WHITE PAPER

Octave Tempo Boundary Analytics: Better knowledge of safe operating limits to improve human reliability

Contents

Abstract

In many plants, the various safe and design process operating boundaries are contained in a variety of disparate and often inconsistent documents. Managers, engineers and operators are responsible to ensure that easily-changed control systems remain both configured and operated within appropriate boundaries. This paper discusses new technology and methods for aggregating, depicting and controlling process boundary information to increase the operator's awareness and ensure to engineers and managers that the process is always being operated appropriately.

Introduction

Major accidents still occur in the process industries with far too high a frequency. Most such accidents involve operating some part of the process outside the designed safe or acceptable boundaries.

For many years, very stringent standards involving comprehensive design methodologies for safety systems have been in effect. Despite these standards, the accidents continue. In many companies, management is highly concerned with verifying, at all times, whether the processes are within acceptable boundaries.

Consistently accomplishing operations within safe boundaries sounds simple – but it is not. Most control systems and human machine interfaces (HMIs) were not designed to track or display such conditions. The very definitions and values defining the various process boundaries are likely to be contained in a variety of company documents or separate databases-seldom in one place.

This paper covers:

- The questions that need to be asked regarding operation within appropriate boundaries
- Relevant standards
- Consistent terminology for defining various process boundaries
- Documentation sources for boundary settings
- Software monitoring of control system settings and values relative to boundaries
- The depiction, tracking and reporting of process conditions and boundaries

Questions: What do you need to know?

Several specific process operational questions are of great interest to management, engineers and operators. These are divided between questions relating to control system configuration and process design and operational questions regarding the current status and operating history.

Configuration questions

Are the settings in my control system proper, considering the design documentation of the process? Or have they migrated over time?

- Are these settings appropriate for normal operations within ranges associated with process design, quality, efficiency, emissions and production rate?
- Are alarms properly set to indicate the movement of the process into ranges requiring operator response to address the condition?
- Are the settings for automatic safety function activation following design documentation?
- Have there been any inappropriate changes to any setpoints or logic conditions of concern for identifying where the process is running relative to these boundaries?

Operational questions

Is the process running within the normal ranges associated with safe design, quality, efficiency, emissions and production rate?

- How often and to what degree has the process been running outside of such normal ranges?
- Is my process running within non-optimum or abnormal ranges but still within safe ranges that do not activate automated shutdown systems, causing disruptive shutdowns that necessitate expensive and potentially hazardous restarts?
- How often and to what degree has the process been running in ranges nearing the activation of automated safety systems?
- Is the proximity of the process to the activation of automated safety systems 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, systems must be in place to answer these straightforward questions. Some background is necessary to describe the solution.

Relevant standards

There is an entire science of process safety design involving the concepts of Safety Integrity Level (SIL) and Safety Instrumented Functions (SIF). The methods described in the standards associated with these concepts involve probabilistic risk assessment, layers of protection and the design of control technologies appropriate to mitigate identified risks to acceptable levels. This is typically using various redundancies of sensors, separation of control and safety functions and fail-safe designs.

This body of knowledge is identified by several International Society of Automation (ISA) and International Electrotechnical Commission (IEC) standards documents (see references) abbreviated in this paper as "S-84."

The development of S-84 involved adopting terminology with precise definitions and some of this terminology involves certain process boundaries. This terminology is now accepted and widely used. However, it is primarily directed at the design of control and mitigation equipment. As such, the terminology only addresses some of the industry's process boundaries of high interest.

