Addressing Common PSM Audit Findings
Part 1 – Operating/Safe Limits Tables[1]

James A. Klein, CCPSC, CPSA, and James R. Thompson, CPSA
ABSG Consulting Inc.

Introduction

Process safety audits [1, 2] are conducted for 2 main reasons: (1) feedback on process safety program implementation and effectiveness to identify potential improvement opportunities for improved performance and (2) compliance with process safety regulations such as OSHA 29 CFR 1910:119 Process Safety Management (PSM) and the EPA 40 CFR 68 Risk Management Rule (RMP). Some may even reverse this order, believing compliance is the primary purpose, both to meet the Compliance Audit element requirements of these regulations and also to help ensure other process safety elements are also in compliance.

If a facility has a process covered by these regulations, compliance audits must be conducted every 3 years. Since the OSHA rule was promulgated in 1992, this means that facilities in existence at that time have conducted 7-9 compliance audits. Newer processes obviously have had fewer audits, but a review of recent audit findings suggests certain issues continue to be commonly identified. This paper addresses some of the most frequent audit findings identified, specifically related to operating limits (required under the operating procedures element) and safe limits (required under the process safety information element). Guidance is also provided on how these findings on these topics can be avoided through appropriate development and implementation of limits tables. A typical audit finding is shown in Table 1.

Operating limits and safe limits tables are typically part of the process safety information (PSI) and operating procedures (OP). They are important because they define the ranges of safe operation for a process, both as operating limits in the OPs and as the ultimate safe (or design) limits in the PSI. Exceeding operating limits can cause process upsets, quality issues, and other problems. Exceeding safe limits will likely cause significant process incidents and result in possible equipment damage, personnel injuries, and environmental harm. Failure to properly document these limits can therefore lead to misoperation and significant operability and safety issues. The consequences of the deviations from these limits must also be documented, including the safety and health effects on personnel. The OPs must document correct operator responses to regain desired control of the process. Many companies choose to combine these sets of limits tables as part of the Ops for ease of reference and use, which while common, sometimes also becomes a source of confusion if the information is not clearly presented.

Based on our experience, having a complete, accurate, and thorough set of operating limits and safe limits tables available to process operators (particularly board operators) as well as engineers, maintenance, etc. is invaluable in (1) focusing them on the really important process parameters, (2) reminding them of the worst-case consequences associated with exceeding these parameters, and (3) providing a ready reference for actions to take when parameters are exceeded. Limits tables are therefore important training tools. Exceeding one flow rate may have minor consequences, but exceeding a different flow rate could lead to destruction of the plant. Knowing these differences and how to respond to these deviations are fundamental to safe design, operation, and maintenance of the plant.

We have also noted that many companies refer to “safe operating limits” (SOLs), which can also lead to confusion since the OSHA regulation refers only to safe limits and operating limits, as discussed. SOL likely

means that the operating limits have been set based on safety (rather than other) considerations, but SOLs should not necessarily be equated to safe limits. Auditors should understand company intent and practice relative to the OSHA PSM regulation to determine if requirements are met.

Requirements/Background

The OSHA PSM requirements for operating limits and safe limits are shown in Table 2, and guidance provided by OSHA to its Compliance Safety and Health Officers is provided in Tables 3 and 4. The requirements in the EPA RMP rule are basically the same. There are two basic approaches for meeting these requirements:

- The PSI and OP requirements are implemented separately, with the PSI safe limits tables providing the basic process variables to be addressed in the operating limits tables implemented in the OPs (see Figure 1).
- The PSI and OP requirements are combined into limits tables in the OPs (see Figure 2).

Both approaches as valid for meeting the regulatory requirements, but there are pluses and minuses to each approach if not implemented and maintained appropriately. For example, combined tables help reduce discrepancies that could develop over time in separate tables as process equipment changes occur. Combined tables are also periodically reviewed as part of OP reviews to confirm that they are current and accurate and therefore are also frequently part of refresher training activities. Improper design and implementation of combined tables, though, can lead to confusion around whether limits are safe limits, operating limits, or something else (e.g., control system alarm points). An example combined limits table is shown in Table 5.

