

From Theory to Practice: Implementing Safe Operating Limits in Major Hazard Facilities

Karthikganesh Senthilvelan ^{a,b} Salim M., Shaik ^{b,c} Wee Chin Wong ^b David Sugiman^a

^a Asahi Kasei Synthetic Rubber Singapore Private Limited, 1 Angsana Drive, Jurong Island, Singapore 627586, Singapore

^b Department of Food, Chemical & Biotechnology, Singapore Institute of Technology, 10 Dover Drive, Singapore 138683, Singapore

^c Institute of Sustainability for Chemicals, Energy, and Environment (ISCE2), Agency for Science, Technology and Research (A*STAR), 1 Pesek Road, Jurong Island, Singapore 627833, Singapore

Abstract

Defining safe operating limits of critical operating parameters, reviewing its validity periodically, and recording its exceedance (if any) are vital for safe operation of the chemical plant, especially for Major Hazard Installations. Despite this, users often encounter challenges such as: (a) difficulty in accurately identifying their limits, (b) uncertainty in the process of determining appropriate limits, and (c) setting limits too close to or too far from the normal operating or mechanical design thresholds of the equipment. This in turn would lead to reduced operational flexibility of the equipment or increases safety concerns due to insufficient margins. This paper briefly discusses lessons learnt from industrial accidents related to safe operating limits, how safe operating limits are linked to regulatory assessments, challenges in defining appropriate limits and methodology for establishing them.

KEYWORDS: safe operating limits, critical operating parameters, independent protection layers, process safety time, design limits, process safety management

1. Introduction

Safe Operating Limits (SOL) are minimum or maximum values of Critical Operating parameters (COP) within which a system can safely function. COP refers to process parameters such as pressure, temperature, flow, and concentration that significantly impact safety and performance. SOLs are established only if it is physically possible to exceed the limit and if exceeding the limit could lead to a catastrophic failure of process equipment or loss of containment. The determination of safe operating limits occurs during Process Hazard Analysis (PHA), Management of Change (MOC), regulatory assessments. One of the challenges in determining SOLs is setting them too close to normal operating limits leading to operational inflexibility, on the other hand, setting SOLs close to mechanical design limits would raise concerns of not having enough safety margins. Anecdotaly, although the engineers who designed the plant should provide values for the safe operating limits, in many cases they fail to do so. Furthermore, if the facility is more than a few years old, it is likely that the current operations sub-optimum from the original design and the original values may no longer be applicable ([Process Safe Limits: Defining Safe Limits Quantitatively, n.d.](#)) This paper aims to provide a brief discussion on past industrial accidents resulting from the absence or inadequate management of safe operating limits. It examines various industrial methodologies used for their determination, as well as internationally recognized guidelines such as those established by the International Society of Automation, the American Petroleum Institute, and the Center for Chemical Process Safety. Additionally, the paper reviews regulatory requirements, including those set by the Occupational Safety and Health Administration, Safety Case regulations, and the Environmental Protection Agency. Furthermore, it assesses current industry practices and proposes a systematic approach for defining and maintaining safe operating limits in major hazard installation.

2. Safe Operating Limits associated with Major Hazards

If a change in an operating parameter, such as pressure, temperature, flow, or level, could lead to a process safety issue such as overpressure, vessel overflow, or the loss of containment of hazardous substances then this parameter is known as a Critical Operating Parameter. In such cases, it is essential to determine a Safe Operating Limit (SOL), that represents the value not to be exceeded as well as serves as a threshold for initiating corrective action. The establishment of Safe Operating Limits (SOL) in Major Hazard Installations (MHI) is based on the fundamental principle that if an operating parameter exceeds the SOL, it can lead to catastrophic failures, including equipment damage or loss of containment. Conversely, if the parameter falls below the lower SOL, it could cause process instability, inefficiency, or unintended reactions, all of which could comprise safety. Therefore, facilities need to identify SOLs and assess the consequences of deviation, determine process recovery to a safe state and determine adequate control measures to protect the plant against excursions beyond design conditions.

Major hazard installations (MHI) in Singapore are required by the Workplace Safety and Health (MHI) Regulations as part of their Safety Case Regime, to have a system for determining, recording, and reviewing Safe Operating Limits showing adequate control measures have been provided to protect the plant against excursions beyond design conditions. In the United States, Safe Operating Limits are governed by the Occupational Safety and Health Administration's Process Safety Management (OSHA-PSM) regulation 29 CFR 1910.119 ([Process Safety Management of Highly Hazardous Chemicals, 2015](#)). This regulation mandates the identification of critical operating parameters, ensuring they are properly managed to prevent process safety incidents. Additionally, API RP-754 ([Process Safety Indicators for the Refining and Petrochemical Industries, 2021](#)) classifies SOL exceedances as Tier 3 Process Safety Management Leading Indicators, meaning they serve as early warning signs of potential process safety issues that require corrective actions. In other regions, similar frameworks exist, such as the UK's Control of Major Accident Hazards (COMAH) regulations and the EU's Seveso directive.

3. Lessons learned from Industrial accidents

This section analyzes four industrial accidents, highlighting key contributing factors, failures in Safe Operating Limits (SOLs) and Critical Operating Parameters (COPs), and the lessons learned. By identifying deficiencies in SOL implementation and management, these incidents provide valuable insights into improving SOL determination, process control, operator response, and emergency preparedness. The findings emphasize the need for robust methodologies and clear guidelines to ensure proactive risk management in industrial operations.

