CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Eddy de Rademaeker, Peter Schmelzer
Copyright © 2016, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-39-6; **ISSN** 2283-9216
DOI: 10.3303/CET1648153

Pushing Process Limits Without Compromising Safety

Hector R. Perez

PAS, Inc, 16055 Space Center Blvd., Suite 600, Houston, TX, 77062
HPerez@pas.com

Numerous accident investigations highlight lack of proper overview displays and alarms as root causes or contributing factors to accidents. One example of this is the Texas City incident in 2005, in which “the control board display did not provide adequate information on the imbalance of flows in and out of the tower to alert the operators to the dangerously high level” (Source: U.S. Chemical Safety and Hazard Investigation Board, Final Investigation Report, March 23, 2007).
Industry has spent billions to design and install automated safety systems, in accordance with highly detailed standards such as ISA-84 (IEC 61511), Safety Instrumented Systems. Despite these efforts, the accidents continue and are often attributed to human error. In many companies, management is highly concerned at verifying, at all times, whether the processes are within a variety of acceptable boundaries.
While operating inside safe boundaries sounds simple, modern control systems (e.g., DCS, SCADA) are not designed to track boundaries other than process alarms. Indeed, alarms setpoints and activation rates are enough of a challenge to control; visualization, management and control of operational boundaries are even more complex.
Consolidating operational boundaries is difficult because the information resides in multiple databases, or worse – in hard copy files. Additionally, capacity “creep” and debottleneck activities or minor betterments will change the throughput of the process, pushing the process closer to or beyond the original design limits. From an operational perspective, the process needs to be compared to these documented limits in real-time for effective operator situation awareness. The actual operational information resides in the automation system, making this comparison a challenge. How can an operator recognize approaching operational, design or safe limit violations in a timely manner without adding excessive alarms? Moreover, how do violations of the limits get logged, tracked, and investigated to prevent recurrence?
Managers, engineers, and operators are responsible for making sure that easily-changed automation systems remain both configured and operated within appropriate boundaries. In this paper, we discuss new technology and methods for aggregating, analyzing, depicting, and controlling process boundary information to increase awareness of the operator while enabling engineers and managers to ensure that the process is always within safe limits.

1. Console Operators and the First Problematic Set of Operational Limits: Process Alarms

Console operators constantly make real-time decisions. Time is a luxury they do not have. Operators must immediately remediate abnormal situations before they escalate into bigger problems that lead to incidents and accidents. On a “lucky” day, an unresolved abnormal situation may result in a shutdown affecting production and profitability. As a worst-case scenario, it can end up as a catastrophic loss of life. The console operator, a critical resource, must have visibility to relevant, accurate, and meaningful information at all times. As a result of the previously mentioned Texas City incident and many other incidents like it, the industry began to address the problem of poor alarm management. The first step in doing so was to understand what created the problem.

1.1 History of the Alarm Management Problem

Prior to the advent of Distributed Control Systems (DCSs), plants had control boards on which “lightbox” alarms coexisted with the live measurements displayed on trends and gauges on the wall. These lightboxes contained a limited number of alarms. Both the installation of the boxes and the installation and configuration

Please cite this article as: Coward A., 2016, How can operating teams push processes to their optimal limits while maximizing safety and minimizing environmental impact?, Chemical Engineering Transactions, 48, 913-918 DOI:10.3303/CET1648153

of alarms on the boxes had costs associated with them, as the engineers had to run wires to make the connections. Due to the high cost, engineers configured only alarms that could be justified to management. For the operator to justify adding an alarm to the lightbox, an alarm had to indicate an abnormal situation with significant consequences if the operator did not take action. For this reason, control panels contained few alarms – typically around 120 alarms.[1]

1.2 The Birth of the DCS and Lack of Guidelines Creates the Alarm Management Problem

Control boards did not provide flexibility for plants to easily modify their control strategies and gain competitive advantage. As an example of this, simply extracting data from the control system to spreadsheets for analysis was nearly impossible. While the DCS provided more flexibility, it also introduced new paradigms that created the alarm management problem.

Three well-known factors contributed to the exponential growth of configured alarms: the loss of the "big picture" control wall, "free" alarms with the DCS, and a lack of guidelines for both effective configuration of alarms and creation of process graphics.[1,2] A control wall representing an overview of the entire span of control was eventually replaced by a DCS screen, with a few live values shown on it. The screens were expensive, and operators typically had only a few screens and thus a limited view of the process. To compensate, engineers created numerous alarms in order to direct the operator's attention. Alarms were (and still are) so easy to configure in the DCS, that engineers began using alarms for inappropriate uses such as maintenance, optimization, use by non-operators, and even for "personal" alarms. As a result, operators received thousands of alarms per day (in many instances, thousands of alarms in minutes during process upsets).[1] Human limitations to internalize and process information at such rapid rates led to unfortunate accidents, in which the alarm load was cited as a key contributing factor.

