A Path Forward for DCS Alarm Management

Pierre Grosdidier, Ph.D., P.E.
Patrick Connor, P.E.
Bill Hollifield
Samir Kulkarni

Plant Automation Services, Inc.
16055 Space Center Boulevard, Suite 600
Houston, Texas 77062
U.S.A.

pgrosdidier@pas.com

Published in Hydrocarbon Processing, November 2003
Follow these guidelines to reduce operator overload and improve plant safety

Despite the recent industry focus on higher-level solutions, such as integration with supply chains and the deployment of ERP systems, substantive technical challenges still abound in the control room. One such challenge, distributed control system (DCS) alarm management, bears considerably on plant safety and yet often fails to make the shortlist during project funding cycles. A familiar complaint from operation superintendents is that they know that there is a problem, as does the entire control room staff, but they struggle to convince senior plant management of its seriousness and of the urgency for a remedy. The reasons, importance, and solutions for the problem of alarm management are the subjects of this article.

INTRODUCTION

A DCS alarm is a displayed message usually coupled with an audible horn that is automatically generated whenever a pre-defined condition is detected, such as a faulty instrument or an abnormally high or low measurement. The purpose of the alarm is to draw the operator’s attention so mitigating actions can be taken. Once reserved for exceptional situations in the age of panel-mounted instrumentation, alarms can be regarded as the overlooked byproduct of the modern DCS. They are free, in the sense that they cost virtually nothing to configure on an ad hoc basis, and as with any free resource, they are misused and overused.

Alarm configuration is determined during the deployment of the DCS, at a time when there are far more pressing issues to address than the minutia of selecting alarm trip values for the thousands of instruments being linked to the DCS. In many instances, even were time not limiting, the technical staff deploying the DCS simply may not know how to properly configure the alarms. As will be discussed later, alarm configuration requires a concerted team effort based on operating history and an intimate knowledge of how each piece of equipment behaves. Both of these requirements are in short supply with grass-root plants, or sometimes even when a modern DCS replaces aging analog instrumentation. The result is that alarms trip points are initially configured “in bulk”
with little attention given to practical meaning and implications. Other alarms are then added as needs arise, with little or no guidance from a consistent alarm philosophy.

The difficulties begin to materialize with the start of routine plant operations. Alarm messages begin to scroll and can overwhelm or “flood” the operators. Guidelines established by the Engineering Equipment and Materials Users Association\(^3\) (EEMUA) recommend that 150 alarms per day (one every ten minutes) presented to an operator may be considered “very likely to be acceptable,” meaning that the operator can meaningfully acknowledge, understand and respond to such a stream of alarms. Under the same guidelines, an alarm every five minutes (300 per day) is still considered “manageable.” In practice, one frequently encounters alarm rates substantially in excess of these guidelines. Figure 1 shows the daily alarm rate for an operator’s station in a European refinery for a continuous 18-day period, with a peak of 26,650 alarms per day and an average of 14,250 alarms per day, all alarms considered. Statistics like these are by no means unusual.

![Figure 1. Alarm count from an 18 day log](image)

---

\(^3\) EEMUA (Engineering Equipment and Materials Users Association) guidelines.
in facilities where proper attention has not been given to alarm management, and the authors of this paper have measured daily alarm rates in the six figure category. Needless to say, such messaging rates are unmanageable and render the alarming process useless to the operator. Thus, a paradox: alarms that are meant to assist operators in running the plant materialize as a distraction, if not an impediment to their end.

Many operators resolve their alarm crisis by suppressing alarms, either from appearing on the screens or in the history journals, or both. Such a practice is tantamount to sweeping alarms under the rug: alarm suppression might relieve the operator by reducing the distraction level, but only creates a false sense of security as the underlying problems remain. In the case of the data in Figure 1, suppressed alarms constitute, on average, 83% of the alarms generated. Under good alarm practice guidelines, suppressed alarms should only exist when there is a reason, such as when a unit or an instrument is temporarily out of service. Moreover, the suppression of alarms, temporarily or permanently, must be under strict management of change (MOC) control, or plant safety could become compromised. Yet, experience shows that most plants have hundreds of suppressed alarms with little or no tracking mechanism.

