GREY PAPER

Process Safety and the Learning Organization

Root Cause Investigation and Analysis (RCIA)

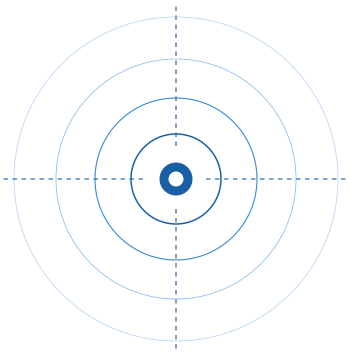
Connecting Investigation Findings to Systemic Improvement at the Right Level of the Organization

Kenan Stevick, CCPSC

Co-Author, CCPS Process Safety Leadership from the Boardroom to the Front Line (2019)

Co-Author, CCPS Guidelines for Process Safety in Outsourced Manufacturing Operations, 2nd Edition (2026)

May 2026



RCIA

ROOT CAUSE INVESTIGATION & ANALYSIS

Zeroing in on the right answer.

Executive Summary

Most process safety investigations produce corrective actions that close in a tracking system but do not prevent the next incident. The equipment gets fixed. The procedure gets revised. The action items get marked complete. And then, months or years later, a similar incident occurs at a different facility, on different equipment, driven by the same management system failure that produced the first one. The investigation found the immediate cause. It did not find the root cause.

This is not primarily a competence problem. It is a design problem. Traditional investigation approaches stop at the safeguard failure — the failed valve, the missed inspection, the outdated procedure — and never ask what management system was supposed to govern that safeguard, why it failed, and what level of the organization is responsible for fixing it. The result is a corrective action that protects one piece of equipment while leaving every other asset governed by the same inadequate system at continued risk.

Effective root cause investigation and analysis (RCIA) requires seven steps and applies to major accidents, Tier 1 and Tier 2 Process Safety Events, and Tier 3 near-miss events (smaller releases). Accounting for every safeguard failure, identifying the management system failure behind each one, involving the function that owns the management system, matching the corrective action to the right organizational level — plant, site, region, technology, or enterprise — and applying the same rigor to near-misses and high-potential events as to major incidents. At Step 6, a Senior Leadership gate ensures that only adequately investigated incidents with properly scoped corrective actions proceed to implementation. Senior leadership engagement is not optional. The RCI effectiveness review and the repetitive incident analysis are the mechanisms by which investigations become organizational learning rather than plant-level paperwork.

The goal is a specific operational outcome: every incident and near-miss produces a management system correction at the right level and a communication that allows the rest of the organization to learn from it. When that cycle functions well, the incident rate does not plateau. It can decline dramatically.

The Investigation That Doesn’t Prevent the Next Incident

Most process safety investigations conclude with a list of corrective actions. The equipment is repaired or replaced. A procedure is revised. A training record is updated. The action items are closed in the tracking system. The incident is declared resolved.

And then, months or years later, a similar incident occurs. Not necessarily on the same equipment. Not necessarily at the same facility. But driven by the same failure mode, the same management system gap, the same organizational blind spot that produced the first one. The investigation

found the immediate cause. It did not find the root cause. And without finding the root cause, there was never a realistic chance of preventing repetition.

This is one of the most persistent and costly patterns in chemical and pharmaceutical process safety. It is also one of the most preventable. The gap is not in investigation technique. It is in what investigations are expected to find, and what organizations do with the findings when the investigation is done.

> *A management system may govern hundreds or thousands of protection layers across a facility, a site, or an enterprise. Fix the equipment after an incident and miss the management system, and nothing has been done to prevent the next one.*

Why Repetitive Incidents Happen

Chemical facilities handling hazardous materials typically have multiple safeguards — engineered controls, administrative barriers, and protection layers — designed to prevent specific process safety scenarios from reaching consequence. Some are defined by corporate or industry standards; others are identified through formal hazard and risk assessments such as Process Hazard Analysis (PHA), Layers of Protection Analysis (LOPA), or Quantitative Risk Analysis (QRA). Once established and implemented, each safeguard must be operated within its defined constraints and maintained in a state of readiness.

This leads to a foundational principle that is often overlooked in practice: when a process safety incident occurs at a facility where safeguards were in place to prevent it, every one of those safeguards failed. By definition. And behind every safeguard failure is a management system failure — the system that was supposed to ensure the safeguard was in place, functioning, and being maintained stopped doing its job.