1.3 The Alarm Management Solution

Several publications, including *The Alarm Management Handbook* published by PAS[1], address the alarm management problem. The ISA-18.2 and IEC62682 standards have been adopted by a vast number of companies, and alarm management has generally become mandatory for the processing industry. By resolving the alarm management problem, companies improve safety and profitability. What other operational limits can be better managed to continue the same trend and drive greater competitive advantage?

2. The Console Operator's Job

A console operator's job is typically to monitor and control the process. What does this really mean? When there are process upsets the automation system cannot handle, the operator is expected to intervene and take action to prevent escalating consequences. When there are no process upsets, the operator is expected to adjust and optimize the state of operations.

2.1 The Console Operator Job During Normal and Abnormal Situations

The automation system is the first line of defense (for safety and profitability) against abnormal situations. Automated processes performed by interwoven disparate systems prevent human error and increase profitability. While well-defined alarms and alarm limits help operators to identify the root cause of abnormal situations and address them, complex automation systems and poor HMI can make it nearly impossible to provide situation awareness. Most operators view the process through dozens of poorly designed and cryptic P&ID-type screens, covered in hundreds of raw numbers.[2] If operators are inundated with such raw data on screens containing no context, they must rely on personal experience to decipher the data on top of an already heavy mental workload. In this scenario, the operator is reacting to an alarm versus proactively monitoring and controlling the process.

Imagine a commercial airline pilot taking off on the plane and setting the controls to ascend and not taking any further action until the "you are flying too high" alarm sounds. The pilot then pushes the controls to descend and does not touch them until the "you are flying too low" alarm goes off. Safety and efficiency would be compromised, and the airline would go out of business. Unfortunately, this is exactly how many plants operate today. Operators wait for an alarm to take an action and then wait for the next alarm to take another action. This problem can easily be resolved by providing the appropriate tools for the expected job.

Using enhanced visualization utilizing the concepts as explained in *The High Performance HMI Handbook*, console operators can proactively intervene. Figure 1 below shows raw data as typically depicted to console operators (left image) versus contextualized data that supports situation awareness (right image).[2]

The depiction on the left shows a vessel that has 200 psig of pressure (raw data). Is this good or bad? One possible answer is, "I have no clue." A better answer is, "it depends." The latter is a better answer, but it is not

good enough. A relatively new and inexperienced console operator may incorrectly assess the 200 psig as an acceptable value, and would not recognize the error until the alarm was activated (confirming that it was the wrong assessment). By this time, a domino effect of escalating consequences may be triggered. Early intervention of abnormal situations is critical.

