COGNASCENTS
PROCESS SAFETY • ASSET INTEGRITY • AI-ACCELERATED

TECHNICAL REPORT | PROCESS SAFETY

The PST Gap: When Your Instruments Can't Respond in Time

> A case study in Process Safety Time validation across refinery units.

Date: June 2026

Scope: Seven units across three refining facilities

Discipline: SOL development · PST validation · PHA / LOPA support

INTRODUCTION

Your safeguards are only as good as their ability to act in time

A trip that activates too late — or can't return the process to safe operation before design limits are exceeded — isn't protection. It's a false sense of security.

Facilities routinely credit instruments — high-pressure alarms, level trips, high-temperature control, operator responses to low O_2 alarms — as Independent Protection Layers (IPLs) in PHAs and LOPAs. The assumption: if the alarm annunciates or the trip triggers, the event is prevented. But what if the instrument or associated alarm response simply can't prevent the design limit exceedance?

Cognascents Consulting has validated IPL response capability across multiple refinery units, and the results are a wake-up call. As an industry, we routinely ensure pressure-relief valves are sized for every credited overpressure case in a LOPA — why don't we hold our instrumented protections to that same standard?

> "A trip that can't return the process to safe operation before design limits are exceeded isn't protection. It's a false sense of security."

THE PROBLEM

Credited protection isn't always real protection

There are multiple ways to define Process Safety Time (PST). For simplicity, here we define it as the window between a process parameter passing an action set point and the undesired event occurring — the span from **IRT + PLT** in the figure below. A safeguard must complete its protective action — automated trip or operator response — within that window.

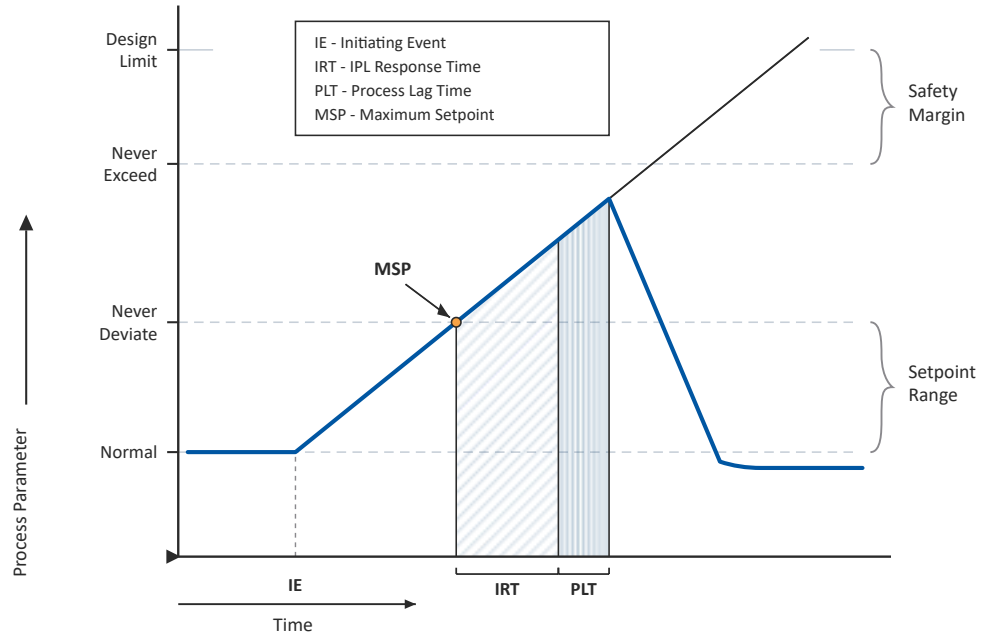

Figure 1 — Timeline for progression of a scenario. Process Safety Time is the window from the action set point to the undesired event (IRT + PLT). The Maximum Setpoint (MSP) is the highest point at which a credited alarm or trip can be set while still leaving enough safety margin below the design limit. Adapted from CCPS, *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis*, Figure 3.1. [1]

Of critical note, a Maximum Setpoint (MSP) must be identified and tracked as a Safe Operating Limit (SOL) — yet most facilities have never calculated it. What ends up occurring is that IPL credit is assigned based on *assumed* effectiveness, not *validated* effectiveness. PHAs identify what instrumented safeguards exist; they don't confirm whether those safeguards can actually respond in time.

The result is a hidden gap: instruments that look protective on paper but cannot prevent the hazard they're credited to address. And without structured validation, that gap is invisible.