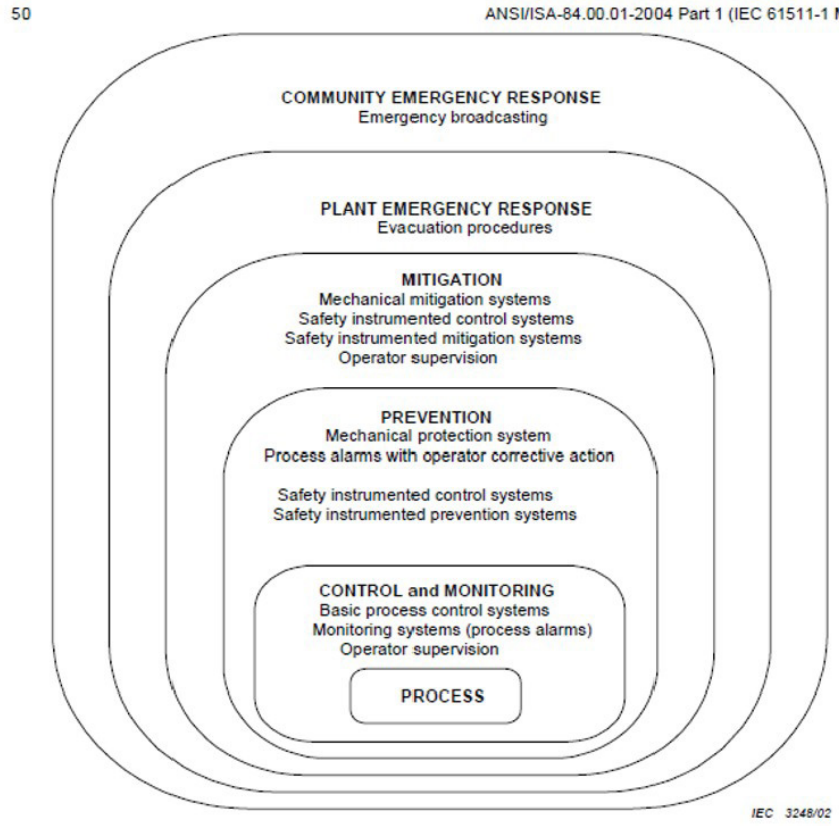


Figure 1.
Risk reduction methods

Some relevant terms in the S-84 documents are as follows; these are direct quotes:

3.2.72 Safety Instrumented System (SIS): an instrumented system used to implement one or more safety instrumented functions. A SIS is composed of any combination of sensor(s), logic solver(s) and final elements(s).

3.2.71 Safety Instrumented Function (SIF): safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.

3.2.74 Safety Integrity Level (SIL): discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level four has the highest level of safety integrity; safety integrity level one has the lowest activation setpoints or internal functioning.

3.2.59 Protection layer: any independent mechanism that reduces risk by control, prevention or mitigation.

NOTE: It could be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical engineering mechanism such as a relief valve, a safety instrumented system or an administrative procedure, such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions.

3.2.25 Functional safety: part of the overall safety relating to the process and the basic process control system (BPCS), which depends on the correct functioning of the SIS and other protection layers.

3.2.19 External risk reduction facilities: measures to reduce or mitigate the risks, which are separate and distinct from the SIS. Examples include a drain system, firewall and bund (dike).

The major focus of S-84 is designing and implementing safety interlock systems independent from the BPCS. These are systems that, when certain process conditions are met, "take over" the process regardless to what the control system or operator is trying to do and automatically return the process to a safe state (often the "shutdown" state). In control systems that follow S-84 (most of them), there exist boundary conditions of many measurements that specifically activate parts of the S-84 safety system and automatic actions that take place that the operator cannot contravene.

Stringent management-of-change requirements are part of S-84 to ensure no improper changes are made in the SIS activation setpoints or internal functioning

Consistent terminology

There are several specific process operational questions of great interest to management, engineers and operators. Management is concerned with much more than just the boundary conditions that activate the safety system. Operating values relative to quality, efficiency, emissions and production rate are also important. Overlap thus occurs in the domain of boundaries relative to normal operations, abnormal operations and SIS functioning. Additional nomenclature is therefore needed and will be shown.

In Figure 2, the added blue outline is at the boundary between preventative and mitigating measures that "keep the process inside the pipe," and emergency response measures associated with dealing with a hazardous release. The role of the plant operator and the major concern of operations management, is with those preventative and control measures, not with emergency response, fire squad, plant or community evacuation. After all, the idea is to keep the process inside boundaries where such responses are never needed.

The Octave Tempo Boundary Analytics (formerly PAS InBound) domain includes everything up to the uncontained release of hazardous material, including emergency vents and relief valve settings (whether, for example, those devices are released to the atmosphere or flare systems).

It includes the basic control system, alarm system, overall HMI and any SIF type of safety system.