Impact of Incorrectly Established Safe Operating Limits

	Details
Incident Date & Location	May 18, 2018, Kuraray America, Pasadena, Texas
Source	CSB Investigation Report (Dec 16, 2022)
Incident Type	Ethylene release and fire
Number of Injuries	23 workers injured
Cause of Incident	High-pressure conditions developed inside the reactor during startup, leading to ethylene release and ignition.
Key Contributing Factors	• Safe Operating Limit (SOL) set too high at 740 psi (matching mechanical design limit). • Emergency pressure-relief system activated at 719 psi, releasing ethylene into the atmosphere.

S. Karthik et al. / Safe Operating Limits: From theory to practice

	- Company's SOL was documented in spreadsheets but not integrated into operations. - Operators had no early intervention opportunity before reactor's emergency pressure relief activation
Reactor Pressure Settings	- Target Operating Pressure: 595 psi - High-Pressure Alarm: 620 psi - High-High Pressure Alarm: 640 psi - Emergency Pressure-Relief Activation: 719 psi - Safe Operating Limit (SOL) Set At: 740 psi (too high)
Lessons Learned from Incident	The company's Reactor involved in the incident had unclear operating limits, with a safe operating limit set too high at 740 psi, instead of a lower actionable threshold like the High-High Pressure alarm at 640 psi. This lack of clear guidance prevented operators from taking timely corrective actions, leading to an uncontrolled pressure rise and the Incident. The CSB concluded that the company could have prevented the incident by, - Defining robust safe operating limits - Incorporating SOL and its response actions in its procedures - Effectively training its operators to take the appropriate, predetermined actions at the high-high pressure alarm condition

Absence of defined Safe Operating Limits and predefined actions for Standby mode

	Details
Incident Date & Location	February 18, 2015, ExxonMobil, Torrance, California
Source	CSB Incident Report (May 2017)
Incident Type	Electrostatic Precipitator (ESP) explosion in Fluid Catalytic Cracking (FCC) unit
Number of Injuries	No Injuries
Cause of Incident	Pressure deviation caused hydrocarbon backflow, leading to ignition inside the ESP during maintenance preparation.
Key Contributing Factors	- No established Safe Operating Limits (SOL) for FCC unit operation in Safe Park mode (standby mode). - No defined process conditions requiring unit shutdown. - Reliance on indirect measurements for reactor pressure balance and catalyst barrier development. - Steam flow reduction caused reactor pressure to drop below the safe level
FCC Unit Pressure Controls	- Minimum Steam Flowrate: 2000 pounds/hour (relied upon maintaining reactor pressure) - Accumulated Catalyst Level above closed SCSV position (used as an indirect indicator of catalyst barrier presence).
Lessons Learned from Incident	- Establish Critical Operating Parameters (COP) relevant to Safe Park mode and set Safe Operating Limits accordingly - Define Low Differential Pressure between reactor and main column as a direct indicator of pressure imbalance. - Define Minimum Differential Pressure or Minimum Catalyst Bed Level with corrective actions upon exceedance (e.g., triggering a full unit shutdown)

	Develop procedures specifying Safe Operating Limits (SOL) for all modes of operation, including consequences of deviations and pre-determined corrective actions.
--	---

Failure to enforce Safe Operating Limits and poor management of its exceedance

	Details
Incident Date & Location	January 21, 1997, Tosco Avon Refinery, California,
Source	EPA Incident Report (November 1998)
Incident Type	Fire and explosion in hydrocracking unit
Number of Injuries	1 fatality, 46 people injured
Cause of Incident	Rupture of effluent piping due to excessively high temperatures (>760°C) in Hydrocracker Stage-2 reactor, leading to the release and autoignition of flammable hydrocarbons and hydrogen.
Key Contributing Factors	- Failure to Depressurize and Shutdown the Reactor: Operators did not follow procedures to shut down when temperature exceeded 425°C - Inconsistent Temperature Limits: Temperature limits in written procedures were conflicting, leading to confusion - Past Temperature Excursions Normalized: Previous reactor temperature excursions above 425°C were not addressed, leading operators to believe deviations were acceptable - Lack of Management Oversight: Management did not enforce corrective actions or investigate past temperature deviations - Insufficient Operator Training: Operators were not fully aware of the risks of exceeding temperature limits or the importance of following corrective actions.
Reactor Temperature settings	- Maximum Safe Reactor Temperature: 425°C (as per procedures) - Actual Temperature at Failure: >760°C - Temperature Excursion Origin: Began in bed 4, spread to bed 5 and effluent pipe
Lessons Learned from Incident	- Strict Adherence to Safe Operating Limits (SOL): Facilities must enforce and follow safe temperature limits - Clear & Consistent Procedures: Operating procedures should have well-defined, non-conflicting limits for temperature control - Proper Investigation & Implementation of Corrective Actions: All temperature excursions must be investigated, and recommendations must be followed - Operator Training & Awareness: Operators must be regularly trained on safe limits, risks of exceeding them, and required corrective actions - Adequate Time & Systems for Operator Response: Facilities must ensure safe operating limits allow enough time for operator intervention before unsafe conditions develop