FAILURE MODES

Where PST failures show up

Not every IPL requires a PST calculation — a pump deadhead scenario, for example, is better validated by a rotating-equipment specialist with hands-on knowledge of that pump and service than by any formula. But for instrumented trips and alarm-based operator responses tied to time-sensitive excursions, structured validation is essential. Two scenarios illustrate the problem well.

SCENARIO 1

Compressor KO drum overfill

A PHA team may credit the high-level trip (LSHH) on the knock-out drum and accept the protection at face value. The deeper issue: the KO drum is significantly smaller than the upstream equipment. When a large liquid surge occurs, the drum may be able to initiate the trip in time — but the volume passes through before the compressor winds down to a safe speed.

Liquid carryover into a high-speed compressor causes catastrophic mechanical failure in seconds. The correct SOL is on the **upstream vessel** — where there is sufficient time and volume to take protective action. The KO drum LSHH is still useful for gradual level-rise events, which is what it was designed for.

SCENARIO 2

Distillation column overpressure

Teams often assume a large column and overhead system has enough vapor space to absorb a pressure excursion and give operators time to respond. PST calculations tell a different story. For the most severe cases, overpressure can develop in 30 seconds to a few minutes — in particular on lighter columns (e.g., depropanizers) with total-condensing overhead systems when cooling is lost. At that point, the pressure accumulation rate is driven directly by column traffic, and the overhead system volume is rarely large enough to provide adequate PST for an alarm-based IPL.

The key point PHA teams sometimes miss: the time available is **not** measured from normal operations or even the first troubleshooting alarm. It is measured from the PVHH — the alarm with predetermined, trained actions intended to prevent the overpressure — because IPL rules dictate that credited alarms must be at the point where troubleshooting has stopped. The window from the PVHH to design pressure is almost always shorter than it appears during qualitative conversations.

Operator-based IPLs deserve the same scrutiny. Even companies that have implemented safety instrumented systems and follow ISA-84 / IEC 61511 often fail to apply those same principles to operator responses — never calculating whether a person can detect an abnormal condition, recognize it as an emergency, determine the correct response, and complete the required action within the available PST. For fast-developing events, that window is frequently tighter than assumed, making operator-based IPLs among the most overlooked gaps in PST discussions.

THE DATA

What the data shows

After implementing SOL programs for various refineries, Cognascents developed the following case study reviewing seven unique units at three facilities. PST validation was performed on instrumented IPLs across pressure, temperature, level, flow, and concentration parameters. The results were consistent — and concerning.

100%

failure rate at one unit — every evaluated instrument was incapable of responding within the required PST

