SPECIFYING AND CONFIGURING ALARMS IS A significant activity associated with most automation systems. A number of valuable resource documents are available to help define individual alarm requirements. For most industries, these will include safety and environmental regulations. For some industries (e.g., pharmaceutical, biotech), additional current good manufacturing practices (cGMP) regulatory requirements exist that help ensure good product quality. Other information sources may be available to help suggest alarms in other categories (e.g., product yield, equipment operational limits).

The use of alarm systems is not generally a hard regulatory requirement, as specific reference to alarms appears infrequently in EPA, OSHA and cGMP documents. However, when alarm systems are used to identify when processes may be exceeding regulatory compliance limits, then they are expected to be configured and managed appropriately. Most industrial plants struggle with maintaining effective alarm systems that are free of nuisance alarms. Causes include:

- Continuing increases in the information available to be alarmed. This is due to the increase in: the level of plant automation; regulatory requirements; and available information from the plant floor via smart instrumentation and networks to communicate this information (e.g., fieldbus).
- Insufficient attention to alarm functions when process control application software is specified, created or changed.
- Limitations in off-the-shelf vendor functionality to manage alarms, such as the lack of ability to link alarm attributes to individual process steps and phases, and providing advice to operators on what actions to take. Other desired functionality includes generating more intelligent alarms by linking to multiple distributed sources of information via user configured if-then-else logic.

With some exceptions, alarm requirements for automation systems have not historically been considered in detail during early phases of projects. Rather, alarms are often addressed near the end of projects when alarm system functionality is constrained to whatever can easily be configured into the system vendor’s standard offerings. Further, alarm limits are often determined without considering measurement uncertainty. This overall approach has led to issues in formal system testing (due to lack of specifications to test alarms against) and excessive nuisance alarms, which can contribute to safety and environmental incidents, product quality deviations and productivity losses. Other concerns that may arise include:

- Compliance issues, such as electronic records
- Statistically significant probability of real alarm conditions existing, even though no alarm is generated
- Ineffective alarm record sorting functionality; users need more than a cryptic listing of alarm records by calendar time
- Limited ability to link to external communication devices, such as pagers, e-mail, etc.

The process alarm lifecycle

Figure 1 shows a graphical interpretation of the lifecycle of process alarms. It indicates that information needed to manage process alarms comes from various sources. Also, several different alarm categories should be defined, such as personnel safety, environmental, equipment protection, product quality, process yield and others. Categories are needed as they are usually managed differently. They may be displayed in different colors, be prioritized differently in
case multiple alarms occur simultaneously, and generate different kinds of reports and follow-up actions. For example, product quality alarms may trigger a formal process deviation investigation and may be useful in helping plant personnel decide whether or not to accept a completed lot or to “forward process” material in the middle of a manufacturing process sequence of operations.

Product quality and certain other measured variables will usually have an “acceptable range” attribute provided by process development personnel. In highly regulated industries, this is often known as the proven acceptable range (PAR), which is defined as a range of values for a critical process parameter or criteria for forward processing documented as having no adverse effect on the safety, identity, strength, purity or quality of process intermediates or products. These ranges may be supported by lab or plant data, including statistically relevant data from past deviation investigations. These ranges represent the documented envelope of acceptable performance.

While alarm information sources (e.g., PARs) may suggest a starting point in setting alarm limits, it is appropriate to consider, and sometimes required, to adjust these limits to incorporate measurement uncertainty. This requires knowledge of the accuracy of measurement systems which, in turn, is tied to calibration standards and procedures and to preventive maintenance (PM) frequency.

It is important to document the rationale for whatever final alarm limits are decided upon (1). There will be times during the life of the process or computer system when changes to alarm attributes are considered. At such times, it is important to know the rationale that went into specifying the original alarm parameters. In addition, in investigating possible product quality deviations prompted by alarm records, that rationale for the alarm limits should be available.

