September 2009

InTech

ISA

Automation Founders Circle Awards

Flow/Level special section

FDT + EDDL = FDI

ISA EXPO preview

Operators on alert

Alarm standards, protection layers, HMI keys to keep plants safe

Setting the Standard for Automation™

www.isa.org/intech

Operators on alert

Operator response, alarm standards, protection layers keys to safe plants

By David Hatch and Todd Stauffer

FAST FORWARD

- Help operators detect, diagnose, and respond on time.
- Use standards for good design, operation of process alarm systems.
- Implement multiple layers of protection to prevent incidents.

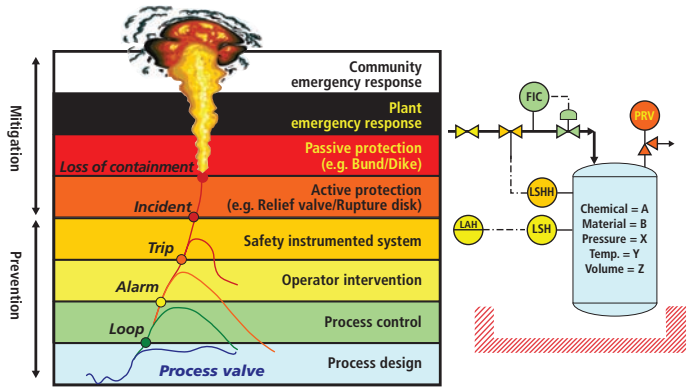
As plants run closer to their performance limits with fewer operators and support staff, alarm management is becoming paramount to maintaining plant safety. The key to maximizing the safety protection the operator provides is creating an environment where they are able to detect, diagnose, and respond to alarms properly and on time. One way to do this is adopt the requirements and recommendations of the standard on alarm management (ANSI\ISA-18.2 standard, *Management of Alarm Systems for the Process Industries*) and take a coordinated approach to alarm management and safety instrumented system (SIS) design. The ANSI\ISA-18.2 standard offers guidance on how alarm management can help a plant operate more safely. The standard can also bring together the disciplines of alarm management and safety-system design, which must work more closely to prevent future accidents.

First layer of protection

The operator's response to alarms is crucial in preventing a process upset from escalating into a more serious event. Multiple layers of protection can prevent an incident from occurring and mitigate its impact if it does occur. Operator intervention is one of the first layers of protection. Next is the SIS, whose job is to drive the process to a safe state, as needed, to protect people, the environment, and equipment. When a safety system trips, it typically results in lost production, which can be very significant—for an oil refinery, it can easily exceed $1 million per hour.

Risk reduction

According to the IEC 61511/ISA 84 process safety standards, you must reduce process risk to a tolerable level as set by the process owner. To do this, use multiple layers of protection, including the basic process control system, alarms, operator intervention, mechanical relief systems, and if necessary a SIS. The more risk the alarm system and operator can reduce, the less risk reduction or safety integrity level (SIL) the SIS must provide. The higher the SIL level, the more complicated and expensive the SIS will be. Also, a higher SIL will require more frequent proof testing, which adds cost and can be burdensome in plants. Unfortunately, human performance factors provide constraints on the level of risk reduction an operator can actually provide. Getting the most from the operator reduces the demands on the SIS, which in turn reduces its chance of failure.



Layers of protection and impact on process

The reliability of the alarm system and operator are an important consideration when performing a layer of protection analysis (LOPA), which is one of several methods for calculating the required SIL target. In a LOPA, you can calculate the frequency of a potentially dangerous event by multiplying the probability of failure on demand (PFD) of each individual layer of protection times the frequency of the initiating event.

Reliable operator

The example LOPA calculation assumes each protection layer, including the operator, is specific, auditable, independent, and dependable. The calculation uses a 20% chance the operator will fail to respond correctly and in time to prevent the outcome (PFD = 0.2). Assuming an 80% success rate might seem conservative, but studies have shown human error is one of the leading causes of industrial accidents.

On the other hand, an 80% success rate might be generous. Consider safety-critical alarms are most likely to occur during major plant upsets. Throw in operator fatigue, lack of proper training, increasing operator workload, physical condition (age, amount of rest), along with alarm overload, and you can see the challenge to improving the operator's response.

Just a matter of time

So how can we improve the operator's performance to keep our plants safer? One way is to think about what constitutes a successful operator response. As ANSI\ISA-18.2 describes, the operator must be able to detect, diagnose, and respond within the appropriate timeframe, sometimes called the process safety time, or else the upset could escalate to cause a trip or an accident.

Consider operator response time up-front during design. When you create a situation in which an operator has only a few minutes to detect, diagnose, and respond, you increase the probability for failure. This means the operator cannot be a significant safety layer. One company has set a threshold requirement of 10 minutes, meaning any alarm that has a process safety time of less than 10 minutes cannot be claimed as a layer of protection (PFD = 1.0).

Life cycle approach

The ANSI 61511/ISA-84 standard on process safety and the ISA-18.2 standard on alarm management advocate the use of a life cycle approach. Two life cycles are similar and can connect during several phases. Results from the safety hazard and risk assessment are an input to alarm management's identification phase. You should assign alarms you are relying on as a safety protection layer as a high priority during rationalization.