Figure 1 – Separate safe and operating limits tables

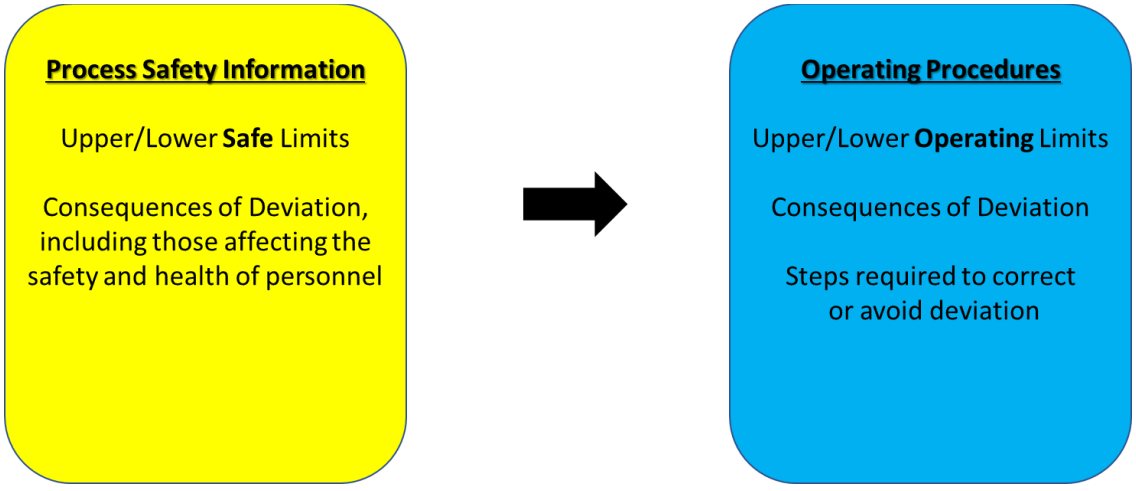


Figure 2 – Combined safe and operating limits table

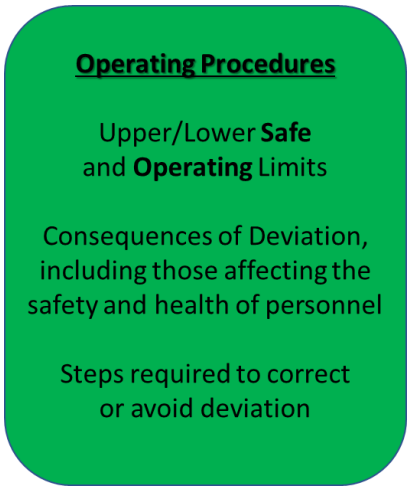


Figure 3 provides a typical way of thinking of limits. Most processes will have a normal operating zone, such as a temperature range from 100-120°C, based on safety, quality, and other operability considerations. This range is used to define the desired upper and lower operating limits. Deviations above or below the operating limits will result in troubleshooting activities by operators and/or automatic response by the control system to return to normal. Usually a response zone is defined before safe limits are exceeded, although the available response time may be very short. In some cases, there may be a buffer zone above the safe limits before worst case consequences can occur, but in many cases, the safe limit defines the point where undesirable safety consequences are possible without a buffer. Figure 4 shows these limits and the activation points for possible process safeguards for pressure in a reactor due to a runaway reaction, based on layers of protection as evaluated in a PHA.

Figure 3 – Zones of Operation (modified from [5])