In parallel with the determination of alarm categories and limits, the overall specification of the alarm system should be determined and documented in the computer system functional requirements. Specification and design might include such aspects as:

- alarm categories
- color coding
- alarm threshold level definitions (e.g., warning and critical alarm levels)
- operator help screens linked to alarm displays
- consequences of alarm acknowledgement (e.g., change in color, record generation)
- alarm and alarm acknowledge logging requirements
- alarm output devices to be used (e.g., horns, pagers)
- how start-up, shutdown, or other batch aspects of processing will be handled with respect to alarms.

It is important for the system to be able to change alarm parameters as a function of the step or phase of the process.

Any need to produce formal alarm reports should be identified. For example, product quality alarm reports can be generated and included as part of official manufacturing batch records.
Changes to alarm configuration (or functionality) within a process control system will sometimes be required. Such changes should be conducted in accordance with local “change control” procedures. Review of alarm records might also be included in periodic system reviews as a good business practice.

Frequently, there is information that is useful for automation systems to communicate to system users (e.g., the completion of an operation) that does not represent an abnormal situation and does not require any response by the user. Computer-generated messages can be used for this purpose, but these should not be labeled as alarms. Every alarm event should represent an abnormal condition and require a response (2). Otherwise, the event should not be configured as an alarm.

**Alarm levels**

Most vendor systems provide for multiple levels of alarms, although the minimum needed is usually two levels — warning and critical. Process plants are typically subject to disturbances that shift the operation away from normal operating conditions. Usually, computer functions, such as PID control loops, will automatically bring the plant back under control. To assist operators in identifying transitions or trends to abnormal states, it is often useful to create “warning” alarms to provide an opportunity to take action to avoid a process excursion or deviation associated with product quality, safety, or environmental limits. If a warning condition is not addressed and corrected, then the process (operation) may approach a critical state that can affect product quality, endanger the safety of plant equipment and/or personnel, or impact the environment.

However, alarm management is really more complicated than this, as measurement uncertainty must sometimes be incorporated, especially for product quality parameters in certain industries. Figure 2 shows a more realistic view of alarms, using a computer-controlled product quality variable as an example. Note that the critical alarm limits are set inside the values associated with the PAR for critical parameters. This is because process measurements are associated with a certain amount of uncertainty (e.g., a flow measurement accuracy might be stated as the measurement ±1% of span). If alarms are set at PAR values, there could be a significant probability that a measured value might fall within the PAR range, although the actual value is outside of this range. This is sometimes referred to as a “false acceptance.”

By using information from vendors and statistical distribution theory, a value is determined for adjusting the alarm limits — a process called guard banding. In essence, this provides statistical confidence that a real alarm is not ignored.Refs. 3 and 4 (from the nuclear industry) provide some specific guidance on how to determine overall measurement uncertainty for many commonly occurring process measurements.

**Regulatory requirements — Environmental**

There are many requirements, originating with federal, state and/or local governments, regarding environmental emissions of gas, liquid and solid compounds. These regulations may apply to processes that:

- emit chemicals directly to the atmosphere or through a process or plant air pollution control device
- discharge liquids to a site sewer system that leads to a publicly owned treatment plant
- discharge liquids to a site treatment plant and then be discharged off site
- collects liquid wastes in a tank or other equipment prior to discharge or recovery/reuse
- relies on any material containment control devices (e.g., sumps, check valves, vents, rupture disks).

These situations may be linked with, for example, requirements to limit discharges with respect to pH, concentrations of organic solvents, metals, halogens, other listed hazardous or toxic compounds, and pharmaceutically active compounds.