This is the mechanism of repetition. A single management system typically governs not one safeguard but many — across multiple pieces of equipment, multiple plants, potentially multiple sites. An investigation that corrects the failed safeguard on the specific equipment involved in the incident, without identifying and correcting the management system failure behind it, leaves every other safeguard governed by that same system at risk. The next incident is a matter of when, not whether.

The legacy investigation problem

Traditional investigation approaches focus on finding an effective solution to the immediate problem. The root cause, in this framing, is defined as the absence of the solution — the thing that was missing that, if present, would have prevented the incident. This approach produces corrective actions that address the specific event but rarely address the system behind it.

What it misses is the second layer of the question. Not just “what failed?” but “what management system was supposed to prevent that failure, and why didn’t it?” That second question is what separates an investigation that prevents the next incident from one that simply documents the last one.

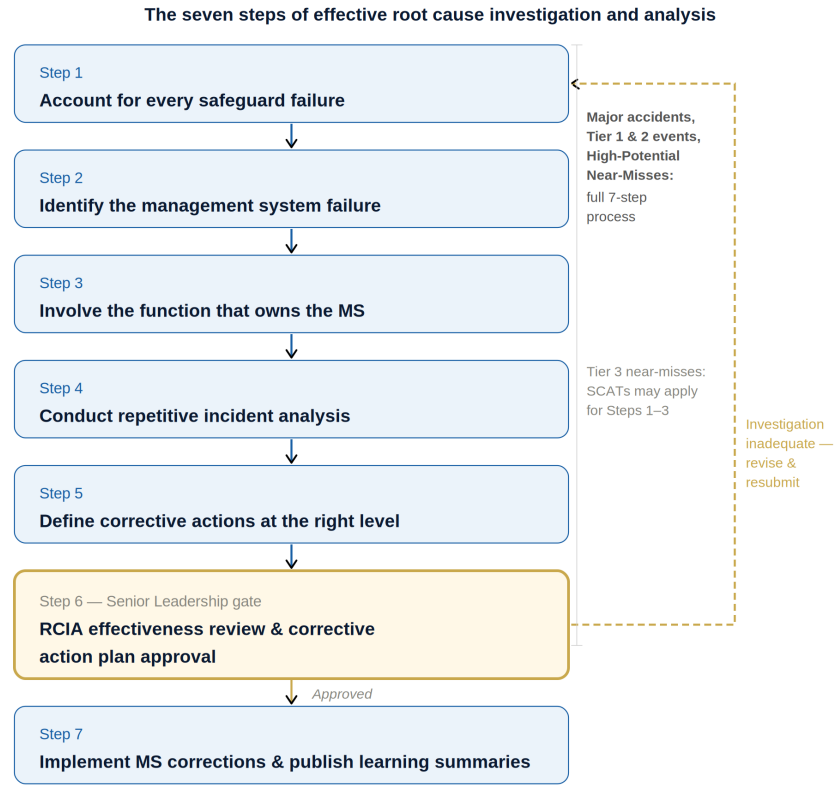
The plateau signal

When process safety incident performance plateaus — when an organization stops making progress despite continuing to investigate and close corrective actions — repetition is frequently the explanation. The incidents keep happening not because they are new problems but because the same failure modes and management system gaps keep producing consequences. The investigation process is working as designed. The design is not adequate.

Recognizing the plateau as a signal, rather than an anomaly, is itself a mark of an organization that is learning. Acting on it requires a different kind of investigation — one that is explicitly designed to find management system failures, not just immediate causes.

The Seven-Step RCIA Framework

The following seven-step framework is designed to produce investigations that find management system failures, determine the right level of correction, and generate learning that reaches the entire organization. It applies to major accidents, Tier 1 and Tier 2 events, and High-Potential Near-Misses in full. For straightforward Tier 3 near-misses without complex safeguard interactions, Systematic Cause Analysis Techniques (SCATs) may apply for Steps 1–3.



The gold gate at Step 6 ensures only adequately investigated incidents with properly scoped corrective actions proceed to implementation.

Figure 1 — The RCIA seven-step process

Step 1: Account for every safeguard failure

The investigation must identify the immediate cause of failure for every required safeguard that was in place to prevent the incident — both those defined by corporate standards and those identified through formal risk assessment. It is not sufficient to identify that a safeguard failed. The investigation must explain how and why each one failed.