**ALARM MANAGEMENT JUSTIFICATION**

The driving forces for alarm management are increased plant productivity, and incident and near-miss reduction. Poor alarm performance results in frequent production loss as operators fail to grasp developing abnormal situations and often respond by either quickly cutting rates (the great process “stabilizer”) or by accepting off-specification products. A rate cut in response to an alarm burst is illustrated in Figure 2 using data drawn from a domestic petrochemical plant. The trends show clearly that the operator responded to the alarm bust by making numerous process changes (up to 35 in a 10 minute period.) Unable to stem the alarm burst, the operator then halved the rates from 12 to 6 Mlb/hr for 20 minutes, costing the plant 1,000 lb of lost throughput.
At the other extreme are less frequent, albeit more dramatic, industrial accidents that can be tied back to dysfunctional alarm systems. The EEMUA report cited above references two major industrial incidents – one in a refinery, the other in the Anglo-French Channel tunnel – where alarms floods contributed to the confusion that preceded accidents involving substantial property loss. These instances are by no means unique; and the authors of this paper are familiar with other such major accidents in plants throughout the world. In almost all instances, alarms that should have helped mitigate the accident did not do so. Additionally, poor alarm management practices may have worsened the accidents. Thus there are tangible reasons to rationalize alarms; a process by which alarms are given structure and become a source of very specific and constructive information from the standpoint of the operators.

That is not to say that alarm systems are without limitations of their own. A properly rationalized alarm system will be effective only within the normal spectrum of process operation and disturbances. Moreover, alarms are reactive by nature and are weak at
anticipating the drift of a process toward an abnormal situation, i.e., an operating point clearly outside the intended envelope of the process. Under such circumstances, alarms lose their effectiveness and must be supplemented with software systems that can detect the developing abnormality and proactively raise it to the operator’s attention (see the definition of a Predictive alarm system in Table 1 below.) The discussion of such systems lies outside the scope of this paper.

SOLVING THE ALARM MANAGEMENT PROBLEM

Alarm management is a set of business processes and DCS strategies deployed to deliver effective alarm messages to the operator. Alarm management can be addressed through a three step methodology that has been developed over the last decade by the consultants at Plant Automation Services (PAS.) The three steps of the methodology are:

- Build a baseline of alarm statistics to benchmark performance
- Develop desired performance goals and define an improvement plan
- Execute the improvement plan and measure the performance improvements

Alarm performance baseline

The first step toward establishing an effective alarm management strategy is to evaluate the state of the existing system and develop a baseline report. The baseline report is an indicator of the “health” of the alarm management system. This report is built on the results of software that analyze the existing alarm database configuration (i.e., the “static alarm” configuration) and the historical alarm journals (i.e., the “dynamic alarms.”) Alarm baseline reports developed by analyzing static and dynamic alarms at plants in the refining, petrochemical and chemical industries lead to three main conclusions:

- Most plants have too many alarms configured
- Most alarms are over prioritized
- Most alarm trip points are set overly aggressively
A good metric of the extent to which a plant is alarmed is the number of alarms per alarmable tag. Figure 3 shows the frequency distribution of this metric for 42 different operator stations (OSs) in plants worldwide. The histogram in Figure 3 shows, for example, that 8 of 42 OSs surveyed had between 1.5 and 2.0 alarms per alarmable tag. One OS, a unit in a Middle Eastern refinery, had nearly 7 alarms per alarmable tag. On the average, the 42 OSs surveyed had 2.6 alarms per alarmable tag, substantially in excess of the upper limit of one alarm per alarmable tag that PAS consultants recommend. EEMUA guidelines for alarm counts are more specific (and beyond the scope of this discussion) and cannot easily be used for comparison with Figure 3. It must be specified that the guideline of one alarm per alarmable tag represents an average. The reality of the situation is that most tags requiring alarms often need two alarms (measurement high and low, for example.) The average of one alarm per alarmable tag is reached because many tags need no alarms at all.