The degree to which various government regulations might impact a process’ alarm strategy is a function of a plant’s configuration and management approach. For instance, a plant may use several dedicated process-specific air-pollution control devices, such as vent condensers,
Alarm Management

**HOW CAN AUTOMATION VENDORS HELP?**

A key to more effective alarm systems is to encourage automation vendors to add more alarm functionality to their systems*. For process control systems, it is desirable to:

- structure alarms such that alarm attributes (status, limits, time duration, priority, etc.) can be configured by customers as a function of the process step/phase. This will greatly help in reducing nuisance alarms.
- structure alarm records to include, in addition to a time stamp, other labels such as tank number, lot number, alarm priority and alarm category. This will greatly facilitate alarm record sorting and analysis in the alarm logger or process data historian.
- present alarms using different colors and flashing attributes to help operators distinguish alarm categories and state of acknowledgement.
- generate alarm-acknowledge records to be sent to the alarm logger or process data historian for at least some categories of alarms.
- provide special windows or help screens linked to individual alarms to enable customers to provide more online information about the alarm, its possible root causes and expected actions for the operators.
- provide an environment (e.g., if-then-else rules) to permit customers to create alarms using multiple sources of information (e.g., multiple process measurements) available in the control system. This will permit more meaningful (intelligent) alarms vs. the default comparison of a single measurement against its set-point (7, 8).
- provide audit trail functionality such that any online changes to the system automatically generates records as to the change, time and person involved.

For alarm loggers/data historians, it is beneficial to:

- provide data-record sorting and query utilities.

Users need to efficiently sort records and generate listings as a function of any alarm tag attribute (e.g., by lot number, alarm priority, category, etc.). This includes the ability to sort by alarm frequency and generate Pareto charts. One of the keys to reducing nuisance alarms is knowing how frequently specific alarms are occurring.

- provide means to create relative time stamps (vs. calendar time stamps). Alarms are often easier to interpret if their time stamp is relative to some benchmark, such as the beginning of the lot, rather than calendar time.

*Some vendors already provide a few of these functionalities.

or it may have a “one stack” approach, collecting air emissions from several processes and routing them to a central or common control device that relieves individual processes from many compliance-monitoring requirements.

Most companies utilize alarm systems to help assure compliance with the many complex environmental requirements. These include not only critical alarms that indicate a threshold has been passed, but also warning alarms that allow sufficient time for action to attempt prevention of a reportable incident.

Alarms are typically used in several ways regarding environmental emissions. They alert personnel that:

- a warning level exists of a control device parameter, or concentration or total weight of chemical emission; this will alert personnel that a permitted operational limit may be exceeded if action is not taken
- a critical level exists of a control device parameter, or concentration or total weight of chemical emission; this event may, in turn, require a process shutdown or generation of a report to an environmental agency
- equipment is not operating properly (either a control device or an analytical instrument)
- an analytical instrument has exceeded its “drift” specification (Note: EPA has published “drift” standards for commonly used analytical devices).

Alarms that inform personnel of equipment breakdowns should also be included to satisfy other aspects of environmental requirements. For example, if a control system’s critical components break down (e.g., a valve fails to close properly, sample pump fails, LEL analyzer signal is lost, etc.), an alarm should be activated to alert operational personnel. This alarm would trigger the implementation of a site plan calling for appropriate action (e.g., the orderly shutdown of the manufacturing process).

There are a considerable number of government environmental requirements that, while not directly specifying alarm expectations, could drive the need for an alarm strategy in a process control design. Some examples are:

- Maximum Achievable Control Technology (MACT) standards, Prevention of Significant Deterioration, Title III, Title V, Title VI, state Dept. of Environmental Management, Environmental Quality Board (for Puerto Rico), etc.

Regarding liquid emissions, there are U.S. federal requirements (40 CFR 261.20 to 261.24), and state release reporting requirements. These regulations pertain to both routine discharges as well as accidental discharges. They concern properties of liquid discharges, such as certain metal content (e.g., copper and chromium), biological and chemical oxygen demand, pH and suspended solids.

Companies often employ specialists to work with government agencies in the development and approval of an environ-
mental permit or license document. The site permit document is generally the primary source of environmental information needed by process engineers and automation groups in specifying and implementing alarms. It is possible that there may be more than one environmental permit per site (i.e., separate ones covering air, liquid and solid emissions/wastes). Also, there may be additional environmental requirements not captured by the permits (e.g., a company may impose tighter limits that those required by the government).