This matters because incidents rarely involve a single failure. Multiple safeguards are typically in place, and an incident reaching consequence means multiple safeguards failed. An investigation that focuses on the most visible or most proximate failure misses the full scope of what needs to be corrected.

Step 2: Identify the management system failure

For every safeguard failure identified, the investigation must ask: what management system was responsible for ensuring this safeguard was in place, functioning, and maintained? And what failed in that management system that allowed the safeguard to fail?

The management system failure is the root cause. Not the failed valve, the missed inspection, or the outdated procedure — those are safeguard failures. The root cause is the system that was supposed to govern those safeguards and did not. That system is what must be corrected to prevent repetition.

For straightforward Tier 3 near-misses without complex safeguard interactions, Systematic Cause Analysis Techniques (SCATs) can efficiently identify root causes without a full formal investigation. A SCAT is appropriate, for example, when a missed inspection near-miss traces directly to a scheduling or work order system gap with no overlapping safeguard failures. In those cases the management system failure is clear and the corrective action is bounded. For Major Accidents, Tier 1 and Tier 2 Events, and High-Potential Near-Misses, the full seven-step process is required.

Step 3: Involve the function that owns the management system

Identifying the correct management system failure requires involving the function responsible for its implementation — the engineering group, the maintenance organization, the operations leadership, the process safety function, whichever owns the element in question. This serves two purposes. First, it ensures the right failure is identified — functions closest to implementation know how the system actually works. Second, it places ownership of the corrective action where it belongs. A corrective action owned by the function responsible for the management system is far more likely to be implemented effectively and sustained.

Step 4: Conduct the repetitive incident analysis

Before any investigation is finalized, the findings must be compared against the organization's incident history: is this a new problem, or have we seen this before? Has this failure mode appeared in a different plant, under a different management system, at a different site?

Key questions include whether the same safeguard failure type has occurred elsewhere in the portfolio, whether the same management system failure has appeared in prior incidents on different equipment, and whether the failure mode was already identified as a known risk in the facility's PHA or LOPA. A searchable incident database, structured consistently enough to support pattern queries, makes this analysis tractable. Without one, pattern recognition depends on institutional memory — which is unreliable and does not survive organizational change.

One critical corollary applies: when the same management system failure appears repeatedly across multiple facilities or organizational boundaries — each with their own independent

management system — those management systems must be fixed or consolidated at a higher level. Repeated failures across boundaries are a signal that the original corrective action was scoped too narrowly and the gap remains unresolved above the plant level.

Step 5: Define corrective actions at the right organizational level

This is the step where most organizations leave the most value on the table. A management system failure at a single plant requires correction at the plant level. A gap in a site-wide standard requires correction at the site level. An inadequate corporate standard or work process requires correction at the enterprise level.

Applying a plant-level correction to an enterprise-level failure is not a fix — it is a workaround that protects one facility while leaving every other facility at continued risk. Corrective action recommendations must be explicitly scoped — plant, site, technology, or enterprise — before being submitted for Senior Leadership approval. Actions should be defined for each applicable facility and tracked by leadership at the level that owns the management system failure.

THE FOUR ORGANIZATIONAL LEVELS OF CORRECTIVE ACTION

1. Plant or facility level — The management system failure is specific to local implementation. The plant owns it, resources it, and tracks it to closure.

2. Site level — The failure reflects a gap across multiple plants at a single site. A plant-level fix protects one unit while leaving the others exposed.

3. Technology or business level — The failure is associated with a specific technology or process type deployed across multiple sites. The correction must reach every deployment.

4. Enterprise level — The failure reflects a gap in a corporate standard or work process deployed company-wide. Only corporate leadership can authorize and resource the correction.

Step 6: Senior Leadership effectiveness review and corrective action approval

Senior Leadership conducts two distinct functions at this gate. The first is assessing whether the investigation was done well — whether every safeguard failure was identified, whether the management system failures were correctly diagnosed, and whether the corrective actions are genuinely adequate. The question that distinguishes a real effectiveness review from a sign-off is this:

> *“Show me where the management system(s) failed, and why your proposed actions prevent that failure at every facility where the same safeguards are deployed.”*

If the investigation team cannot answer that question, the investigation goes back. Findings are revised before any corrective action is approved.

The second function is approving the corrective action plan based on the pattern recognition conducted in Step 4. Senior Leadership approves the management system corrective action plan for Major Accidents, Tier 1 and Tier 2 Events, and High-Potential Near-Misses. Tier 3 event trends, near-miss findings, and challenges to safety systems are not individually escalated to Senior Leadership for approval — instead, they are reviewed in routine management system reviews, where patterns are assessed and systemic corrective actions identified.