A key deliverable is to create an alarm philosophy document that defines how a company or site will address alarm management throughout all phases of the life cycle. It should contain information such as the criteria for classifying and prioritizing alarms (safety-related alarms are classified as highly managed alarms), what colors to use to indicate an alarm in the HMI, and how to manage changes to the configuration. It should also establish key performance benchmarks (such as the acceptable alarm load for the operator).

Initiating event	Protection layer #1	Protection layer #2	Protection layer #3	Protection layer #4		Outcome
Loss of cooling water	Process design	Operator response (to alarm)	Pressure relief valve	No ignition		Fire
				0.3		2.10E-05
			0.07			Fire
		0.2				
	0.01					
0.5/yr						
						No event

Example layer of protection analysis (LOPA) calculation

Easy alarm detection

Design HMI to make the operator aware of a situation. The operator's performance is directly linked to the proper use of color, text, and patterns within the HMI, which should be configured to uniquely indicate the state of the alarm (normal, unacknowledged, acknowledged, suppressed). Since 8-12% of the male population is color-blind, it is important to consider what colors to use. Ideally colors used for alarm indication should be reserved for alarming only and should be different depending on priority.

Minimize operator's number of alarms. Alarm overload is a key reason operators miss alarms. An operator should be hit with no more than one to two alarms every 10 minutes during steady-state operation. In many control rooms, operators are hit with one alarm every minute, which is considered unmanageable.

Make sure operators can differentiate high priority alarms from other alarms. ANSI\ISA-18.2 recommends using three to four different priorities, where no more than 5% of alarms are configured as high priority. Set priority based on the potential consequences and on the time available to respond.

Eliminate nuisance alarms. The presence of standing alarms (lasting more than 24 hours) and chattering alarms (points that go needlessly in and out of alarm on a frequent basis) can obscure the operator's view and make it more difficult for him to detect a new alarm. Poor configuration practices are one of the leading causes of nuisance alarms. The proper use of alarm deadbands and on/off delays can go a long way to eliminating them. An ASM study found the use of on/off delays in combination with other configuration changes was able to reduce the 10-minute alarm rate by 45-90%.

Correct diagnosis

Make information available on cause and corrective action. Ideally, you should make available the cause of the alarm, corrective action, consequence, time to respond, and safety in real time and in the proper context.

Suppress unimportant alarms during a flood. Plant upsets, which can generate tens to hundreds of alarms, are one of the most challenging times for the operator. Advanced alarming techniques, such as state-based alarming, can temporarily suppress alarms when they are not meaningful. When a distillation column crashes, it is best to present only those few alarms that affect the diagnosis and response, rather than all temperature and pressure alarms that occur.

Shelving helps the operator stay focused. Alarm shelving allows an operator to temporarily suppress an insignificant alarm, removing it from view. It is a great tool for improving response during a process upset. The alarm will come back later (after 30 minutes for instance), so it can be addressed when things have calmed down in the control room. It is important to provide controls on who can shelve an alarm and which alarms can be shelved.

Correct response

Practice makes perfect, so it is important to train operators to make sure they are comfortable with the system, and that they trust it to help them do their job. The last thing you want is the operator abandoning the control system during an upset. Training the operator as part of a process simulation can create a drilled response in which corrective action is so well reinforced it is automatic.

Provide alarm response procedures; specifically, written alarm response procedures should include potential causes and consequences of the alarm, recommended corrective action, alarm limit, and allowable response time (information fleshed out during rationalization and hazard and risk assessment).

Maintenance, change control

Review and learn which alarms are out of service. Alarms will periodically go out of service for maintenance, repair, replacement, or testing. It is important to document why an alarm was removed from service, the operation of interim alarms, special handling procedures, as well as testing required prior to returning to service. For safety reasons, the system should be able to produce a list of which alarms are currently out of service. This serves as a reminder of what alarms are suppressed. Then you can review the list before putting a piece of equipment back into operation to ensure all critical alarms are functional.

Manage and control configuration changes; even the most well-designed alarm system can run into problems if there is poor control over who can make changes. Implement a management-of-change procedure to ensure review and approval of modifications (such as changing an alarm limit, disabling an alarm, or adjusting its priority) prior to implementation. Do not make modifications without proper analysis and justification, particularly if the alarm is a safety layer of protection.

ABOUT THE AUTHORS

David Hatch (david.hatch@exida.com) is a certified functional safety engineer (CFSE) with exida, a certification and consulting firm specializing in safety critical/high-availability automation systems, control system security, and alarm management. Hatch is also a member of the ISA18 committee and EEMUA 191 working group. **Todd Stauffer** (tstauffer@exida.com) is director of alarm management services for exida, and a member of ISA18.

View the online version at www.isa.org/intech/20090901.

RESOURCES

Ultimate conductor
www.isa.org/InTech/20090403

Fault tolerance and disaster recovery
www.isa.org/link/FaultT

Clearly Superior
www.isa.org/InTech/20090201