20–100%

range of failure rates observed across all seven units evaluated

Zero of seven

units in which all credited instruments passed PST validation

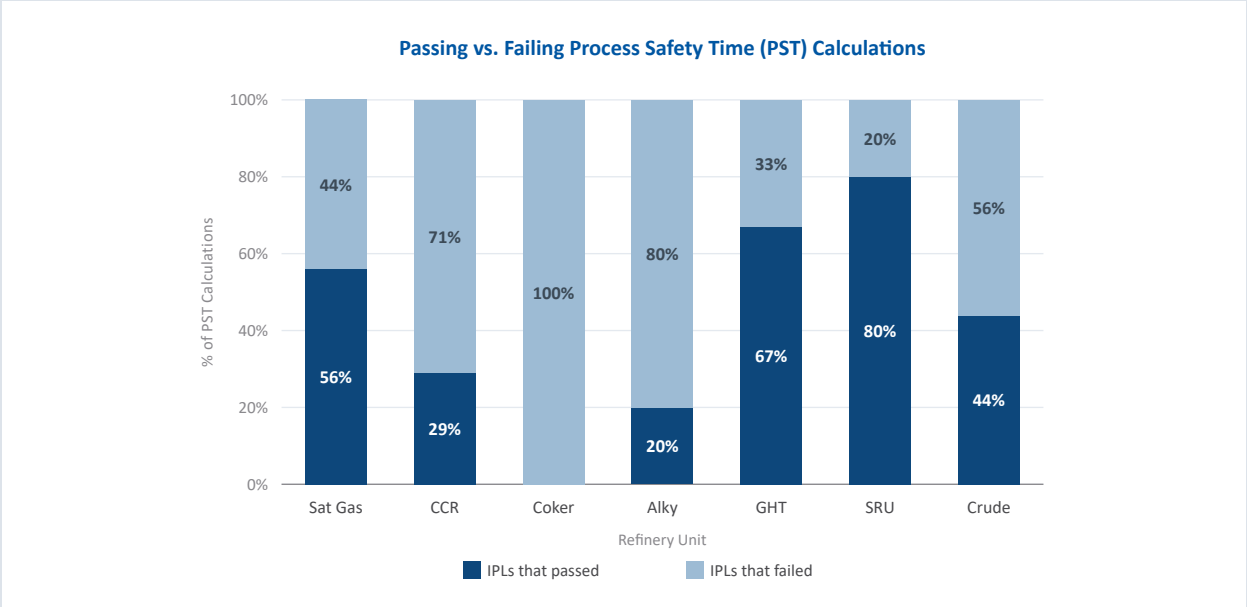

Figure 2 — Passing vs. failing PST calculations by unit. The share of credited instrumented IPLs that could (dark) and could not (light) complete their protective action within the available Process Safety Time. In no unit evaluated did all credited instruments pass; one unit (Coker) failed every evaluated case.

These are instruments formally credited in LOPA studies as providing a defined order of magnitude of risk reduction. They couldn't do the job when it mattered.

THE FRAMEWORK

How the gap gets closed

Closing the PST gap requires a structured framework — not just calculations in isolation. The approach Cognascents applied combined PHA outputs, engineering validation, and corporate equipment guidance.

STEP 1

Start with PHAs, but don't stop there

Corporate equipment and unit guidance runs in parallel to catch high-severity scenarios that PHAs missed — particularly at units with less mature risk assessments.

STEP 2

Calibrate against operating reality

Red Flag Reviews overlay historical data with proposed setpoints to catch limits that would cause nuisance trips or fail to reflect actual emergency thresholds. Operator engagement here is essential.

STEP 3

Run PST calculations where they add value

For time-sensitive, high-severity scenarios, calculations confirm that sensor lag, logic-solver execution, and final-element stroke time all fit within the available window.

STEP 4

Feed findings back into the PHA cycle

Where PST failures are identified, LOPA studies are updated, and compensating measures are evaluated and documented.

The outcome is not just a list of SOLs — it's a clear, documented answer to a question most facilities have never asked: which instruments can actually prevent their associated high-severity events, and which cannot.

> "When an incident occurs, the first question should no longer be 'Why didn't the operator respond in time?' — it should be 'Why didn't we set our operators up for success?'"

THE BROADER IMPLICATION

A systemic gap — and what it means for your facility

The PST gap is systemic. It emerges directly from how PHAs and LOPAs are designed: PHAs are risk-assessment tools, not instrument-response validators. That work has to happen outside the PHA room. PST validation is documented as a standard expectation in LOPA guidance — yet it remains inconsistently applied across the industry.

Until it becomes a standard step in SOL development, facilities will continue to operate with protection layers that exist on paper but not in practice. In high-consequence environments, that distinction could be the difference between a near-miss and a fatality.

If your facility hasn't conducted structured PST validation, ask yourself:

1. Have your alarm-based IPLs been validated for operator response time — including detection, recognition, decision, and action — against the available PST?
2. Have your instrumented trips been evaluated to confirm that sensor lag, logic-solver execution time, and final-element stroke time fit within the PST window?
3. Where PST failures exist, have your LOPA studies been updated to reflect the loss of credited risk reduction?

TALK TO A SENIOR ENGINEER

If any of these don't have a clear answer, the gap may already exist at your facility — you just haven't found it yet. Cognascents Consulting Group specializes in process safety management, including SOL program development, PST validation, PHA / LOPA support, and risk-based decision making across refining and chemical operations. Reach out at cognascents.com.

References

The Process Safety Time framework and the scenario timeline (Figure 1) used in this report follow the guidance of the AIChE Center for Chemical Process Safety (CCPS).

1. CCPS, *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis*, 1st Ed., John Wiley & Sons / AIChE Center for Chemical Process Safety, New York, NY, 2015.

https://onlinelibrary.wiley.com/doi/book/10.1002/9781118948743

DOI: 10.1002/9781118948743 · Figure 1 in this report is adapted from Figure 3.1.

Standards & guidance referenced

- **ISA-84 / IEC 61511** — Functional safety: safety instrumented systems for the process industry sector.
- **OSHA 29 CFR 1910.119** — Process Safety Management of Highly Hazardous Chemicals.

Prepared by Cognascents Consulting Group. Figures 1 and 2 were recreated for this report; Figure 1 is adapted from the CCPS reference cited above and is reproduced here for instructional purposes with attribution.