![Figure 3. Alarm count for 42 instrumentation nodes](image-url)
While specifics vary from one set of equipment to the next, alarms are typically categorized into three priority levels: low, medium and high. EEMUA guidelines recommend that these three categories represent 80%, 15% and 5% of the total static alarm count, respectively. Baseline audits conducted by PAS consultants show that high priority alarms are over represented in most OSs. Figure 4 shows the frequency distribution of the high priority alarms within the sample group of 42 OSs previously discussed. The data show that of the 42 OSs, only one had less than 5% of its alarms configured with high priority. Two OSs had between 75% and 80% high priority alarms. On average, the OSs had 28% of their alarms configured as high priority alarms, substantially beyond the 5% EEMUA guideline. Such overuse of the high priority category shows that in configuring static alarm databases, engineers prefer to err on the side of safety and systematically overestimate the importance of alarm conditions. This is a commendable attitude in itself, but one that has the perverse effect of devaluing the alarm messages insofar as the operators are concerned.

Figure 4. High priority static alarm histogram (all alarms)
The third conclusion, that alarm trip points are set overly aggressively, is illustrated with the data in Figure 5, which shows the histogram of unsuppressed high priority alarms for 37 of the 42 OS nodes in our discussion (five data are missing.) The histogram shows that, on average, high priority alarms make up 35% of the unsuppressed dynamic alarms, i.e., of the alarms notified to the operator. Moreover, in seven OSs, over 50% of the dynamic alarms were high priority alarms. These results indicate that operators either selectively suppress low priority alarms, in order to show preference to the high priority ones, or have high priority alarm trip points set overly aggressively, once again under the logic that it is better to be safe than sorry. In both instances, the result shows the overuse of the high priority designation: if there were that many “truly” high priority alarms, incidents and automated shutdowns would be much more frequent.

![Figure 5. High priority dynamic alarm histogram (unsuppressed alarms)](image)

The systematic analysis of alarm journals yields valuable information on the status of an alarm system and its underlying problems, and is part of the process of establishing the performance baseline. This analysis also establishes five categories into which alarm
systems fall (Table 1,) and provides substantive direction for the subsequent alarm rationalization effort.

<table>
<thead>
<tr>
<th>Alarm System Performance Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overloaded</td>
<td>A continuously high rate of alarms, with rapid performance deterioration during process upsets. The alarm system is difficult to use during normal operation and is essentially ignored during plant upsets as it becomes unusable.</td>
</tr>
<tr>
<td>Reactive</td>
<td>Some improvements compared to Overloaded, but the peak alarm rate during upset is still unmanageable. The alarm system remains an unhelpful distraction to the operator for much of the time.</td>
</tr>
<tr>
<td>Stable</td>
<td>A system well defined for normal operations, but less useful during plant upsets. Compared to Reactive, there are improvements in both the average alarm and peak alarm rates. Nuisance alarms are resolved and under systematic control. Problems remain with the burst alarm rate.</td>
</tr>
<tr>
<td>Robust</td>
<td>Average and peak alarm rates are under control for foreseeable plant operating scenarios. Dynamic alarming techniques are used to improve the real-time performance. Operators have a high degree of confidence in the alarm system, and have time to read, understand and respond to all the alarms.</td>
</tr>
<tr>
<td>Predictive</td>
<td>The alarm system fully encapsulates the aspirations of the EEMUA guidelines. The alarm system is stable at all times and provides the operator with the right information at the right time. Alarms are predictive and anticipate problems before they actually occur in order to avoid process upset or minimize their impact on production.</td>
</tr>
</tbody>
</table>

**Performance goals and improvement plan**

The definition of goals and the development of a plan must precede any effort to bring structure into an alarm system. Alarm management experts recommend that operating companies aspire to achieve at least the Robust alarm performance level should their facilities not already meet its criteria. This achievement level is consistent with the overall direction of the process industries and is well within the reach of current DCS functionality. Achievement of this level of performance requires the adoption of an improvement plan that is implemented through project execution internally or jointly with outside resources.