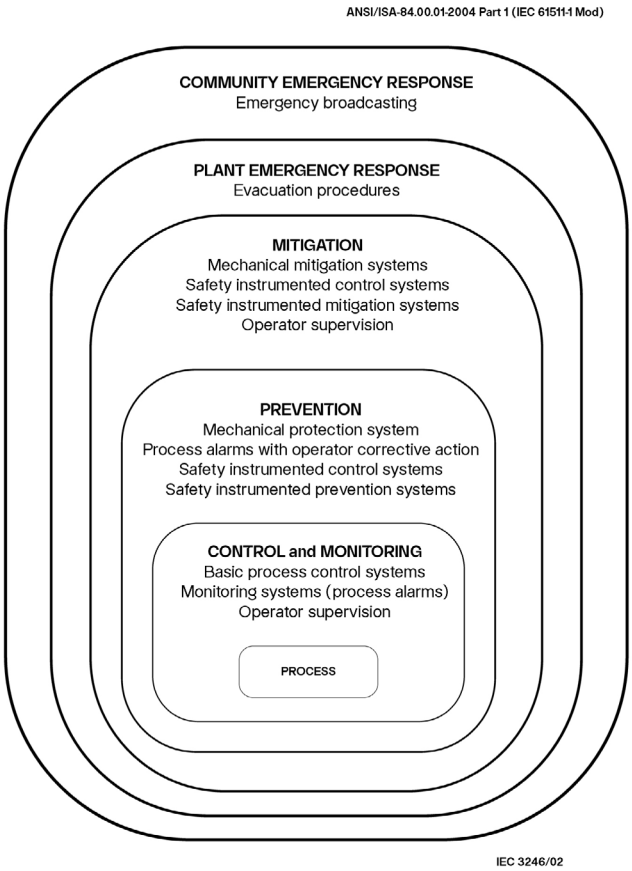


Figure 2. The domain of Tempo Boundary Analytics

The Figure 2 diagram is inadequate as-is for use with Tempo Boundary Analytics because it does not differentiate several of the things that greatly concern process management. For example, a relief valve venting a flammable gas into a flare system is a very different scenario than a relief valve that vents a flammable gas directly into the atmosphere. In determining whether the process is running within acceptable boundaries, such a situation may be treated or documented differently. So, the diagram requires some expansion.

A more granular and appropriate breakdown is shown in Figure 3:

Expanded risk reduction methods and boundaries

Tempo Boundary Analytics begins

Process design

- Equipment pressure, temperature and similar parameter ratings
- Design margins
- Inherently safe design

Control and monitoring

- Basic process control systems
- Monitoring systems and process alarms
- Operator supervision

Hazardous release prevention

- Pre-trip process alarms with operator corrective action
- Safety instrumented control and prevention systems
- Mechanical protection systems such as relief valves, vents exhausting non-hazardous material or exhausting hazardous material to acceptable treatment systems such as flares, scrubbers and incinerators
- Automated emergency shutdown systems (ESDs) involving fully contained post-shutdown processes or involving process release through mechanisms that treat any hazard such as scrubbers or flares.

Equipment protection/rupture avoidance

- Relief valves avoid vessel rupture by venting hazardous material directly into the atmosphere
- Safety instrumented automatic control and shutdown systems involving hazardous material release directly into the atmosphere

Non Tempo Boundary Analytics dividing line

Release mitigation (related to post-release)

- Mechanical mitigation systems such as dikes

Plant emergency response

- Evacuation procedures

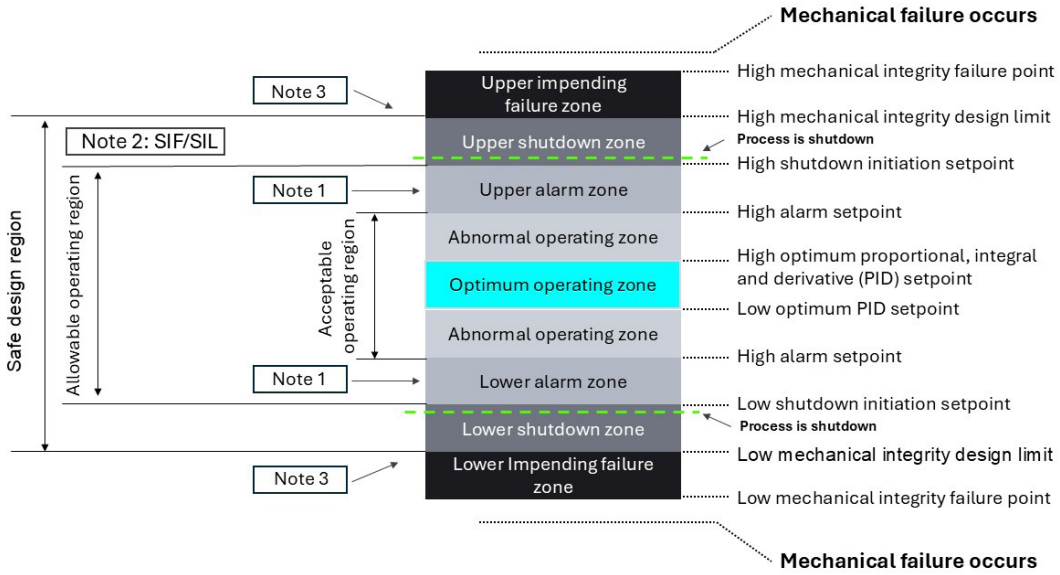
Community emergency response

- External emergency responders

Figure 3: A more detailed breakdown

Figure 3 more clearly differentiates the basic control system from the safety system and the types of mitigation associated with a variety of situations where the process is "still in the pipe." A distinction is made between non-hazardous or treated releases, with untreated releases that can pose a much more significant hazard (all releases are not created equal). Major accidents are often associated with untreated releases of flammables or toxins directly into the atmosphere rather than through appropriate flares or scrubbers.