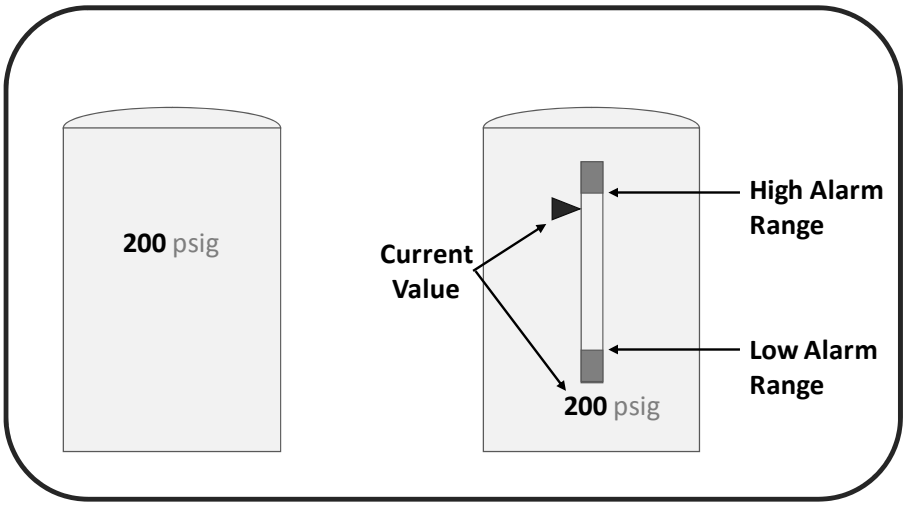

Figure 1: Raw Data vs. Contextualized Information

The vessel on the right-hand side of Figure 1 shows an analogue indicator bar with a pointer (triangle) that moves up and down as the pressure increases/decreases as well as the actual value of the pressure (number below the bar). Based on this information, is this pressure value good or bad? We can see that the pointer triangle is quite close to the High Alarm, and it looks like this process variable is about to go into abnormal conditions (alarm). This is easily interpreted by any operator, new or experienced; this graphical representation enables proactive intervention before an alarm occurs and enhances situation awareness.
During abnormal situations, the right-hand side depiction helps operators detect abnormal situations before they occur. If diagnosing a situation, operators can see how the process is moving, anticipate additional problems, and address them as they are working on the initial trigger of the problem at hand.

3. Alarms with Improved HMIs and Contextual Information Yield Enhanced Operator Performance

Let's assume the console operator has a fully rationalized alarm system with exactly the alarms that they need, which point to root causes of the problem, and that the operator has a High Performance HMI for complete situation awareness of the evolving abnormal situations. To improve efficiency and improve competitiveness, an organization may consider:

1. *What is the console operator's job description during normal situations?*
2. *What is the console operator's job description during abnormal situations?*

The answer to question #1 should be to optimize the process. If everything is running fine, High Performance HMIs enable the operator to make it run better. Figure 2 shows if the value is close to the alarm setpoint (left image) or if the value is within the depicted optimized operating region (right image). Anything between the optimized range and the alarm region triggers an operator action to optimize the process. It is an important principle in High Performance HMI displays to show the optimum ranges.
The answer to the reiterated question #2 remains the same – to take over the control system and take the necessary corrective actions. The operator needs tools that provide information to make the right decision. If best practices have been followed, alarms have been rationalized and every alarm has been documented with potential causes, consequences, and corrective actions, this information should be embedded in context within the graphics. In Figure 3, the alarm has occurred, and the operator should be able to easily "right click" the alarm region or indicator element and access this information to resolve the situation without escalating consequences.

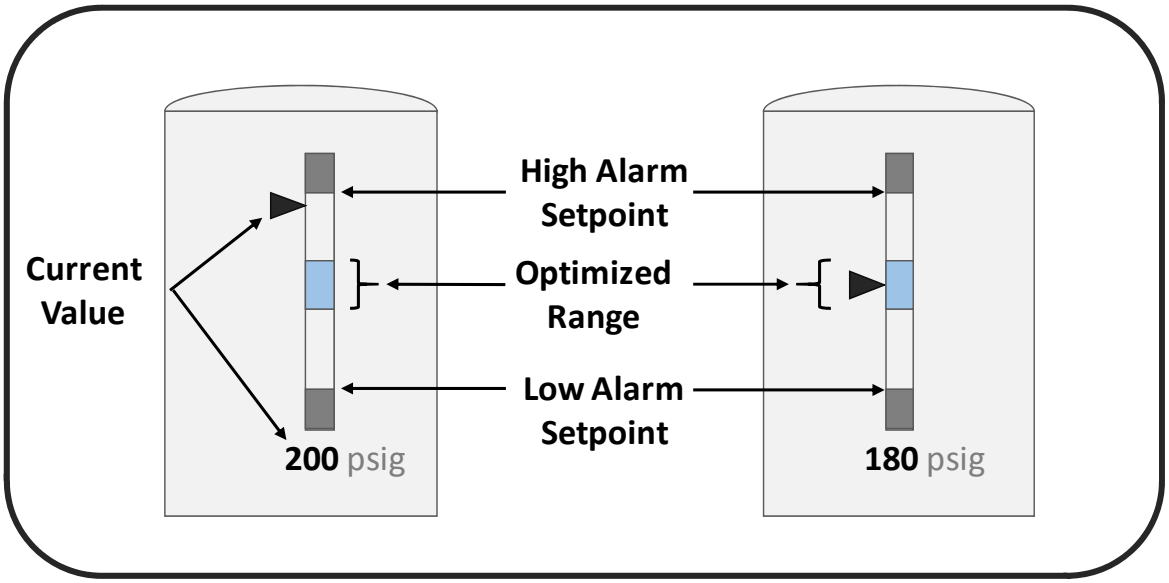

Figure 2: Situation Awareness for Process Optimization (Optimization Limits)