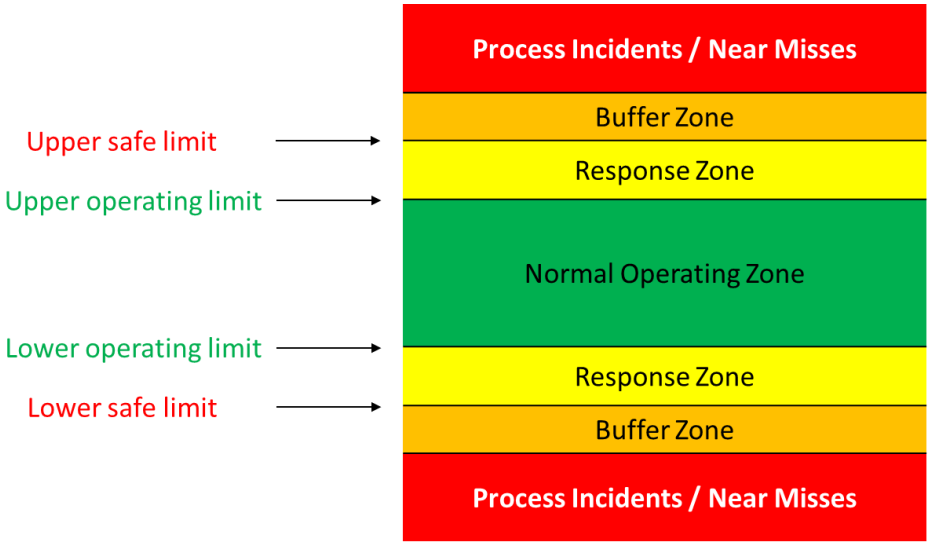
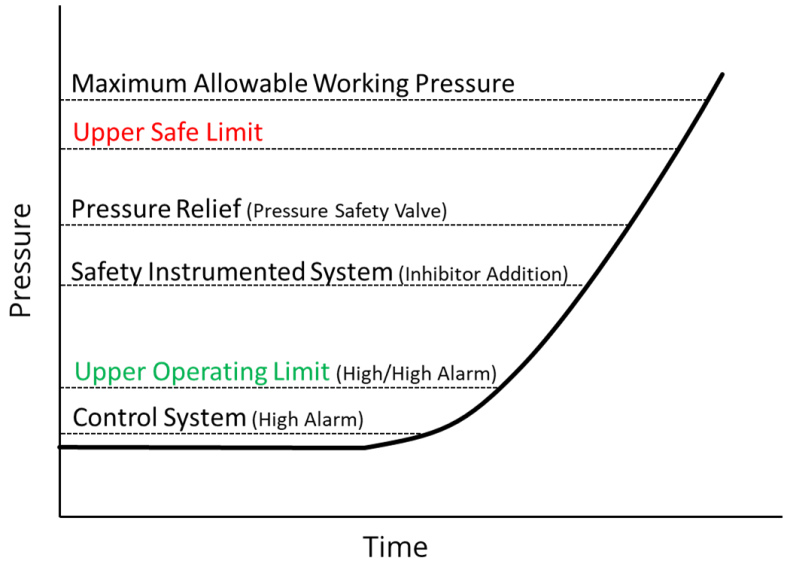


Figure 4 – Example Pressure Limits for a Runaway Reaction (modified from [6])



Common Issues Observed in PSM Audits

While the limits table requirements, as shown in Figures 1 and 2, seem relatively straightforward, there may be literally hundreds of limits that need to be documented for large processes. Critical variables may include temperature, pressure, flow rates, levels, and/or many other variables for each piece of process equipment. Developing this information can be a challenge, especially for older processes, due to limited availability of the PSI. With multiple requirements for developing, documenting, and maintaining limits, it is not surprising that process safety audits often identify compliance and/or improvement opportunities related to limits tables. Changing criteria or OSHA direction may also raise issues, even though previous audits did not identify issues. Following are examples of some of the common issues with operating/safe limits that we have observed in PSM compliance audits:

1. **Separate operating and safe upper/lower limits are not provided**

   As noted in the "Requirements/Background" section, the OSHA regulation and Good Industry Practice (GIP) clearly require/expect that each covered process will have two separate sets of limits:

   - operating limits , defining the boundaries outside of which a system upset or abnormal operating condition could occur.
   - safe limits, representing the design safe upper and lower limits of the equipment or process, above or below which it is considered unsafe to operate.

   However, we still observe that facilities:

   - establish only one set of documented "limits," rather than two sets, and it is often not clear whether they are operating or safe limits.

- establish operating limits in tables in the OPs, but have not included safe limits in these OP tables or in separate tables as part of the PSI. The reverse of this (i.e., establishing safe limits in tables in the PSI, but not operating limits in tables in the OPs) is less common.
- reference the alarm/interlock settings in the distributed control system (DCS) and the pressure safety valve (PSV) settings as providing their operating/safe limits.