Figure 4 relates all of the prior material with the addition of new terminology addressing the non-SIS aspects of the process; terminology lacking in the S-84 documents. Also incorporated are typical terms used in process control.



In Figure 4, Tempo Boundary Analytics terminology.

Detailed explanation of Tempo Boundary Analytics terminology

In Figure 4, Tempo Boundary Analytics terminology defines three regions.

- Safe design region
- Allowable operating region
- Acceptable operating region

The regions are divided into zones.

For explanatory purposes, it is easiest to think of Figure 4 as relating to a single process measurement such as pressure in a vessel. Figure 4 can also represent groups or combinations of different measurements and individual pieces of equipment or larger combined parts of a process. Here are the details of each identified region and zone.

Optimum operating zone

In the center of the diagram is the optimum operating zone, a range for a value (or values, from now on referred to in the singular) representing the desired condition. This zone is associated with on-spec, efficient operations per the process design. Note that the values defining this zone may differ for the same physical measurement or equipment when different products or materials are being processed. The edges of the optimum operating zone are associated with the high and low optimum PID setpoints if the measurement is associated with a PID controller.

Abnormal operating zone

This zone, adjacent to the optimum operating zone, indicates the range between optimum and where an alarm on the value is configured to occur.

Acceptable operating region

The combination of the optimum operating zone and adjacent abnormal operating zones defines the acceptable operating region. It is acceptable to run the process with alarms occurring.

Upper and lower alarm zone

If one exists, a high or low alarm setpoint define the boundary between the abnormal operating zone and the alarm zone. High and low alarms are used for simplicity of explanation. The concept applies to any type of alarm indicating a condition that requires operator response to avoid a consequence. This includes alarms based on logic constructs involving several measurements or status conditions.

Note 1: Upper or lower alarm zones may be subdivided into high-high (HI-HH), low-low (LO-LL) alarm zones, usually depending upon the nature of the corrective action being significantly different in kind or degree. The justification requirements for implementing separate HI-HH or LO-LL alarms should be detailed in the alarm philosophy. If there is an automated shutdown action based on the measurement, the HH or LL alarm might be considered as a pre-trip alarm, being the last such separate annunciation before the shutdown is initiated.

Allowable operating region

Since it is allowed (if not necessarily desired) to operate with an alarm in effect as the operator addresses the alarmed condition, the combination of the acceptable operating region and the alarm zones is called the allowable operating region.

Upper (and/or lower) shutdown zone

The outer boundary of either alarm zone is defined by the high or low shutdown-initiated setpoint (if one exists). This is the value at which an automated action(s) takes place to bring the process to a safe state (typically a shutdown implemented in the SIS, Note 2 on the diagram). Since there is inertia in most processes, the measurement may go higher (or lower) than this shutdown-initiated setpoint as

automated actions take effect. Such automated actions include valve closures, feed cutoffs or automated venting. This is why there is a dotted line for "process is shutdown" depicted in this zone.

The usual design of an SIS takes into account this inertia so that the shutdown process is safe and no equipment damage occurs. Therefore the upper (or lower) boundary of the shutdown zone is defined by high or low mechanical integrity design limit.

Note 3: The most typical examples of the high or low mechanical integrity design limits are the maximum allowable working pressure (MAWP) or temperature (MAWT) of a vessel. These are determined in the design of the vessel. The vessel will not fail at such a value, as there are significant safety margins built into their calculation. For example, relief valves are typically set at 100% of MAWP, even though sizing of the relief valve assumes a 10% overpressure accumulation to achieve rated flow. Codes allow for this practice. Similarly, a vessel will not fail at one degree above MAWT.

Safe operating region

The combination of the allowable operating region and shutdown zone(s) determines the safe operating region. Operation outside of this region is unsafe and unallowed.

Upper (and/or Lower) impending failure zones

At some point above the mechanical integrity design limit, the equipment will fail. The precise value for this occurrence, the high (or low) mechanical integrity failure point is often unknown. This is the range comprising the margin of safety in the equipment design itself. All protective systems are designed to not use this margin, with only specified exceptions allowed, such as limited relief valve overpressure. These zones are not truly used in process control but are in the figure for completeness.