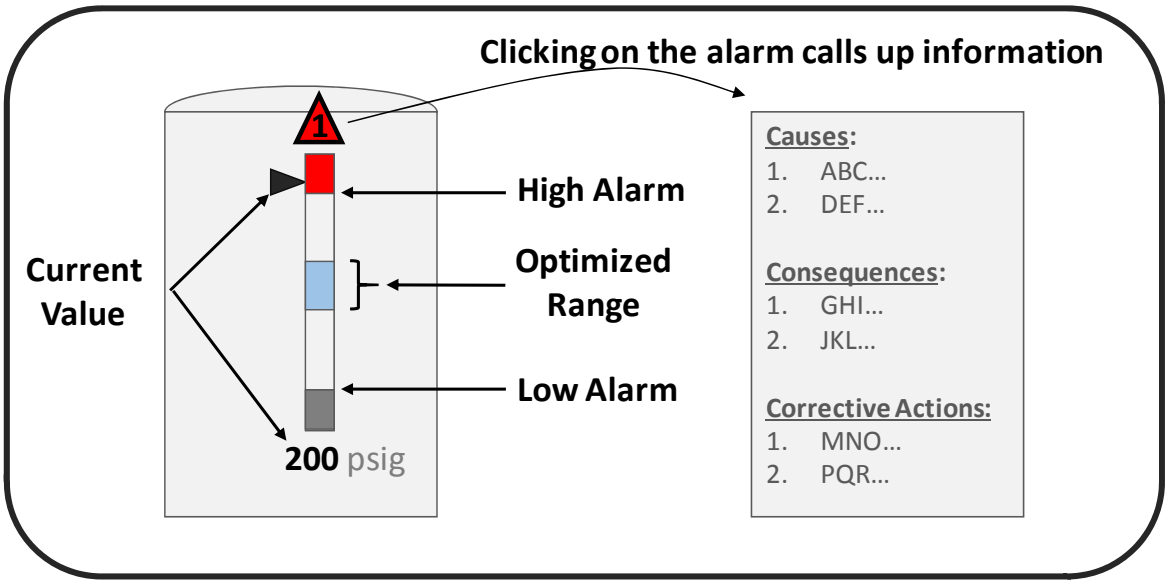

Figure 3: Contextual Information in HMIs

4. The Relationship Between Alarms and Other Operations Limits

To remain competitive, firms should continuously debottleneck processes and push production to the limits of equipment design specifications. To do so, the operator must monitor limits beyond just alarms, such as safety system activation points, environmental limits, and relief valve settings. This data exists in every plant, but unfortunately it is "sprinkled" amongst a multitude of different databases across different systems. To proactively monitor in this environment, an operator would have to memorize thousands of limits, look at the live values on the control system, and make mental comparisons to ensure no limit is violated. In simple words, that is not happening.

A best practice is to aggregate all of those limits and visualize them contextually in relation to each other. In Figure 4 below, the operator can see the pressure is in High Alarm and that – if no action is taken – increasing pressure will open an automated vent valve to a flare, resulting in product loss. If the vent valve cannot

decrease the pressure and bring the process back to normal, a second High-High alarm (acting as a pre-trip alarm) will indicate the process is headed to the next limit, a safety shutdown, which will cost considerably more production. If the safety shutdown fails to bring the process back to normal, engineers would be responsible to have designed the relief valves per code, so that the vessel will not exceed the Maximum Allowable Working Pressure (MAWP) by an unacceptable amount, and get nowhere near the actual vessel mechanical design limit.
In plants where production is constantly adjacent to the design limits of the process, this type of situation awareness assists the operators and guides their actions. A visual representation of limits reduces the mental workload of an operator and greatly enhances plant safety.