**Regulatory requirements — Safety**

A practical necessity of process safety management requires that alarms be thoroughly designed to alert operators in a timely fashion and/or automatically shutdown processes within safety constraints when needed. OSHA established, in 29 CFR 1910.119 Process Safety Management (PSM) of Highly Hazardous Chemicals, that information or procedures pertaining to the hazards of the highly hazardous chemicals in the process must contain:

- safe upper and lower limits for such items as temperatures, pressure, flows or compositions
- an evaluation of the consequences of deviations, including those affecting the safety and health of employees
- a qualitative evaluation of a range of the possible safety and health effects of failure of controls on employees in the workplace.

OSHA established in 29 CFR 1910.119 (echoed by EPA in EPA 112(r) 40CFR 68 Risk Management Plan – Prevention Program), that for covered chemical processes (an area or location where a company is using either a regulated substance, as defined by the EPA, or a highly hazardous chemical, as defined by OSHA, above threshold quantities as listed in the two regulations, EPA 112(r) and OSHA 1910.119):

- Process Hazard Analysis shall address: ...Engineering Controls...including...control instrumentation with alarms...— 29 CFR 1910.119 (e) (3) (iii) and 40 CFR 68.67 (c) (3)
- A mechanical integrity program is to be established for Controls (including monitoring devices, sensors, alarms and interlocks) — 29 CFR 1910.119 (j)(1) (v) and 40 CFR 68.73 (a) (5).

In order to address these requirements, a thorough and well-designed alarm and operator response strategy, including operating and maintenance procedures containing the required information, is necessary. An effective method to meet regulated safety requirements is as follows:

**Step 1.** Identify the PSM-covered processes.

**Step 2.** Establish safe operating limits during a process hazards review (or equivalent).

**Step 3.** Prioritize safety system alarms in accordance to their mission (e.g., prevention, emergency response).

**Step 4.** For alarms associated with fully automated safety systems that can be defined as safety instrumented systems, refer to ISA-S84.01-1966, “Application of Safety Instrumented Systems in Process Industries,” for design, installation, commissioning, pre-startup, acceptance testing, and operational and maintenance criteria.

**Step 5.** Incorporate safety systems and their associated alarms into the qualification and commissioning plan.

**Step 6.** Confirm that safety systems (and their alarms) are operational during pre-startup safety review.

**Step 7.** Incorporate information on safety systems (and alarms) into operating procedures and training programs.

**Step 8.** Safety system equipment lists should be forwarded to the applicable maintenance group for inclusion in the site’s preventive maintenance/mechanical integrity program.

**Regulatory requirements — Product quality**

Some industries can expect the FDA, as well as non-U.S. agency, regulatory inspectors to review product-quality-related alarms during cGMP audits of processes using automated control systems. Inspection guides include the FDA’s “Guide to Inspection of Computerized Systems in Drug Processing” (5), which notes, for example, its expectation that responses to alarms be documented and that alarm activations be logged. Further insight as to FDA expectations are obtained by reading cGMPs and FDA public record audit reports. Examples include:

- product quality related alarm events should be retained as permanent records
- certain critical alarms need to be investigated
- need for data to support certain alarm attributes
- need to ensure that certain critical alarms have taken “margin of error” into consideration; this in turn indicates consideration of the “entire measurement signal path”
- need to validate systems that generate alarms and store alarm records
- need to use change control when editing alarms
- documented procedures regarding review, approval and maintenance of records.