An analogy to this situation is in aircraft design. All aircraft are certified with a V(ne) – a never exceed indicated airspeed. Operation above this airspeed is prohibited. At some value above V(ne) (around 150% depending on g-loading and other factors) the rudder, elevator, ailerons, tail, wings or some combination thereof will depart the fuselage. Flights above V(ne) are the domain of the test pilot, who is always equipped with a parachute. Operation past the mechanical integrity design limit is similarly prohibited. In process design, it is not generally important (or even possible) to have specific and highly accurate values for the failure point – since the entire safety design approach is never to get to that point.

Documentation sources for boundary limits

One cannot answer the question, "Am I inside my allowable boundaries?" if those boundaries are not specifically identified, documented and agreed upon. In most process plants, there is little to no consistent documentation of these boundaries. For example, the high shutdown initiation setpoint may be mentioned in a process hazard analysis or a SIF design document. It may be mentioned in an operating procedure. It may (or may not) be depicted on an HMI display used by the operator, on a help screen, or a P&ID or instrument loop drawing. Wherever it is, are all these values consistent and known by the person on the front line – the operator?

Are they reliably known or accessible to the engineer who modifies the control system?

ISA-18.2, the 2009 standard on alarm management, requires a master alarm database (MADB). This is a database of every alarm in the control system, along with several information items about each alarm. This database must be controlled through management-of-change and there must be periodic checks to ensure that the alarm settings are actually in effect on the control system accurately match the MADB.

Many companies have already created MADBs during the process of alarm rationalization, which is also a required element of ISA-18.2. It is desirable that this database also contains information on every single point on the control system, whether it is alarmed or not. Because of the practicalities of alarm rationalization of existing systems, most software designed to assist in rationalization. Octave Tempo Control System Effectiveness (formerly PAS PlantState Integrity) does this. It is logical to integrate Tempo Boundary Analytics with the MADB. With the simple addition of several database fields, the MADB becomes the perfect, managed place in which to aggregate the correct values for these mentioned important boundaries. Tempo Boundary Analytics can then accomplish certain analysis and reporting tasks regarding these boundary values and the actual settings on the control system.

A one-time effort is needed to collect or determine the boundary data and place it into Tempo Boundary Analytics. Sources of the data include:

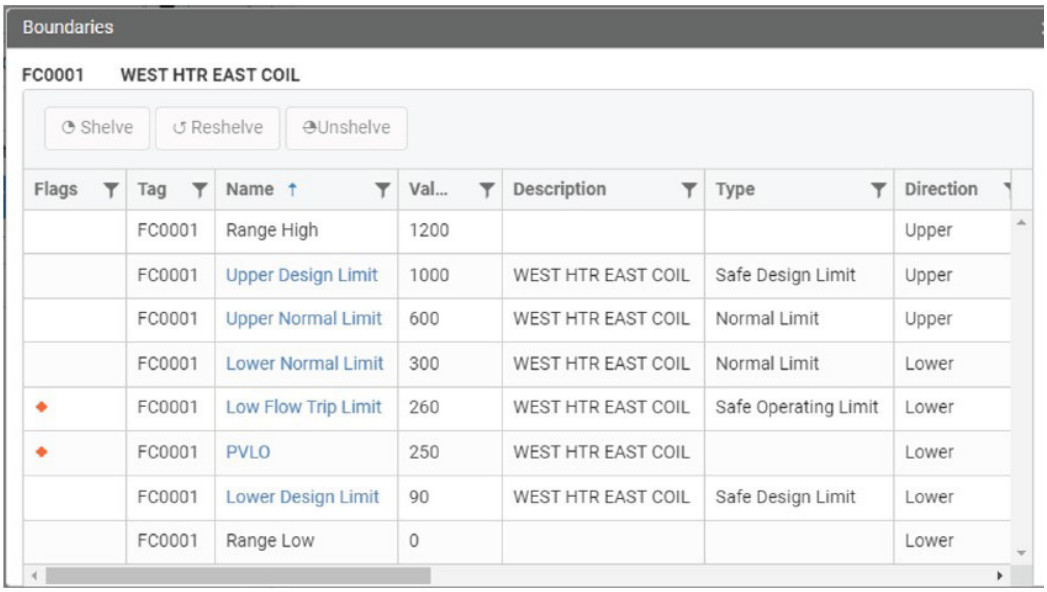
- Process design documents
- Project implementation reports
- P&IDs
- Instrument loop drawings
- Equipment design drawings or specifications
- Process hazard analyses
- Layer of protection analyses
- SIF/SIL design documents
- Operating procedures
- And other similar engineering documentation

In some cases, the same physical equipment is used to process different materials or make different products. Some of the Tempo Boundary Analytics values may be different in those cases. Just as alarms can be made “state-based” and the MADB stores different alarm settings and priorities for such cases, so can the boundary values be similarly differentiated.