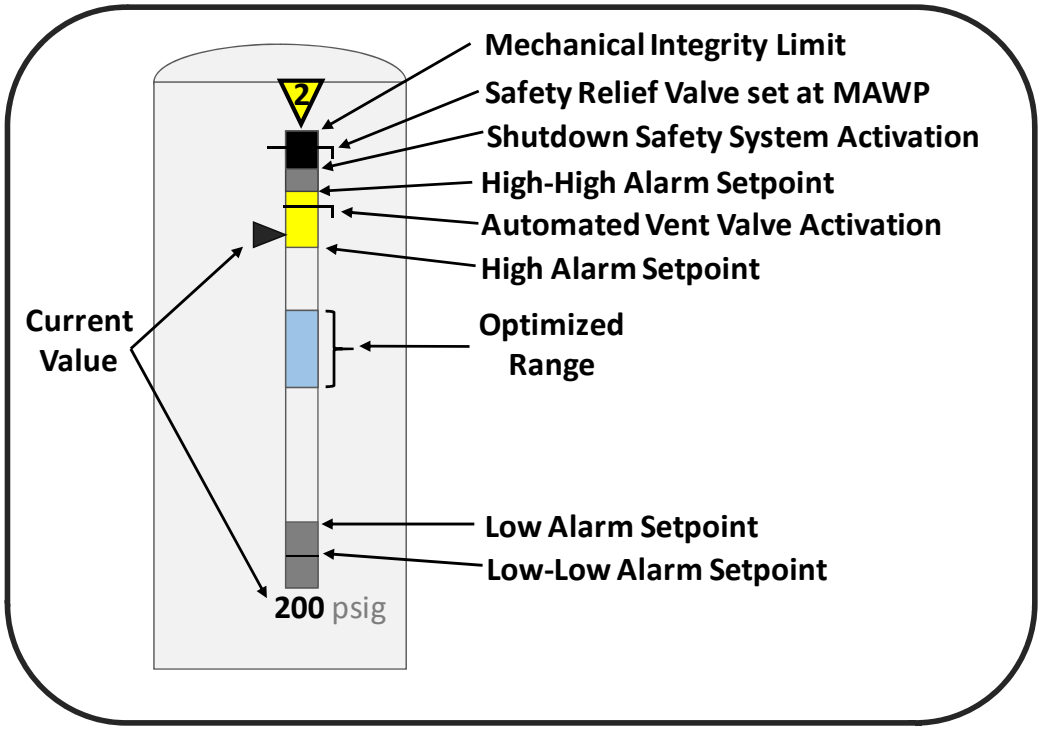

Figure 4: Contextualized Alarms with Other Operational Limits

4.1 Addressing the Concerns of Plant Management

Management must have confidence that the plant is running within proper operational boundaries. This requires assurance that not only the current operating process values are proper, but also that the underlying control system configuration reflects the known and proper operating boundary information. DCSs are notoriously easy to change, and accidents have been traced to improper changes in alarms and interlock settings.

These control system configuration questions must be continually verified:

1. Are the current settings in my control system proper considering the design documentation of the process? (Or have they migrated over time?)
2. Are these settings appropriate for normal operations within ranges associated with process design, quality, efficiency, emissions, and production rate?
3. Are alarms properly set to indicate the movement of the process into ranges requiring operator response to address the condition?
4. Are the settings for automatic safety function activation in accordance with design documentation?
5. Have there been any inappropriate changes to any of the setpoints or logic conditions of concern for identifying where the process is running relative to these boundaries?

The plant's current and recent operation relative to proper boundaries should also be easily seen and verifiable by operators, engineers, and managers. Questions to be answered include:

6. Is the process currently running within the normal ranges associated with safe design, quality, efficiency, emissions, and production rate?
7. How often and to what degree has the process been running outside of such normal ranges?
8. Is my process running within non-optimum or abnormal ranges, but still within safe ranges that do not activate automated shutdown systems, thus causing disruptive shutdowns that necessitate expensive and potentially hazardous restarts?
9. How often and to what degree has the process been running in ranges nearing the activation of automated safety systems?
10. Is the proximity of the process to the activation of automated safety systems clearly depicted to the operator?

When the answers to these questions are regularly determined and easily known, management can be much more confident that significant accidents or expensive shutdowns are unlikely. Engineers and operators can have confidence that the process is truly under control. But, in many companies there are no systems in place to answer these straightforward questions.

5. Conclusions

Real-time visualization of aggregated and validated operational boundary limits improves safety and compliance. With improved situation awareness, operators can take pre-emptive corrective actions. Using High Performance HMIs to aggregate operational limits, console operators can push operational limits without compromising safety or the environment.[2]

Process limits include those for quality, efficiency, and safety. Situation awareness of the process relative to those limits is essential. Rules can be established to create dynamic relationships between different limits, and technology tools exist to monitor deviations from these limits. As an example, a rule can ensure that high pressure alarms are set no higher than 90 percent of the relief valve activation pressure. If an alarm is incorrectly configured too closely to the relief valve activation point, technology tools can automatically detect this condition and send an automated email to the responsible party. These tools also provide valuable insight through data analysis on violations per week, most frequent violations, chattering violations, stale violations, and more. Costs or losses associated with violations can be automatically calculated and reported. These analyses can be used to create score cards to help prevent recurrence.

Console operators cannot memorize thousands of limits and make the correct decisions in real-time, every time. Their situation awareness can be greatly increased by presenting aggregated and contextual information. The result will be increased efficiency and profitability.

References

Hollifield B., Habibi E., 2010, The Alarm Management Handbook, Second Edition
Hollifield B., Oliver D., Habibi E., Nimmo I., 2008, The High Performance HMI Handbook.