Inadequate Control of Reaction Temperature Limits and lack of corrective actions

	Details
Incident Date & Location	April 08, 1998, Morton International, New Jersey
Source	CSB Investigation Report (August 16, 2000)
Incident Type	Explosion and fire due to runaway reaction
Number of Injuries	9 people injured
Cause of Incident	A runaway reaction led to overpressure in a 2000-gallon reactor vessel, releasing flammable material that ignited.
Key Contributing Factors	• Reaction was initiated at a temperature higher than the prescribed limit • Steam to the jacket was open too long, and cooling water was not initiated soon enough • High temperatures triggered a secondary runaway decomposition reaction • Operators manually controlled temperature using steam and cooling water valves • Operating procedures required running at temperatures (150-153°C) dangerously close to the uncontrollable reaction onset temperature (195°C) • Previous temperature excursions in 8 out of 32 batches were not investigated • No corrective actions were taken in response to these temperature deviations • Operating procedures did not include safety consequences of exceeding SOL or corrective steps
Process Temperature settings	• Normal Reaction Onset Temperature: 38°C • Rapid Reaction Temperature: ~75°C • Standard Operating Temperature: 150-153°C • Uncontrollable Reaction Onset Temperature: 195°C
Lessons Learned from Incident	• Robust operating procedures (batch sheets) must be established for reactive chemical processes • Procedures should describe the consequences of exceeding safe operating limits and define corrective and emergency actions • Training programs should reinforce the importance of process safety in reactive chemical operations • To document, investigate, and address process deviations that could lead to safety incidents.

A review of industrial incidents underscores a common failure, i.e., poorly defined Safe Operating Limits (SOLs) during design and lack of management during operation, leading to preventable safety breaches. Key Lessons Learned:

- SOLs must be set at proactive thresholds to enable timely operator intervention
- Critical Operating Parameters (COPs) should be direct measurements (e.g., differential pressure, catalyst bed level) and integrated into safety controls
- Operating procedures must outline SOLs, consequences of deviation, and corrective actions for all operating modes (including stand-by mode)
- Operator training should reinforce consequences of deviation and intervention strategies
- Must apply robust Incident investigations upon SOL exceedance to prevent recurrence

4. Background of determining Safe Operating Limits

Industry guidelines and methods are widely inconsistent ([Stauffer & Chastain-Knight, 2021](#)) and different industrial sectors seem to adopt a different basis such as based on equipment mechanical design limits, mechanical integrity limits, process dynamic consideration, alarm or instrumented protective system set points or a combination of the above. The Normal Operating Limit (NOL) defines the minimum and maximum values of a critical operating parameter within which normal operations occur. If this limit is exceeded, an alarm is triggered, allowing operators time to adjust and restore normal conditions. This is illustrated in Figure-1 as the troubleshooting zone. The Safe Operating Limit (SOL) represents the absolute boundaries for safe operation. If exceeded, an alarm or automatic trigger initiates immediate operational or mechanical corrective actions to bring the equipment and process units to a safe state ([American Institute of Chemical Engineers Inc., 2012, Pg.135-137](#)). The process is not allowed to intentionally operate beyond this limit. Mechanical Design Limit (MDL) refers to maximum temperature, pressure, and other physical parameters that a piece of equipment can withstand without experiencing failure or damage. This normally acts as a limiting factor for determining SOL.

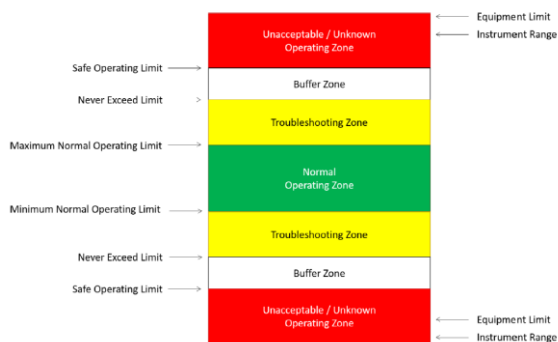


Figure 1: illustration of zones by engineering design for process safety

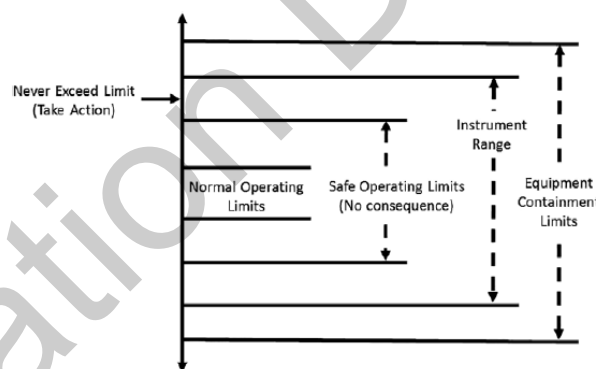


Figure 2: Operating range and limits adopted from Inherently safer chemical process

Low and high alarms are set at boundaries of normal operating zone, whereas Low-Low and High-High might be set in the troubleshooting zone. A Safety Instrumented System (SIS) trip might be set beyond the SOL to prevent the consequence ([Forest, 2018, Pg.498–501](#)). Inherent safer designs ensure that the normal or quality operating limits are well within safe operating limits, that the limits are well within the instrumentation range, and that the instrumentation range are well within the equipment containment limits ([American Institute of Chemical Engineers Inc., 2008, Pg.103-105](#)). Processes having wide safe operating limits are inherently safer than those having narrow ones ([Dowell, 2001, Pg.208-214](#)).

