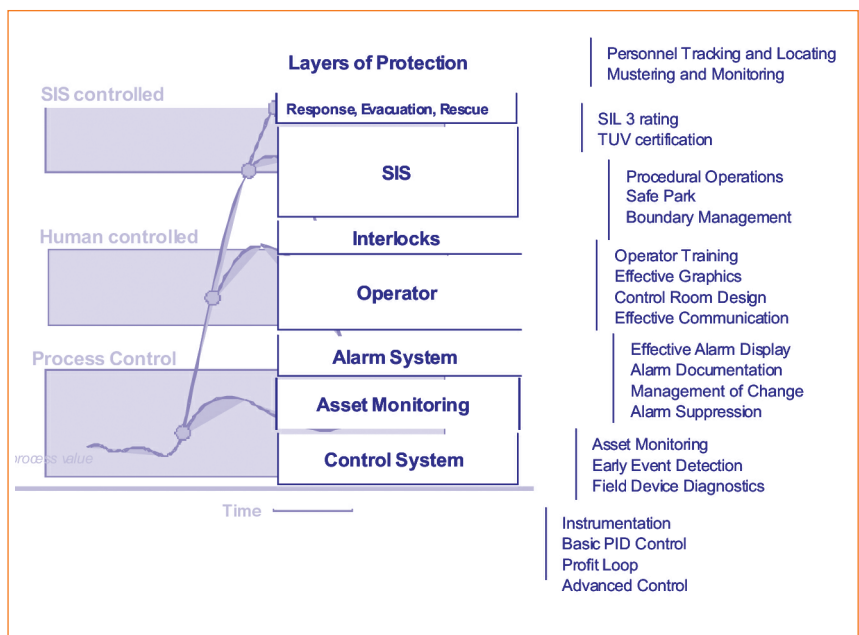


Figure 5. Components of the layers of protection.

able and boundary.

The final two layers play an integral part in the protection of life and plant assets. 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 needs to be considered comprises the applications that aid in tracking personnel and mustering those that are evacuated in the case of an emergency. Figure 5 details some of the applications associated with each of the layers. However, missing from this diagram is the implied layer that wraps around each layer and ensures the site is physically secure, as are the control system networks and the information and control that lies within in them.

DEFENCE IN DEPTH

In a recent technical symposium a large audience of automation professionals expressed clearly their concerns over security and safety with trends in industry pointing to a world

of increasing process and cyber complexity and diminishing institutional knowledge.

One element was clear from this debate and discussion: there is a need to better manage security and safety threats in a multi-layered approach of independent yet interrelated measures. Safety and security have to be built into all levels of the system. It requires a defence in depth approach that can be best visualised as the layers shown in this paper or as successive spheres of protection similar to Russian dolls, designed to protect employees, the plant and the surrounding community. In any case, the approach to plant safety requires protection that deters, prevents, detects and mitigates potential threats.

REFERENCES

1. A Manager's Guide to Reducing Human Errors, API Publication 770, March 2001. ■