A central feature of the improvement plan is the alarm philosophy document, which must be developed through a team effort that brings together all the parties concerned. Team members must at least include the technical supervisors who understand how the
equipment behaves and the shift operators who, literally, will have to live with the alarms. There should be no hesitation to involve an external specialist to ensure that the alarming capability of the DCS is understood and leveraged to its full potential. It cannot be overemphasized that only a comprehensive approach that looks at all the alarms and listens to all the stakeholders can succeed in the long term. Beyond writing down rules for consistent alarm creation, prioritization, shelving, suppressing, dynamic alarming, etc., the alarm philosophy document must address the following points:

- Ergonomics of alarm display must be reviewed to ensure the implementation of good principles of human machine interface (HMI).
- MOC practices for alarms must be defined, publicized and deployed. Known and enforced business processes for changing alarm configuration will prevent operators from making point changes without considering their impact on the rest of the alarm structure, as is too often the case.
- Key performance indicators (KPIs) must be defined to track the long term performance of the alarm system.
- Sustained performance practices must be defined and assigned. It is important that someone in the plant be responsible for periodically auditing the alarm journals, reviewing the KPIs, and systematically addressing the nuisance alarms. Alarm management is a continuing process, not a milestone.
- Alarm versus alert? Alarm flood conditions are often compounded by on-line applications that use the alarm log to issue what are really alert messages. The latter are intended to advise the operator of a change in operations, such as an advanced control loop coming off-line, and for which no immediate action is necessarily required. The alarm philosophy must define the criteria for sending on-line application messages to the alarm journal or to an alert log.
Improvement plan execution

A phased approach to rationalizing alarms is often the only realistic path forward in this age of lean operating staff. As a first step, quick relief is available for overwhelmed alarm systems by resolving the most frequent alarms, the so-called nuisance alarms, and by fixing and removing all suppressed alarms. The effect of removing nuisance alarms from a daily alarm count is illustrated in Figure 6. This figure shows that over a 55 day period, removal of the ten most frequent alarms reduced the daily alarm count by two thirds, from an average of 2,650 alarms per day to less than 900 (this data set of dynamic alarms is from a plant in the Middle East.) The baseline report is instrumental in identifying the nuisance alarms by providing tables that summarize the most frequent chattering, duplicate, stale, consequential alarms, etc., thus allowing the immediate removal of the worst offenders.
While the removal of nuisance alarms can provide a dramatic improvement in alarm counts, it is only a step in a comprehensive rationalization effort. Alarm rationalization proceeds by configuring all the alarms in the static database in a consistent and thought-out manner based on the results of the philosophy document. It can be, and often is perceived, as a demanding task. Modern DCSs can be linked to thousands of instruments and the rough count of one alarm per alarmable tag implies that there can be an equal number of alarms to define. In most instances, there is no alternative but to plod through the instrument list to rationalize alarms point by point; a laborious and tedious task, but the only one that can successfully create a consistent implementation of alarm settings.

The rationalization is best conducted one OS at a time, with experience from one rationalization effort feeding the next. Fortunately, experience shows that rationalization sessions pick up in pace as similarities between instruments allow entire classes of alarms to be configured in a repetitive and efficient manner. Moreover, the support provided by a strong philosophy document, and the right alarm analysis software, do much to guide and streamline the rationalization effort.