Tempo Boundary Analytics supplies a safe and secure repository for important process boundary values that are likely to spread among many often unused, obscure and hard-to-access company documents. By being incorporated into the master alarm database, effective management of change is accomplished for these values.

Once incorporated, automated analyses can be made on an ongoing basis as to whether any control system settings are incompatible with proper settings relative to the various boundaries and constraints.

Figure 5: Value placement into Tempo Boundary Analytics



Flags	Tag	Name	Val...	Description	Type	Direction
	FC0001	Range High	1200			Upper
	FC0001	Upper Design Limit	1000	WEST HTR EAST COIL	Safe Design Limit	Upper
	FC0001	Upper Normal Limit	600	WEST HTR EAST COIL	Normal Limit	Upper
	FC0001	Lower Normal Limit	300	WEST HTR EAST COIL	Normal Limit	Lower
◆	FC0001	Low Flow Trip Limit	260	WEST HTR EAST COIL	Safe Operating Limit	Lower
◆	FC0001	PVLO	250	WEST HTR EAST COIL		Lower
	FC0001	Lower Design Limit	90	WEST HTR EAST COIL	Safe Design Limit	Lower
	FC0001	Range Low	0			Lower

Tempo Boundary Analytics monitoring of control system settings vs. boundaries

Whether the control system settings (configuration) remain in alignment with these identified boundaries is of high interest to engineers and managers. This can be accomplished and automated by coupling the database to the control system via an OPC data collection and display system. Configuration and process values read from the control system can be displayed compared to the various boundaries. Configuration violations can be easily detected and reported. Figure 5 shows two such violations. The low flow trip limit has been set above the measured value low setpoint (PVLO) alarm limit in this example. The PVLO alarm intends to alert and inform the operator of a low flow condition so that they can intervene in the process and avoid the low flow trip. However, the operator won't receive the alarm before the trip since the alarm is misconfigured in this scenario.

Periodic change and violation reports can be automatically generated to verify the performance of the management of change work process. Such reports can ensure the managerial requirement that the process control configuration is correct and safe.

Depiction of real-time performance vs. Tempo Boundary Analytics boundaries

By integrating live data from the control system and a process historian, different displays can be created for managers, engineers and operators to show process performance relative to real-time boundaries and incorporate process history.

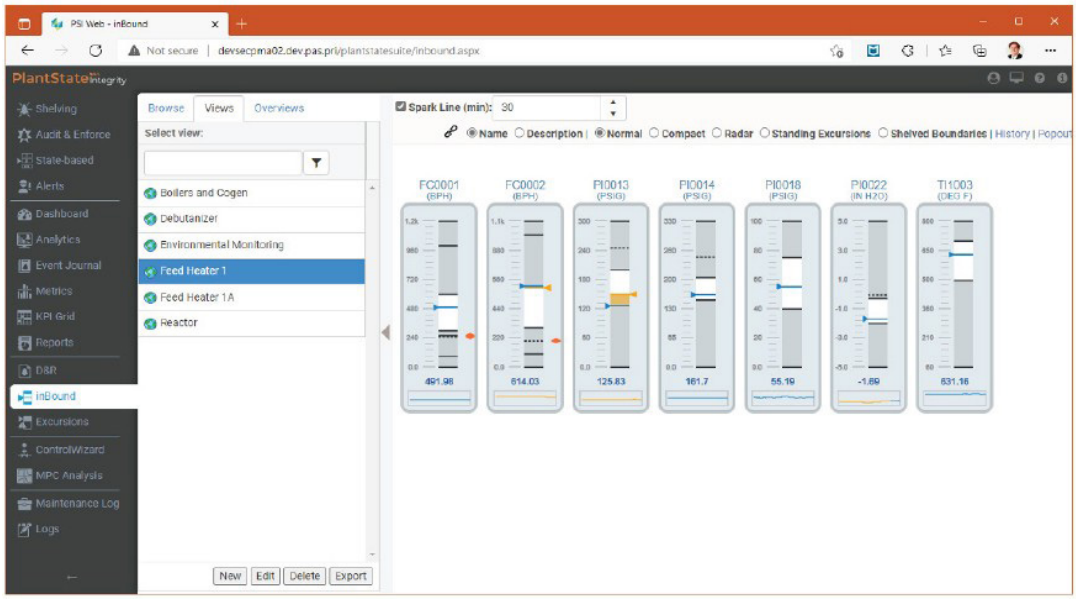


Figure 6: Tempo Boundary Analytics analog visualization of boundaries

For the operators, in particular, the principles of High Performance HMI trademark this depiction of process values in a context that shows some of this information. Most HMIs lack this, containing only raw numbers displayed on P&ID-style graphics. Such HMIs provide very poor situation awareness.