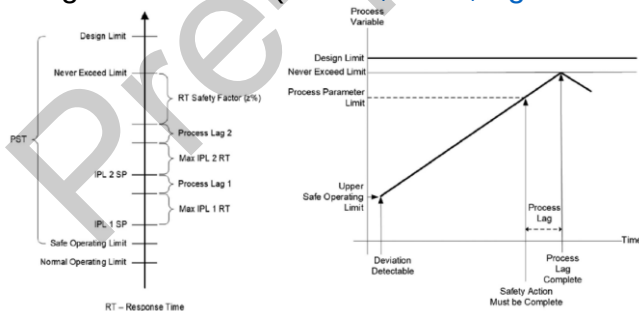


Figure 3: SOL in relation to design limit, NEL, and IPL setpoints (ISA-TR84)

A new ISA-TR84.00.04-2019 (Part-1: guidelines for the Implementation of ANSI/ISA-61511-1-2-18, 4th edition, Rev D) suggests SIS trip points (shown as IPL 1 SP or IPL 2 SP in Figure-3) would typically be set above the safe operating limit, but below the never exceed limit (NEL) - closest approach value to design limit, allowing for operational and asset integrity uncertainties and design limits (DL). It also shows how process safety time (PST), Response Time (RT), and Process Lag relate to these limits ([Stauffer & Chastain-Knight, 2021](#))

Safe operating limits are determined by identifying design limits of equipment within a system, considering most limiting elements ([American Institute of Chemical Engineers Inc., 2007, Pg.476-477](#)). For new equipment, specification of safe operating limits based on design criteria is

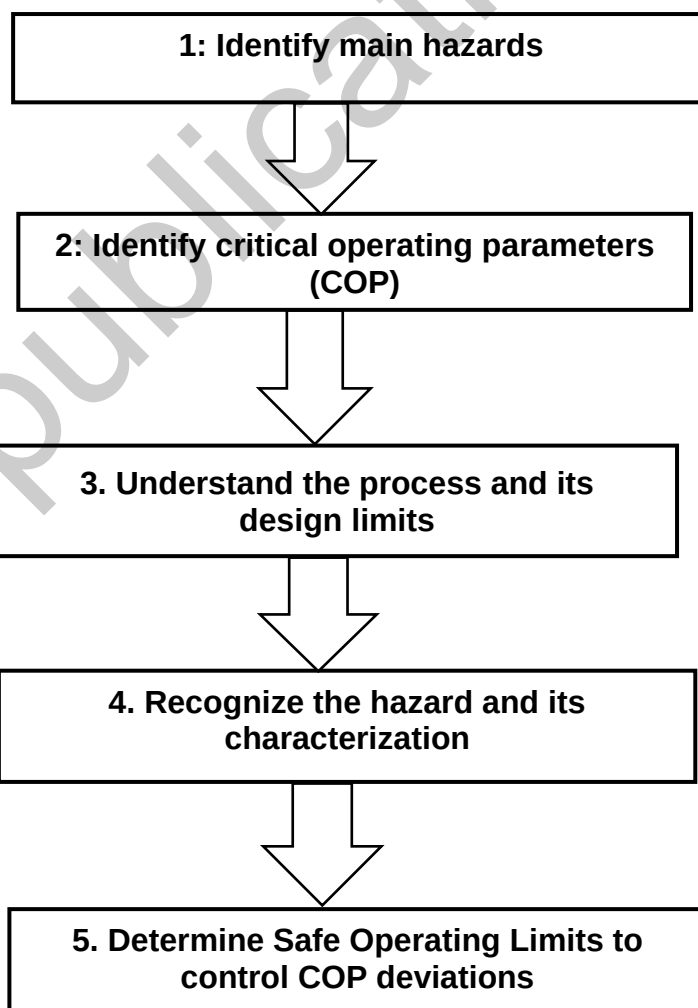
appropriate. Nevertheless, as time passes, the equipment can lose mechanical integrity and then can no longer conserve its original design limits. For example, corrosion could reduce the thickness of a piping's wall and the equipment could go out of service or be operated under reduced operation conditions. Thus, a program on mechanical integrity, specifically the test and inspection are fundamental to assure the safe operating limits are still applicable (De La Cruz-Guerra & Javier Cruz-Gomez, 2002, Pg.115-117). When design values are not provided, current techniques used by existing facilities are Industry Information, Operating experience, extrapolation, mathematical modelling, nudging. Among this, operating experience is probably the most-widely used methods (Sutton, 2011). The Set pressure of pressure relief device should be considered wherever applicable and process safety time that factors speed of the development of the scenario, response time and lag of to be considered in determining safe operating limits.

5. Recommended Approach and Methodology

Good practices for determining safe operating limits shall include clear and consistent guidelines and definition of terms to understand how they relate to other protection layers, also this consistent application is vital to major hazard installations and is integral to their use as effective leading indicator. Now, we will look at the proposed methodology in-principle for determining safe operating limits and we believe this can be applied to atleast all major hazard installations at the minimum. This methodology, as it has been tested so far seems to be useful that has the flexibility and simplicity needed to address at least some of the challenges mentioned before.