In attempting to meet regulatory expectations, which are often also best practices, evolving industry practices include:

- Alarm system requirements (e.g., tagging, sorting, categorization, prioritization, paging, color coding, acknowledging, historizing, use of time delays, etc.) should be included in the computer system “functional requirements” (i.e., system specifications) document. By definition, such requirements will then be addressed in “system design” and in “system testing.” This is in keeping with the computer system validation traceability matrix principles.
- Alarm limits for product quality parameters should consider measurement uncertainty. More specifically,
Alarm Management

when manufacturing processes are developed, companies are required to identify “critical process parameters,” which are those parameters that could affect some aspect of product quality. It is also required that a PAR be established for each of these parameters. However, it is often not acceptable to set alarm limits at the PAR limits, since measurement uncertainty exists.

- Alarms and, in some cases, alarm-acknowledge events, for product quality parameters that are managed by automation systems must generally comply with 21 CFR Part 11 (6), which describes the requirements for electronic records and electronic signatures. Expectations include the need for unique user passwords and audit trails.
- Primary alarm output and historian systems should be validated. This may influence whether or not to use external paging and e-mail technologies.
- Certain computer-system-validation maintenance activities can also prompt review of process alarms. These can include formal change control when application software is modified.

Other best practice considerations

Several additional alarm management considerations have evolved within industry, some of which are summarized as follows.

Alarm characteristics. For safety and other highly critical alarms, alarm generation should occur in the computer system as close as practically possible to the process (i.e., PC, PLC, DCS or hardwired directly from the sensor), i.e., the generation of critical safety alarms should not depend on multiple computers and computer interfaces being up and running.

E-mail and pager annunciation. If e-mail and/or paging systems are used to communicate alarms, users may need to establish that such systems are validated. This may be difficult to do for external providers of paging systems or for software systems such as Lotus Notes.

Alarm logging/recording. Critical alarms in regulated alarm categories (e.g., product quality, environmental) should be logged. However, logging all alarms is a good business practice. It facilitates the root cause analysis of problems and is of value in the analysis of alarm information (e.g., for determination and remediation of nuisance alarms).

In logging critical process measurements and alarms, the user area should rationalize and document any adjustments that occur to the data as it makes its way from the measurement sensor to the historian. Some factors that can influence the final recorded value include: digital filtering of the raw signal in the sensor and/or process control computer; data sampling frequency; truncation or rounding of numbers; and data compression algorithms.

Literature Cited


JOSEPH S. ALFORD, PhD, P.E., is an ISA Fellow and an engineering advisor in the Engineering Technology Center at Eli Lilly and Co. (E-mail: Alford_Joseph_S@Lilly.com; Phone: (317) 276-7653). He is responsible for coordinating and promoting alarm management governance and best practices at Eli Lilly and is a member of ISA’s Alarm Management SP 18 Standard Committee. He has spent much of his 33-yr career in automating fermentation processes and has over 20 publications in this area, including ones on state-of-the-art alarm management. Alford received his BS from Purdue University and MS and PhD from the Univ. of Cincinnati, all in chemical engineering.

JOHN KINDERVATER is an environmental consultant with Eli Lilly and Co. (E-mail: john.k@lilly.com; Phone: (317) 276-6330). He is currently working on developing and integrating environmental, health and safety improvement strategies into Lilly’s new process development methodology. Prior to joining Lilly’s Corporate Environmental Affairs staff, John led the group responsible for environmental improvement and compliance programs at Lilly’s bulk pharmaceutical manufacturing plant in Clinton, IN. Kindervater is a chemist with a MS degree in analytical chemistry from the Univ. of Maryland.

ROBERT STANKOVICH is a process safety engineer at Eli Lilly and Co. (E-mail: bprosafety@Lilly.com; Phone: (317) 433-0793). His primary emphasis is process safety management (PSM). He is also the author of several papers and coauthor of several books in PSM. Stankovich holds a BS from McMaster Univ. of Hamilton, Ontario, Canada in chemical engineering and management. He is a registered professional engineer in Ontario. He is also a certified safety professional in the U.S. and a registered safety professional in Canada.

Acknowledgements

The authors are indebted to the following Eli Lilly and Co. personnel who served as consultants in the development of this paper — Rick Lambert, William Marshall, Lance McElhaney, Ben Paterson and Rad Scott.