Together, these two reviews transform the investigation from a plant-level event into an organizational learning process — the mechanism by which Senior Leaders engage with process safety in a substantive way, evaluating the quality of analysis and the adequacy of response rather than simply reviewing incident rates.

> *Engaging senior leaders in investigation reviews changes the culture in a way that metrics reporting cannot. It signals that the organization takes its investigation findings seriously enough to have leadership validate them.*

Step 7: Implement corrections and publish learning summaries

The final step has two components. The first is implementing the approved management system corrections at the right organizational level — not just closing the specific action items, but updating the standards, procedures, and work processes that govern the protection layers across every affected facility.

The second component is communicating findings in a form that allows the entire organization to assess whether the same vulnerability exists elsewhere. One-page learning summaries serve a purpose that formal investigation reports cannot — they are readable at the front line, can be discussed in safety meetings and toolbox talks, and end with the most important question an investigation can generate: “Could this happen in your facility?”

The template below provides a consistent structure for learning summaries:

ONE-PAGE LEARNING SUMMARY — TEMPLATE STRUCTURE	
Event description	Brief summary of what occurred, what tier, and what facility or process type.
Picture or diagram	Picture or diagram of the process or facility
Safeguards that failed	List each safeguard that was in place but failed to prevent the event.
Management system failure(s) identified	For each safeguard failure, name the management system element that failed and why.
Corrective actions taken	State each action and the organizational level at which it was implemented (plant / site / technology / enterprise).
Could this happen at your facility?	Key questions for other facilities to self-assess against the same management system gap.

A learning summary might indicate an incident caused by the use of a templated software code, where the technology-level action was to check all plants using that code — and several plants found the same problem. This finding could then prompt other technologies that use templated software codes to check their own software templates. What began as a single plant incident becomes a technology-wide management system improvement, and potentially an enterprise-wide standard review.

The Measure of a Working RCIA Process

A working RCIA process produces measurable results. At Dow Chemical, the investigation framework described in this paper was deployed across a global Fortune 50 chemical company as part of a corporate process safety improvement initiative. The results: a 75% reduction in Tier 1 and Tier 2 incidents in the first four years, preventing more than $50 million in annual incident costs — a result that remains an industry benchmark.

The framework was included in an evaluation and improvement plan for a specialty chemical company using the CCPS Risk Based Process Safety (RBPS) framework. The result was a 50% reduction in process safety incidents over three years. In both cases, the improvement was not driven by more investigations — it was driven by better investigations that found management system failures, applied corrections at the right organizational level, and communicated learnings across the enterprise.

The difference between an organization that improves and one that plateaus is not the frequency of investigation. It is whether the investigation process is designed to find what actually needs to be fixed.

THE GOAL OF THE LEARNING ORGANIZATION

The goal isn't just to fix what broke. It's to build an organization that learns from every incident, corrects management systems at the right level, and becomes genuinely less likely to repeat the same failures.

What This Requires of Operations Leaders and Process Safety Professionals

A learning organization in process safety does not emerge from a methodology alone. It requires specific behaviors from the people who own the investigation process and the people who are accountable for the management systems being corrected.

For Operations Leaders — Plant Managers, Site Directors, VPs of Operations, COOs	
• Participate in investigation reviews as a principal, not as an audience. The effectiveness review is a technical evaluation that requires operations leadership to challenge the adequacy of the analysis and the scope of the proposed corrections — not a briefing to attend.	☐
• Own the decision about correction level. Determining whether a management system failure requires plant, site, technology, or enterprise-level correction is a leadership decision, not a technical one. It requires understanding the full scope of where the management system is deployed and the organizational authority to act at the appropriate level.	☐
• Track pattern data, not just incident counts. Incident rates tell you what happened. Repetitive incident analysis tells you why the same things keep happening. Operations leaders who are not regularly reviewing management system failure patterns across their portfolio are missing the most actionable information they have.	☐
• Treat near-misses with the same rigor as incidents. A near-miss that reveals a management system gap is functionally equivalent to an incident that did not reach consequence. The investigation standard should be the same.	☐