Main Inputs

- ✓ Existing safety reports and risk assessments,
- ✓ HAZID, Safety Concept, Compliance analysis
- ✓ Process Safety Information, HAZOP/-PHA, operating procedures,
- ✓ industry standards, regulatory agencies
- ✓ Table workshop with multi-disciplinary team
- ✓ equipment data sheets, process manuals, process safety information, functional data specifications, safety critical system
- ✓ consequence modelling and effects distances
- ✓ process dynamics, reaction hazards and calorimetry studies
- ✓ Output from step-3 & 4
- ✓ Plant historical experience of process deviations/-incidents
- ✓ Corrective actions



Main Outputs

- ✓ List of Major hazards
- ✓ Major accident events
- ✓ List of COPs
- ✓ Safety Critical equipments
- ✓ SOL basis, SOL pre-alarms
- ✓ List of controls/-actions to avoid SOL deviation
- ✓ List of safeties/-actions to avoid design excursions
- ✓ Severity of consequence of deviation
- ✓ Process safety time
- ✓ onset temperature, heat of reaction/-decomposition, pressure & TMR
- ✓ List of raw-SOL values
- ✓ List of predefined actions to correct deviations or avoid design excursions

S. Karthik et al. / Safe Operating Limits: From theory to practice

Step-1-Identify main hazards

Identification of main hazards could be extracted from existing safety reports/-cases or relevant risk assessments. However, in the case of a new facility where such documents do not yet exist, the determination of Safe Operating Limits (SOL) should be scheduled to start once the main hazards become clear. This step is likely to involve consultation with process safety specialists, site personnel and authors of risk assessments, to ensure that all correct and most up-to-date documentation has been received, and that the identification of major hazards is comprehensive. The resulting list of higher risk units should be the starting point to identify Critical Operating Parameters (COP) in Step-2.

Step-2-Identify critical operating parameters (COP)

Critical Operating Parameters (COP), such as level, pressure, temperature, concentration, flow, and other process variables that have the potential to cause unacceptable risk to health, safety and environment or property damage are typically determined through a combination of engineering analysis, process hazard analysis, industrial standards, and experience. Process Safety Information, which includes documentation related to the design, operation, and hazards of a process, is one of the valuable sources. Standard Operating Procedures (SOP) and Process Hazard Analysis (PHA) are other valuable resources where COP is discussed widely when operating parameters upon process or human deviations could lead to accidents.

Step-3-Understand the process and its design limits

SOL workshop to be conducted with multidisciplinary team to review and confirm Mechanical Design Limits (MDL), which defines SOL basis and operating beyond this range (high and low) is potential for catastrophic failure of process equipment and loss of containment. Then, Normal Operating Limit (NOL) and controls/-monitoring ways to maintain operating parameter within NOL, which defines SOL pre-alarm and operating beyond this range (high and low) is potential for SOL deviation, steps that are predefined/-taken to avoid such deviation. Lastly, Safety alarm and interlocks serve as part of the Independent Protection Layers (IPL), providing predefined automatic or operator-driven actions to correct deviations in a timely manner and prevent excursions.

Step-4-Recognize the hazard and its characterization

Study of consequence of deviation is necessary for operator knowledge and awareness to know the potential severity and risk associated upon exceeding any safe operating limits or design limits. Study of Process Safety Time (PST) would help to estimate the time interval between the initial failure in a process and the occurrence of a hazardous event if no mitigating actions are taken. It represents the available window for operators or automated systems to respond before the situation escalates into a loss of containment, fire, explosion, or other hazardous consequences. The Key factors that affect PST are Process dynamics, System Inertia, Instrumentation and alarms, Operator and control system response. By integrating PST analysis into the determination of SOLs, industries can ensure (a) response actions are activated in time to prevent hazardous events; (b) Optimize alarm and shutdown thresholds based on escalation speed; (c) balance automation and human intervention based on response feasibility.

Step-5-determine safe operating limits to control COP deviations

Based on the results obtained from Step 3 (SOL basis, SOL Pre-alarm) and Step 4 (Process Safety Time), safe operating limits (SOL) can be determined by considering response actions, estimated time required for operator response (detection, diagnosis, and reaction) and the overall

process response time. The SOL should be set such that the total response time remains within the estimated process safety time, ensuring adequate protection of equipment from excursions beyond acceptable limits.

The initial SOL value, derived from theoretical analysis and preliminary testing, serves as a reference point. However, it must be validated under actual operating conditions and continuously monitored for opportunities to expand its operating window. For instance, adjustments may be made to shift SOL within a safe range or modify predefined actions based on process behavior and operational needs.

6. Case Study- Safe Operating limit in Flammable Storage

Step-1: Identify Main Hazards

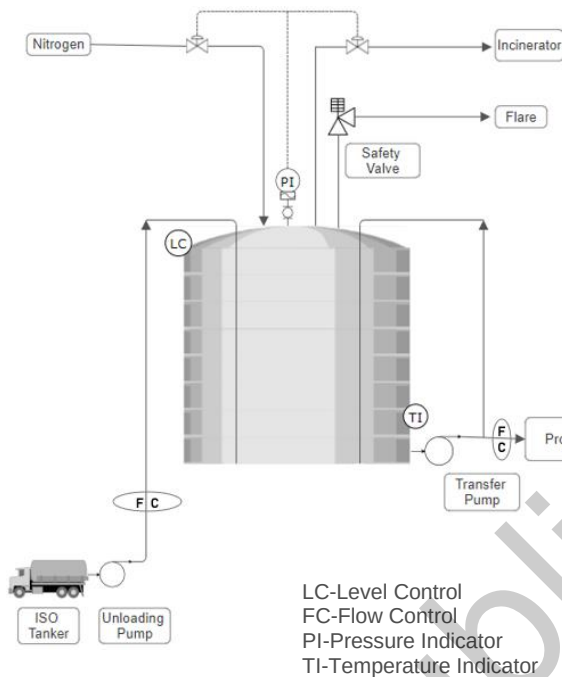


Figure 4: Flammable Storage Tank

Identification of main hazards could be extracted from existing safety reports/-cases or relevant risk assessments. In the context of MHIs, it should minimally cover all the major hazard units. Some of the examples can be ISO-containers handling dangerous substances, Flammable Storages, steam distillation columns, polymerization reactors. In this paper, we will go through a case study of **flammable storage** to illustrate steps for determining SOLs. The stored substance is highly flammable. To keep it outside the flammable range, nitrogen blanketing is used with split-range control. Significant pressure variations occur inside the storage tank, unlike atmospheric storage, particularly during receiving and transfers. A pressure safety relief valve is connected to the flare to manage excess pressure. The tank receives material from an ISO tanker or pipeline and transfers it to a buffer tank or process.