In the first and second cases, there is clear non-compliance with the regulations, since both sets of required limits are not provided. In the third case, many DCS alarm settings are not established for safety reasons but are for quality or operability purposes. Therefore, defaulting to the DCS parameters may indicate the requirements of operating limits are not well understood. In some cases, listed safe limits may also be part of the tables but may be difficult to distinguish from quality limits, environmental limits, etc.

Guidance: Ensure that both operating and safe limits are provided in the PSI, OPs, or combined tables and (2) the limits documentation addresses the different zones of operation shown in Figure 3, as applicable. Also, avoid imprecise terminology when possible. See Table 5 for an example limits table that contains both operating and safe limits per regulatory requirements.

2. **All pertinent operating/safe limits are not addressed**

In some cases, inspection of the limits tables may suggest that some critical variables are missing (e.g., temperature in a reactor), leading to additional discussion with site personnel to understand (1) how the limits tables were developed and (2) why, in the case of high temperature in a reactor, the particular limits have not been established. Operating/safe limit tables for all the pertinent process parameters can be effectively evaluated (as time permits) by comparing the limits tables data to the current PHA for the process and other PSI documentation. This can be done by:

- reviewing the PHA report worksheets for parameter deviations leading to potential hazardous events (e.g., loss of containment) that are not addressed in the operating/safe limits. If high flow or high level in a HAZOP table, for example, is shown to lead to hazardous events in the PHA, then it would be reasonable that limits for these variables should be provided in the limits tables. Note: PHAs typically do not provide the actual limits. Use the PSI to find this information.
- reviewing listed safeguards in the PHA (e.g., alarms, interlocks, pressure safety valves) or a separate safeguards table (if available) to determine if the associated process parameters are included in the operating/safe limits table. If a high flow alarm or PSV is included as a safeguard, then it would be reasonable that limits for flow or pressure would be provided in the limits tables.
- reviewing PSI documentation for specific equipment to see if design limits have been correctly listed in the limits table.

Based on review of PHAs and other PSI documentation, we often find that a significant number of pertinent process parameters are not included in the operating/safe limits tables. From our experience, this situation often develops because the operations and engineering personnel developing/updating the limits tables perform this work independently, without ever looking at the operating/safe limits through the “lens” of the PHA reports or PSI documentation. Audits also provide an opportunity to review the “reasonableness” of the limits. If the limits table shows a

high pressure safe limit of 100 psig but the PSI and/or PHA shows the related PSV setpoint as 150 psig, further discussion to understand the difference is warranted.

Guidance: Review PHAs and other PSI documents to ensure that appropriate process variables are addressed in the limits table and that values appear correct. Clearly address both upper and lower limits and note as "not applicable" where there is no low/high limit. Also review relevant management of change documentation to see if limits tables have been updated as needed.

3. **Consequences of Deviation are not clearly documented**

The consequences of deviation beyond both operating and safe limits must be documented. For operating limits, simple descriptions, such as "process upset," or something similar are often listed, which does not adequately describe the possible consequences., It is frequently observed that the regulatory requires that the consequences of deviation from safe limits including those "affecting the safety and health of employees" is not addressed. Fundamentally, all of these consequences should match, or at least be similar, should be described in the PHA worksheets and should describe potential safety and health impacts on personnel, as well as impacts on processes and equipment. For example, the PHA and safe limits table for high pressure in a reactor might indicate overpressure leading to loss of containment and potential toxic exposure to a specific chemical(s) or fire/explosion hazards.

When auditing consequences of deviation, we often see:

- worst-case consequences are not adequately addressed (no column provided or left blank)
- the consequences say something like "leading to a high pressure interlock" or "lifting the PSV" rather than the potential worst-case consequence of overpressuring a vessel and loss of containment. Note that activation on of a PSV may also result in a hazardous release at the discharge point.
- safety and health effects on personnel are not documented, such as a toxic exposure hazard resulting from the release of a hazardous chemical
- safety consequences are mixed with operability/quality/environmental consequences.

Guidance: Review PHAs to ensure that consequences of deviation outside the safe limits are properly documented, including possible worst cases and potential safety and health effects on personnel. Clearly distinguish between operating/safe limits and quality, environmental, and other limits.