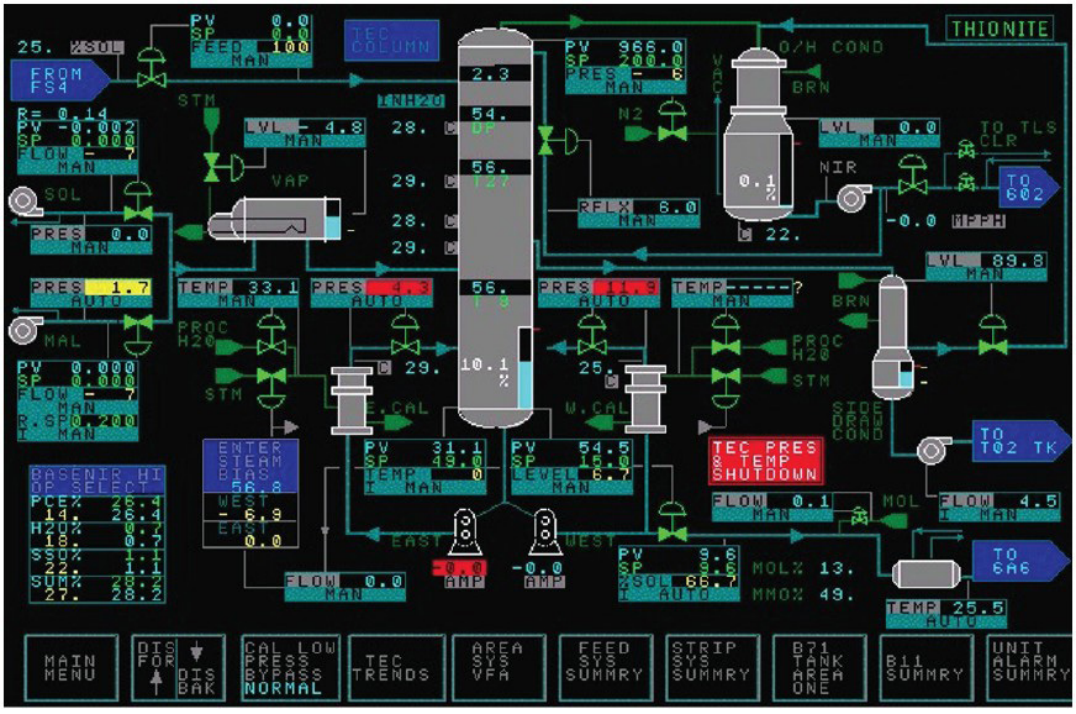


Figure 7: Poor but typical display of raw data to operators

High Performance HMI includes the depiction of values relative to the range where automated safety interlocks or actions occur. Including certain process boundary data into the operator's HMI can greatly increase an operator's situation awareness, significantly improve abnormal situation detection and response and avoid upsets entirely.