Step-2: Identify Critical Operating Parameters

To systematically identify COPs, it is recommended to map the major accident scenarios with their corresponding COP and SOL. Likewise, we can list down all the causes that may lead to major accident scenarios associated with storage tank during receiving, storage and transfer and map it up with relevant COPs (eg., level).

Table 1: Critical Operating Parameter of Flammable Storage (Level)

Cause	Scenario	COP	SOL
LC-fails low/-FC-fails high during receiving	Overflow of tank	Level	High
LC-fails high during transfer	Transfer Pump Cavitates	Level	Low

LC-Level Control; FC-Flow Control

Here, we identified **overflow** scenario for the storage tank upon initiating cause of LC fails low and/or FC fails-open and **pump cavitate** scenario upon initiating cause of LC-fails high that leads

S. Karthik et al. / Safe Operating Limits: From theory to practice

to identification of 'Level' as one of the critical operating parameters with corresponding 'high' and 'low' limits (SOL) to be set to prevent the unwanted overflow event.

Step-3: Understand the process and its design limits

Now in step-3, we need to understand the process to determine the basis of SOL, normal operating limits (NOL), existing control philosophy, NOL value and corrective actions to avoid any excursion beyond design conditions.

Table 2: Process and Design limits of Level (High) of Flammable Storage

COP, unit	High/Low	SOL Basis	Consequence of deviation	Control/-Monitoring	NOL Value	Steps to avoid design excursion	MDL Value
Level, %	High	Maximum liquid level is 100% level of storage	When the tank is full of liquid, potential for overflow, loss of containment	LC: 30-70% transfer XV closes based on 30% of transfer tank & 70% of receiving tank	80% level	LH: 80% Verify level through LG; decrease FC opening; short-stop to bring-down level	100% level
			Exceeding incoming rate would potentially lead to overflow, loss of containment	FC: 20-25 m³/hr FIC controls this rate to maintain 30-70% level in storage			

LH-Level High; LG-Level Gauge; XV-On/off Valve; MDL-Mechanical Design Limits

Step-4: Recognize the hazard and its characterization

Step-4 comprises of two sub-steps: (i) Study the consequence of deviation and document its potential severity for operator awareness. If severity information is already available from safety reports for the same deviation, it can be leveraged for operating procedures. However, if such information is unavailable, it becomes necessary to assess and document the consequences using techniques like consequence modeling. In this case, severity is assumed to be 'Catastrophic' based on the effects distance calculation and the number of people exposed within the harm footprint; (ii) Assess the process safety time (PST) between the point of failure and the occurrence of a hazardous event, as detailed in Step 4 of the methodology. The time required for the tank to overfill due to different initiating causes, such as LC failure in the low position and FC failure in the open position, is calculated as follows,

For LC-fails low:

- **A:** Total Tank Volume (assume 100m³)
- **B:** Incoming flowrate (assume 25m³/hr, limited to FCV opening)
- **C:** Tank recirculation flowrate (if any) (assume 5m³/hr)
- Time required: $A/(B-C) = 30 \text{ mins}$

For FC-fails open:

- **A:** Total Tank Volume (assume 100m³)
- **B:** Incoming flowrate (assume 40m³/hr, limited to pump capacity)
- **C:** Tank recirculation flowrate (if any) (assume 5m³/hr)
- Time required: $A/(B-C) = 17 \text{ mins}$

To calculate the time required for the tank to overfill in the event of an LC (Level Control) failure in the high position, the incoming flow rate is determined by the flow control valve opening limit. However, in the case of an FC (Flow Control) failure in the open position, the incoming flow rate is constrained by the pump's maximum capacity, as the flow control valve is assumed to fail open.

S. Karthik et al. / Safe Operating Limits: From theory to practice

As previously mentioned in step 2, by identifying the exact initiating cause of failure, we can determine the worst-case process safety time globally, rather than basing it on a single failure cause that may not represent the worst-case scenario. In this case, the worst-case process safety time is 34 minutes from 80% tank level (NOL value) to 100%, during which the operator can troubleshoot and restore normal operations and **17 minutes for the level to rise from 90% to 100%**, leading to overfill. This data must be considered when establishing Safe Operating Limits (SOLs) in the next step.

Step-5-Determine safe operating limits to control COP deviations

In this final step, we consider the results from step-3 and step-4 results to determine the safe operating limits for flammable Storage **level-high as 90%** with the corrective action of Automatic closure of shut-down valve to storage as shown in Table-3.