4. **Corrective actions are not clearly provided**

The steps required to avoid or correct deviation must be addressed in Ops, but this information is not always provided or corrective actions are provided for only some operating limits with varying degrees of clarity. Although the regulation does not specifically require the documentation of corrective actions for deviations from safe upper/lower limits, OSHA's guidance (see Tables 3 and 4) indicates that "emergency shutdown" should be a final corrective action. Obviously, the steps to correct a deviation outside operating limits will help prevent upset situations or safe limits from being exceeded, but the required actions are likely to be different as

a potential deviation approaches and/or exceeds documented safe limits. For example, operators are typically encouraged to safely shutdown a process when in doubt about continued safe operation; even before reaching an interlock/trip point or safe limit.

Guidance: Review PHAs, OPs, emergency procedures, and other documents as needed to ensure that clear guidance is provided on corrective actions for deviations outside of both operating and safe limits.

5. **Process safeguard setpoints are not included**

   As a best practice, it is valuable for operators to know at what point various process safeguards will activate as they potentially deal with process deviations. What alarms and interlocks are provided and when will they activate? What are the setpoints for pressure relief? This information may be included in the DCS, in the OPs, in training materials, and/or PSI documents. It is therefore desirable to consider adding this information to the limits tables to provide for immediate operator access relative to the defined limits listed in the table. For example, as shown in Figure 4, several safeguards for high pressure in a reactor are provided to activate as the upper safe limit is approached. Knowledge of these setpoints as operators respond to process deviations is important, both so the operators can anticipate safeguard action and so they can respond appropriately if the safeguard fails to activate as expected.

   Guidance: Consider including process safeguard setpoints in the limits tables as appropriate.

Summary

Well-documented operating and safe limits are an important foundation for safely and reliably operating processes that contain highly hazardous chemicals. Process safety regulations and industry best practices therefore require that limits, consequences of deviation, and corrective actions be clearly documented in OPs and PSI. Process safety audits, however, continue to find poor understanding and ineffective implementation of these requirements.

We hope that the information provided in this paper will help you better evaluate and improve your operating/safe limits documentation – before you receive a regulatory citation or compliance audit finding.

Jim Klein and Jim Thompson are process safety consultants with ABSG Consulting. Both are certified process safety auditors (CPSA) by the Board for Global Environmental, Health & Safety Credentialing. Jim Klein can be contacted at jklein@absconsulting.com.

References

1 Center for Chemical Process Safety, Guidelines for Auditing Process Safety Management Systems, 2nd Edition, John Wiley & Sons, 2011

2 Center for Chemical Process Safety, Guidelines for Risk Based Process Safety, John Wiley & Sons, 2007.

3 OSHA CPL 03-00-004 – Petroleum Refinery Process Safety Management National Emphasis Program

4 VPP Process Safety Management (PSM) Supplement B For Calendar Year 2011

5 Normal operating range reference (to be determined)

6 J. A. Klein and B. K. Vaughen, Process Safety: Key Concepts and Practical Approaches, CRC Press, 2017.

Table 1 – Typical limits table audit finding

Requirement	Audit Findings	Recommendations
[1910.119(d)(2)]. Information pertaining to the technology of the process. (i) Information concerning the technology of the process shall include at least the following: (D) Safe upper and lower limits for such items as temperatures, pressures, flows, or compositions; and (E) An evaluation of the consequences of deviations, including those affecting the safety and health of employees.	**PSI-1:** Based on a review of the "Safety Systems," "Operating Limits," and "Deviations" sections of several covered process SOPs, the following issues were noted: • Safe upper/lower limits are not provided for all parameters in the PHA with process safety consequences • Several of the SOPs reviewed did not provide consequences of deviation in the "Deviations" section • All of the SOPs reviewed listed "Operating Limits" that are not included in the "Deviations" section • The consequences of deviation (where provided) and corrective actions for the deviations generally cover these only for deviations outside operating limits, not for deviations outside safe upper/lower limits	**PSI-1-R:** Upgrade the coverage of operating and safe upper/lower limits by (1) ensuring that all parameters in the process PHA with process safety consequences are included in the "Deviations" section of the applicable SOP, (2) clarifying which SOPs are PSM-covered and which operating limits in the SOPs have process safety consequences, (3) documenting safe upper/lower limits associated with each SOP, and (4) consistently discussing/documenting the consequences of deviation (typically, loss of containment) and corrective actions (e.g., execute emergency shutdown) for deviations outside safe upper/lower limits.