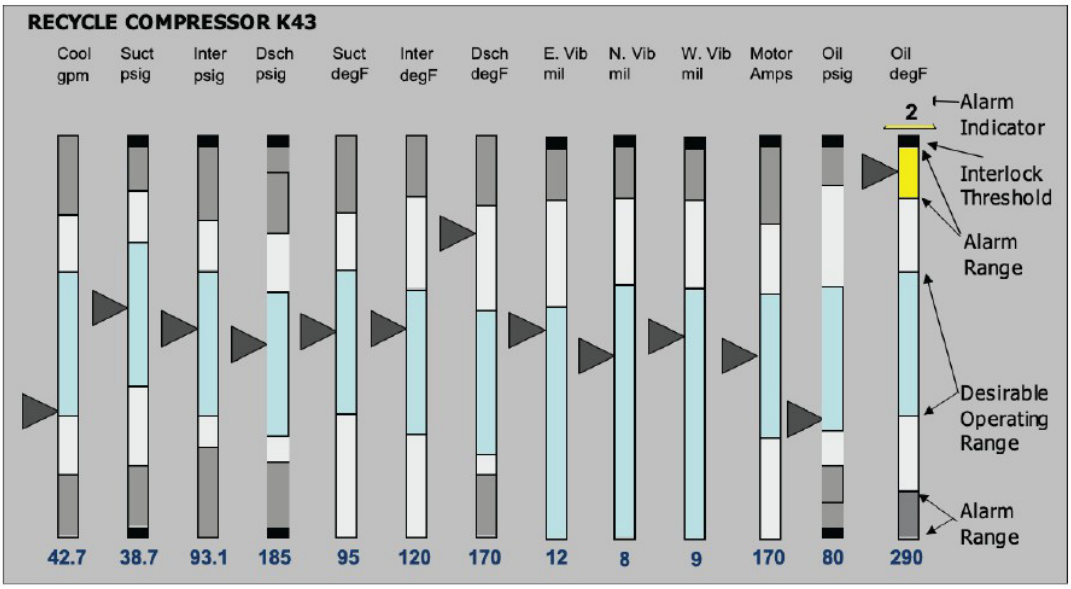


Figure 8: High performance HMI analog depiction of process values

In the Figure 8 example, abnormal values and alarmed conditions stand out clearly. Operators can rapidly scan dozens of such depictions in a far easier cognitive process than comparing raw numbers to memorized (and often incomplete or inaccurate) mental maps of what constitutes good or bad performance. Note that values that initiate interlock actions (such as SIFs) are clearly identified to the operator.

Summary

Important information about the boundaries of safe and effective plant operation is often difficult to find and hard to use. Tempo Boundary Analytics provides a safe, effective single place for such information, along with programmatic evaluation and capabilities. Tempo Boundary Analytics can ensure that control system settings are always properly selected and within important safety limits. Tempo Boundary Analytics concepts can be extended into relevant visual displays for engineers, managers and operators to ensure that the process is always operating within appropriate boundaries.

References

The domain of probabilistic risk assessment, Layer of Protection Analysis (LOPA), Safety Instrumented Function (SIF), and Safety Integrity Level (SIL) assessment ("S-84") is governed by these standards and guidance documents:

ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod)
Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements

ANSI/ISA-84.00.01-2004 Part 2 and Part 3
Functional Safety: Safety Instrumented Systems for the Process Industry Sector
Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1, Informative
Part 3: Guidance for the Determination of the Required Safety Integrity Levels – Informative

The International version is:
IEC 61511-1 ed1.0 (2003-01) Functional safety - Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

And Parts 2 and 3:
IEC 61511-2 ed1.0 (2003-07) and IEC 61511-3 ed1.0 (2003-03)
Part 2: Guidelines for the application of IEC 61511-1
Part 3: Guidance for the determination of the required safety integrity levels

Hollifield, B., Oliver, D., Habibi, E., & Nimmo, I. (2008). The High Performance HMI Handbook.

Hollifield, B., Habibi, E., (2010). The Alarm Management Handbook, 2nd Edition.

Hollifield, B., Perez, H., "High Performance HMI Principles and Best Practices Part 1 of 2" (2016)

Hollifield, B., Perez, H., "High Performance Case Studies, Recommendations, and Standards, Part 2 of 2" (2016)

About the authors

Mark Carrigan

Former Octave colleague

Mark was responsible for defining and implementing Octave's strategy for process safety and OT cybersecurity solutions. He previously served PAS Global – acquired by Octave – for 20 years in a variety of roles, including senior vice president of technology, managing director for the Middle East and Global Sales Leader, culminating as the company's chief operating officer and chief revenue officer. Prior to joining PAS, Mark spent 10 years with Air Products & Chemicals in several technical and commercial roles.

An industry veteran, Mark has extensive experience in international business, engineering, sales and technical consulting in the processing industries. He holds a Bachelor of Science degree in mechanical engineering from the University of Michigan.

Bill R. Hollifield

Retired Principal Alarm Management and HMI Consultant

Bill is a retired principal consultant responsible for the areas of both alarm management and high performance HMI. He is a member of the ISA SP-18 Alarm Management Committee, the ISA-SP101 HMI Committee, The American Petroleum Institute's API RP-1167 Alarm Management Recommended Practice committee and the Engineering Equipment and Materials Users Association (EEMUA) Industry Review Group.

Bill has multi-company, international experience in all aspects of alarm management and HMI development. He has 28 years of experience in the petrochemical industry in engineering and operations and an additional 18 years in alarm management and HMI software and services for the petrochemical, power generation, pipeline, pharmaceutical and mining industries.

Bill is co-author of The Alarm Management Handbook, The High Performance HMI Handbook and The Electric Power Research Institute (EPRI) Guidelines on Alarm Management for both Power Generation and Power Transmission.

Bill has authored several papers on alarm management and HMI and is a regular presenter on such topics in such venues as API, ISA and Electric Power symposiums. He has a BSME from Louisiana Tech University and an MBA from the University of Houston.

In 2014, Bill was made an ISA Fellow.

About Octave

Octave is a leader in enterprise software, turning data into decisive action and intelligence into your edge. Our software solves for and simplifies complexity, from the design and build to operations and protection of people, property, and assets– for any scope, at any scale. For decades, we've partnered with customers to sharpen performance, elevate efficiency, and amplify results. From factory floors to entire cities, our solutions are tuned to scale up what's possible from day one onward.