Table 3: SOL Table of Flammable Storage Level (High)

COP, unit	High / Low	SOL Basis	Consequence of deviation	Sev	Control/-Monitoring	NOL Value	Steps to avoid SOL deviation/-design excursion	SOL value	Steps to correct deviation or to make safe	MDL Value
Level, %	High	Maximum liquid level is 100% level of storage	When the tank is full of liquid, potential for overflow, loss of containment	C	LC: 30-70% transfer XV closes based on 30% of transfer tank & 70% of receiving tank	80% level	LH: 80% Verify level through LG; decrease FCV opening; short-stop to bring-down level	90% level	LSH: 90% (SIS-ESD) Automatic closure of inlet SDV to storage LSH-Level Safety High; SDV-Shut-down valve; SIS-Safety Instrumented System; ESD-Emergency Shutdown	100% level

The High SOL value for the level is set at **90%**, based on:

- An estimated process safety time of **17 minutes**, considering the worst-case scenario between LC failure in the low position and FC failure in the open position, to reach the MDL value (100%)
- The assumption that the combined operator response time (detection, diagnosis, and action) and process response time (deadtime and reaction time) is less than the estimated process safety time.

Likewise, to determine the Safe Operating Limit (SOL) for low level, we first assess the minimum tank level required to prevent pump dry-run or cavitation, which may not be 0% but rather the minimum level required in tank to prevent dry run or cavitation. Like high-level SOL, the normal operating limits (NOL) and control philosophy remain unchanged, but the NOL value differs at 25%, with corrective actions adjusted accordingly. Key factors in this assessment include tank volume (100m³), incoming flowrate (25m³/hr, limited to FC opening of transfer pump in Figure-4), recirculation rate (if any, assume 5m³), tank height (10m), suction line height (0.5m), required NPSH (0.5m), and based on this estimated minimum fluid volume needed to prevent dry run is 10%. Given the provided data, the process safety time is 22 minutes from 25% (NOL value) and 10 mins from 15% to reach 10% of tank level. Subsequently, we set SOL at 15%, with the corrective action of triggering automatic suction XV closure and pump shutdown to prevent pump cavitation. Below is the summary of operating limits of 'level' and its corrective actions upon exceedance for flammable storage to be included in the operating procedures,

Table 4: Summary of Operating Limits (Flammable Storage-Level)

COP	SOL basis	Consequences	NOL/-SOL		Corrective Actions	Time*
Level %	Maximum liquid level is 100% level of storage	When the tank is full of liquid, potential for overflow, loss of containment	90%	SOL-High	Automatic closure of inlet SDV to storage	17 mins
			80%	NOL-High	Verify level through LG short-stop to bring-down level	17 mins
	NA	Normal Operation	30-70%	NOL	NA	NA
	Minimum level required to prevent dry run of Pump (10%)	Potential for dry running of Pump, cavitation, risk of loss of primary containment	25%	NOL-Low	Verify level through LG; slowly decrease discharge rate; restore receiving/-top up to tank	12 mins
			15%	SOL-Low	Automatic stoppage of transfer pump and close suction SDV	10 mins

* Time available between different stages (eg., NOL-High to SOL-High and SOL-High to MDL)

In the same manner, we shall identify other COPs of Flammable Storage (pressurized and atmospheric) by mapping major accident scenarios with relevant COP and SOL as follows,

Table 2: Other Critical Operating Parameter of Flammable Storage

Cause	Scenario	COP	SOL
PI-Fails low/-Vent fails close during storage	Tank Overpressure	Pressure	High
PI-Fails high/-Nitrogen fails close during storage	Tank Collapse	Pressure	Low
TI-fails low during storage	Thermal run-away	Temperature	High
Inhibitor fails during receiving/-storage		Inhibitor	Low
O ₂ I fails high during storage		Oxygen	Low
O ₂ I fails low during storage	Gas Explosion	Oxygen	High

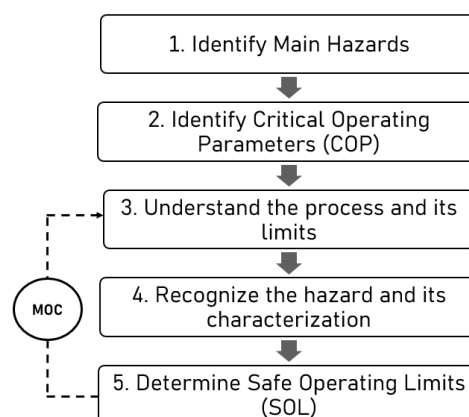
PI-Pressure Indicator; TI-Temperature Indicator; O₂I-Oxygen Indicator

Note: COPs such as inhibitor and lean oxygen might not be applicable for other flammable storage that doesn't have a risk of polymerization

Reviewing Safe Operating Limits during Changes

Whenever a change in process or equipments that affects critical operating parameters identified, then we may need to go-through back again from Step-3, Step-4 & Step-5 for the following reasons,

- To evaluate and revalidate SOL basis and other limits of the Critical Operating Parameters
- To evaluate and revalidate process safety time, response time and corrective action
- To evaluate and revalidate other safety alarms/-interlocks trigger points in the same process



7. Future scope of work

This study should be considered for extending research on optimizing and validating safe operating limits (Step-6), coupling plant-wide safe operating limits (Step-7), and integrating process safety elements (Step-8).

Step-6: Optimize and Validate Safe Operating Limits

Extract actual industrial-scale process data and conduct a variability study to assess maximum and minimum values, normal operating envelopes, and exceedance of SOLs (values from Step-5). The goal is to optimize and validate SOLs using a risk-based approach, considering the likelihood and consequences of exceedance. This step also addresses limitations in small-scale experimental setups that may not capture rapidly developing scenarios or sensor inertia.