Tangible dynamic alarm performance improvements after rationalization can be measured against the data in the baseline report. Table 2 shows the effect of rationalization on several alarm KPIs for a US petrochemical plant. From the operator’s perspective, the average daily unsuppressed alarm count was reduced from 1900 to 231, as shown in Figure 7 (note data gap on days 66-69.) These statistics and trends demonstrate the effectiveness of the methodology described in this paper and justify the value of investing in alarm rationalization projects.
### Table 2. Alarm system improvements after rationalization

<table>
<thead>
<tr>
<th>KPI</th>
<th>Reduction (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total alarms generated by the system</td>
<td>93</td>
</tr>
<tr>
<td>Total alarms presented to the operator</td>
<td>88</td>
</tr>
<tr>
<td>Chattering alarm occurrences</td>
<td>65</td>
</tr>
<tr>
<td>Total alarms configured on the system</td>
<td>50</td>
</tr>
<tr>
<td>Alarms not in service (disabled or inhibited)</td>
<td>50</td>
</tr>
<tr>
<td>Duplicate alarms</td>
<td>50</td>
</tr>
</tbody>
</table>

### Figure 7. Pre- and post-rationalization daily alarm counts

Average = 1900  
Average = 231
Appendix. Alarm management glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static alarm configuration</td>
<td>All the alarm configuration data in the instrumentation system, such as what happens when a temperature indicator reaches a high limit (e.g., issue a message; disable a control loop, etc.) The configuration data are collectively known as the static alarm database.</td>
</tr>
<tr>
<td>Dynamic alarm journal</td>
<td>The log of all the alarm messages that are triggered over time when conditions in the plant satisfy those defined in the static alarm database.</td>
</tr>
<tr>
<td>Dynamic alarming</td>
<td>The alarm equivalent to control’s “gain scheduling.” Alarm trip points can require different settings depending on the operating condition of the process. Dynamic alarming automatically changes the trip points based on the detected “state” of the process.</td>
</tr>
<tr>
<td>Suppressed alarm</td>
<td>An alarm that is prevented from appearing on the operator screens or in the history journals, or both.</td>
</tr>
<tr>
<td>Nuisance alarm</td>
<td>An alarm that is suspect and cannot be relied upon to deliver accurate information to the operator, such as stale, chattering, duplicate or suppressed alarms. Also called a “bad actor.”</td>
</tr>
<tr>
<td>Chattering alarm</td>
<td>An alarm that transitions into and out of alarm in a short amount of time.</td>
</tr>
<tr>
<td>Duplicate alarm</td>
<td>An alarm that persistently occurs within a short period of time of another alarm.</td>
</tr>
<tr>
<td>Consequential alarm</td>
<td>The source alarm around which duplicate alarms occur.</td>
</tr>
<tr>
<td>Shelved alarm</td>
<td>An alarm that is temporarily suppressed.</td>
</tr>
<tr>
<td>Stale alarm</td>
<td>An alarm that remains “in alarm” for an extended period of time.</td>
</tr>
<tr>
<td>Alarm trip point</td>
<td>The value that must be crossed by a measurement, or a condition that must happen, in order to trigger an alarm.</td>
</tr>
</tbody>
</table>

References


Acknowledgments

The authors are indebted to Donald Campbell Brown of BP Exploration Operating Co. for his valuable comments and ideas. All of the data in this paper come from production plants. The data set used in Figures 3 to 5 is based on a collection of baseline reports created over the years by PAS consultants. It is a selective data set only in the sense that it reflects the state of affairs within facilities that have recognized an alarm problem and have solicited expert consulting services to help them resolve it.

The authors

Pierre Grosdidier works at PAS, where he is Director of Engineering Services for Asset Optimization, a division that includes alarm rationalization services. Pierre earned B.Eng. and M.Eng. degrees from McGill University and the Ph.D. from Caltech, all in chemical engineering. He is a registered professional engineer in the State of Texas.

Patrick Connor works at PAS, where he is a Lead Project Engineer. Patrick earned a B.EE. from Georgia Institute of Technology and is a registered professional engineer in the State of Texas.

Bill Hollifield has 27 years of experience in the chemical industry in both engineering and production, with focus in automation and control systems design and support. At PAS, Bill specializes in alarm management project work. Bill has a mechanical engineering degree from Louisiana Tech University and an MBA from the University of Houston.

Samir Kulkarni works at PAS, where he is lead control system engineer for Asset Optimization. Samir earned B.Eng. degree from Bombay University in instrumentation engineering. He worked for BASF and Kuwait National Petroleum Company before joining PAS.