Table 2 – Limits table requirements – OSHA 29 CFR 1910:119 PSM

1910.119(d) *Process Safety Information* 1910.119(d)(2)(i) Information concerning the technology of the process shall include at least the following: 1910.119(d)(2)(i)(D) Safe upper and lower limits for such items as temperatures, pressures, flows or compositions; and, 1910.119(d)(2)(i)(E) An evaluation of the consequences of deviations, including those affecting the safety and health of employees. 1910.119(f) *Operating procedures.* 1910.119(f)(1) The employer shall develop and implement written operating procedures that provide clear instructions for safely conducting activities involved in each covered process consistent with the process safety information and shall address at least the following elements. 1910.119(f)(1)(ii) *Operating limits:* 1910.119(f)(1)(ii)(A) Consequences of deviation; and 1910.119(f)(1)(ii)(B) Steps required to correct or avoid deviation.

Table 3 - Refinery National Emphasis Program (RNEP) Guidance [3]

Compliance Guidance: 1910.119(f)(1)(ii) requires that all written operating procedures include "operating limits". For NOP, the "operating limits" required are those operating parameters that if they exceed the normal range or operating limits, a system upset or abnormal operating condition would occur which could lead to operation outside the design limits of the equipment/process and subsequent potential release. These operating parameters must be determined by the employer and can include, but are not limited to, pressure, temperature, flow, level, composition, pH, vibration, rate of reaction, contaminants, utility failure, etc.

It is at the point of operation outside these NOP "operating limits" that EOP procedures must be initiated. There may be a troubleshooting area defined by the employer's EOP where operator action can be used to bring the system upset back into normal operating limits. During this troubleshooting phase, if an operating parameter reaches a specified level and the process control strategy includes automatic controls, other safety devices (e.g., safety valves or rupture disks) or automatic protection systems (e.g., safety instrumented systems/emergency shutdown systems), would activate per the process design to bring the process back to a safe state. Typically, once the predefined limits for troubleshooting have been reached for a particular operating parameter, the process has reached a "never exceed limit". A buffer zone is typically provided above (and below if applicable) the trouble shooting zone ("never exceed limit") to ensure the operating parameters do not reach the design safe upper or lower limit of the equipment/process ((1910.119(d)(2)(i)(D), require these design limits to be documented in the PSI). This design safe upper and lower limits of the equipment or process are also known as the boundaries of the design operating envelope or the limit above (or below) which it is considered unknown or unsafe to operate. Once the operating parameter(s) reach the buffer zone entry point, there is no designed or intentional operator intervention (i.e., troubleshooting) to bring the process system upset back to a safe state. Any intervention in the buffer zone is as a result of the continued activation of the safety devices and automatic protection systems which initially activated at the predefined level during the troubleshooting phase. All of these predefined limits are important information for operators to know and understand and must be included in the PSI and operating procedures.

As shown above, there is a distinction between the 1910.119(f)(1)(ii) requirement for listing the "operating limits" for the normal range of operating parameters and the design safe upper and lower limit of the equipment or process. Since it is necessary to define the design envelope which establishes how various conditions/operating parameters may vary within the safe upper and lower limits, but may not exceed those limits, 1910.119(d)(2)(i)(D) requires that the employer include the design operating envelope or the safe upper and lower limits for the operating parameters of the equipment or process in its PSI. (See e.g., CCPS [32], Chapter 6, Writing Emergency Operating Procedures and CCPS [40], Appendix 12B, Example of Critical Operating Parameters: Interpretation Guidelines). If the employer has not included the safe upper and lower limits for the design operating parameters of its equipment/process, CSHOs may cite 1910.119(d)(2)(i)(D.

Table 4 - OSHA's Voluntary Protection Program (VPP) Guidance [4]

11) Have the written operating procedures been audited to ensure they clearly identify all written operating limits? What prompts an audit team to review these operating limits?