Step-7: Coupling Safe Operating Limits

To ensure a holistic approach to process safety, it is essential to integrate safe operating limits across different units rather than treating them in isolation. This step involves:

- Identifying interdependencies across units
- Determining critical plant-wide operating parameters
- Coupling plant-wide SOLs with unit-level SOLs for system-wide risk management and cascading failure prevention

Step-8: Integration of Process Safety Elements

Recognizing the interaction of SOLs with process safety elements (PSEs) such as process hazard analysis, operating procedures, and safety-critical systems is key to preventing deviations from escalating into hazardous situations. This ensures SOLs are accurately defined and effectively managed throughout the plant's lifecycle.

8. Concluding Remarks

Properly defined Safe Operating Limits (SOL) can provide operator with a possibility to prevent safety instrumented system (SIS) or pressure relief device activation, as well as loss of primary containment (LOPC), therefore, they are true leading indicators. Systematic evaluation and identification of the normal/-safe operating/-design envelopes as well as consequence of deviation would help to maintain efficient/-effective operations, meet environmental restrictions and ensure process safety. It will also serve as a quick reference guide for operations personnel during process upsets. It closely interacts with other process safety elements such as operating procedures, hazard analysis, process safety information, mechanical integrity.

This study would help to standardize and be consistent with the established process by developing industry specific guidelines for determining and managing SOL, performance indicators and exceedance management. Further, its success is expected to benefit the industry to close the knowledge gaps based on science-based evidence and provide greater transparency and consistency in regulatory requirements to enable better decision making and reduce opportunity costs by enabling them to pursue more cost-effective options. The goal is not only to address safety issues (for example, drive SOL as far from design limits), but also to explore opportunities to optimize and expand normal operating limit to the extend not compromising on safety from sustainability standpoint

9. Acknowledgments

We would like to express our sincere gratitude to **Singapore Institute of technology, Institute of Sustainability for Chemicals, Energy, and Environment, A*STAR** for their support and valuable resources in conducting this study. Special appreciation is extended to **Prof. Paul Nicholas SHARRATT**, Department of Food, Chemical and Biotechnology, Singapore Institute of Technology, Singapore for his insightful discussions, technical expertise, and constructive feedback, which significantly contributed to the development of this research.

Furthermore, we acknowledge the contributions of some industrial colleagues for their assistance in data collection, case study analysis, and reviewing the manuscript. Lastly, we thank **Asahi Kasei Synthetic Rubber Singapore Private Limited** for their financial support and commitment to advancing process safety research in major hazard installations.

10. References

1. Occupational Safety and Health Administration (OSHA), 29 CFR 1910.119, Process Safety Management of Highly Hazardous Chemicals - Compliance Guidelines and Enforcement Procedures. (2015).
2. De La Cruz-Guerra, C., & Javier Cruz-Gomez, M. (2002). Using Operating and Safety Limits to Create Safety Procedures. *Process Safety Progress* 21(2). Wiley
3. Dee, S. J., Ogle, R. A., & Walters, M. S. (2022). Writing in the margins: Considerations for safe operating limits. *Process Safety Progress*, 41(2). Wiley
4. A.M. Dowell III, P.E. (2001). Critical safe operating parameters: "Never Exceed" Limit and "Never Deviate" Action. *Process Safety Progress*, 20(3). Wiley
5. Jerry Forest (2018). Know Your Limits. *Process Safety Progress* 37(4), Wiley
6. American Institute of Chemical Engineers Inc., (2012). Guidelines for engineering design for process safety. 2nd Edition, John Wiley & Sons, Hoboken: New Jersey.
7. American Institute of Chemical Engineers Inc., (2007). Guidelines for Risk Based Process Safety, John Wiley & Sons, Hoboken: New Jersey.
8. American Institute of Chemical Engineers Inc., (2008). Inherently Safer Chemical Processes: A Lifecycle approach. 2nd edition. John Wiley & Sons, Hoboken: New Jersey.
9. Sutton Ian (2011). Process Safe Limits: Defining safe limits quantitatively. DOI: <https://suttonbooks.wordpress.com/article/process-safe-limits-2vu500dglb4m-4/>
10. American Petroleum Institute (API), Recommended Practice 754. Process Safety Indicators for the Refining and Petrochemical Industries (2021)
11. Inglenook Engineering Inc., (2017). Safe Operating Limits Definition, DOI: <https://www.inglenookeng.com/services/safe-operating-limits-definition/>
12. Stauffer T, Chastain-Knight D. Do not let your safe operating limits leave you S-O-L (out of luck) (2020). *Process Safety Progress* 2020; e12163. Wiley
13. Sutton Ian (2015). Hazard Identification: Process Risk and Reliability Management. Elsevier
14. Workplace Safety and Health Act- Major Hazard Installations (WSHA-MHI) Regulations (2017)
15. U.S. Chemical Safety and Hazard Investigation Board (CSB), Ethylene Release and Fire at Kuraray America, Inc. EVAL Plant, Investigation Report, Published: December 16, 2022
16. U.S. Chemical Safety and Hazard Investigation Board (CSB), Electrostatic Precipitator at ExxonMobil Torrance Refinery, California, Investigation Report, Published: May 2017
17. U.S. Environmental Protection Agency (EPA), Fire and Explosion hydro catalytic cracking unit at Tosco Avon Refinery, California, Investigation Report, Published: November 1998
18. U.S. Chemical Safety and Hazard Investigation Board (CSB), Explosion and fire at Morton International, New Jersey, Investigation Report, Published: August 2000