Compliance Guidance: Reference standard 1910.119(f)(1)& .119(h)(3)(ii)

Did the PSM compliance audit review Normal Operating Procedures (NOPs) "operating limits"? The "operating limits" required are those operating parameters that if they exceed the normal range or operating limits, a system upset or abnormal operating condition would occur which could lead to operation outside the design limits of the equipment/process and subsequent potential release. These operating parameters must be determined by the employer and can include, but are not limited to, pressure, temperature, flow, level, composition, pH, vibration, rate of reaction, contaminants, utility failure, etc. It is at the point of operation outside these NOP "operating limits" that EOP procedures must be initiated. There may be a troubleshooting area defined by the employer's EOP where operator action can be used to bring the system upset back into normal operating limits. During this troubleshooting phase, if an operating parameter reaches a specified level and the process control strategy includes automatic controls, other safety devices (e.g., safety valves or rupture disks, or automatic protection systems (e.g., safety instrumented systems/emergency shutdown systems), these would activate per the process design to bring the process back to a safe state. Typically, once the predefined limits for troubleshooting have been reached for a particular operating parameter, the process has reached a "never exceed limit." A buffer zone is typically provided above (and below if applicable) the trouble shooting zone ("never exceed limit") to ensure the operating parameters do not reach the design safe upper or lower limit of the equipment/process. The design safe upper and lower limits of the equipment or process are also known as the boundaries of the design operating envelope or the limit above (or below) which it is considered unsafe to operate. Once the operating parameter(s) reach the buffer zone entry point, there is no designed or intentional operator intervention (i.e., troubleshooting) to bring the process system upset back to a safe state. Any intervention in the buffer zone is as a result of the continued activation of the safety devices and automatic protection systems which initially activated at the predefined level during the troubleshooting phase. All of these predefined limits are important information for operators to know and understand and must be included in the PSI and operating procedures. (See e.g., CCPS Guidelines for Writing Effective Operating and Maintenance Procedures, Chapter 6, "Writing Emergency Operating Procedures" and CCPS Plant Guidelines for Technical Management of Chemical Process Safety, Appendix 12B, "Example of Critical Operating Parameters: Interpretation Guidelines". Also reference CCPS Essential Practices for Managing Chemical Reactivity Hazards, Figure 4.5.)

Table 5 – Example Operating/Safe Limits Table

Instrument Tag	*Parameter (Process Variable)*	*Normal Operating Limits*	*Consequences of Deviation (exceed Normal Limits)*	*Corrective Action (Troubleshooting)*	*Interlocks*	*Safe limits Do Not Exceed*	*Consequences of Deviation (exceed Safe limits)*	*Corrective Action (exceed Safe limit*
TC-1700	OX-201 Temperature	Max: 95°C Min: 85°C	Max: Poor yield and increased side reactions; begin to approach runaway reaction Min: Loss of reaction and peroxide concentration in oxidizer is reduced; operability/quality issues	• Reduce air flow to oxidizer • Increase water flow to circulation cooler	TC-1200 will activate and (1) shutoff the air to the oxidizer and (2) open water valves to circulation coolers 100% if reading is above 105°C	Max: 120°C Min: N/A	High temperature leads to runaway reaction. Temperature increases quickly, resulting in a release of gas that may cause a fire/explosion hazard to personnel.	• Shutoff air to oxidizer. • Open cooling water valve to circulation coolers to 100%. Divert additional cooling water if needed. • Refer to procedure XX "Response to High Temperature in an Oxidizer" for further steps.
AI-1703AS AI-1703BS	OX-201 Offgas Oxygen Percent	Max: 9% Min: 4%	Max: Approach explosive atmosphere in the oxidizer Min: Poor yield and increased side reactions	• Increase temperature to the oxidizer by reducing water flow to the circulation cooler • Increase temperature to the oxidizer by increasing steam flow to the pre-heater • Increase temperature to the oxidizer by putting steam on the circulation cooler	AI-1203AS/BS will activate and shutoff the air to the oxidizer if reading above 15%	Max: 20% Min: N/A	Explosive atmosphere is present in the oxidizer, resulting in fire/explosion hazard to personnel if an ignition source is present.	• Shut-off air to the oxidizer. • Open nitrogen valve to the oxidizer vapor space. • Increase oxidizer temperature before putting air back on the oxidizer.