For Process Safety Professionals	
• Build investigations around safeguard failure and management system failure, not just immediate cause. Every investigation should be structured to answer both questions: what safeguard failed, and what management system failure allowed it to fail.	☐
• Bring the repetitive incident analysis to every investigation review. Pattern recognition does not happen spontaneously. It requires a deliberate comparison of current findings against the incident history, conducted before the investigation is closed.	☐
• Specify the correction level in every recommendation. Corrective action recommendations should explicitly state whether the proposed action addresses the plant, site, technology, or enterprise management system, and why that level is appropriate.	☐
• Make near-miss investigation a cultural norm, not an exception. The volume of near-miss learning available in most chemical and pharmaceutical operations is vastly underutilized. Building an organization that investigates near-misses rigorously and communicates findings broadly is one of the highest-leverage investments in process safety improvement available.	☐

Questions Worth Asking

The following questions tend to surface whether an organization's investigation process is designed to produce systemic improvement — or whether it is producing well-documented repetition.

FOR OPERATIONS LEADERS

1. When did you last participate in an investigation review as a principal — challenging the adequacy of the analysis — rather than receiving a briefing on findings?

2. Do you know what percentage of your incidents in the past three years involved the same management system failures as prior incidents? If not, why not?

3. Can you name the management systems in your portfolio with the most repeat findings? Do you know what level of the organization owns the fix?

4. When a near-miss occurs at one of your facilities, does it receive the same investigation resources as a Tier 1 incident — or is it closed with a one-paragraph summary?

5. If your incident rate has plateaued, have you examined whether your investigation process is identifying management system failures — or only immediate causes?

FOR PROCESS SAFETY PROFESSIONALS

1. In your last five investigations, how many explicitly identified a management system failure — not just an immediate cause? Were the management system owners involved in developing the corrective actions?

2. Have you conducted a repetitive incident analysis before closing your most recent investigation? Did you compare the failure mode against your incident history at the plant, site, and business level?

3. For each corrective action in your most recent investigation, can you state whether it addresses a plant, site, technology, or enterprise-level management system — and whether the action is scoped to match?

4. Does your organization publish learning summaries for major accidents, Tier 1 and Tier 2 events, and High-Potential Near-Misses?

5. Are near-miss root causes analyzed to identify trends, findings, and potential actions for review in management system reviews?

6. When you recommend a corrective action, do you specify the organizational level at which the management system needs to be corrected — or do you leave that decision to whoever receives the report?

These questions are not adversarial. In organizations where the investigation process is working well, they are easy to answer. In organizations where it is not, they surface exactly where the gaps are.

RCIA: Root Cause Investigation and Analysis

The framework described in this paper is the foundation of Kenan Stevick's RCIA practice. RCIA services are available across three engagement types, depending on where an organization is in its investigation maturity.

Investigation leadership and facilitation

For organizations that have experienced a significant process safety incident, near-miss, or high-potential event, Kenan provides hands-on investigation leadership — structuring and facilitating the root cause investigation process to ensure every safeguard failure is identified, every management system failure is diagnosed, and corrective actions are scoped at the right organizational level.

Investigation quality assessment

For organizations that have conducted investigations but are uncertain whether they found the real root causes, or whose incident trends suggest investigations may not be finding root causes, Kenan assesses the quality of past investigations against the seven-step framework. This engagement typically surfaces unresolved management system gaps that prior investigations missed, and identifies the corrective actions that should have been taken — before another incident makes them unavoidable.

Corrective action program development

For organizations seeking to build or rebuild a systematic approach to investigation and learning, Kenan designs corrective action programs that match the fix to the right organizational level — from a single plant to enterprise-wide — so that systemic causes are addressed rather than symptoms. This includes the leadership review structure, the repetitive incident analysis process, and the enterprise communication framework needed to convert individual incident findings into organization-wide learning.

kenanstevick.com • kenan@kenanstevick.com • 970-409-2528

About the Author

Kenan Stevick is a process safety professional with 44 years of experience in chemical and pharmaceutical manufacturing, including 34 years at Dow Chemical (Fortune 50) in operational and technical leadership. Across two positions, Kenan led the corporate initiative that achieved a cumulative 90% reduction in Tier 1 incidents over ten years — including a 75% reduction in Tier 1 and Tier 2 incidents in his first four years as Chief Process Safety Engineer, preventing more than $50 million in annual incident costs. These results remain industry benchmarks. The investigation framework described in this paper was developed and deployed across a global Fortune 50 chemical company as part of that effort, and was presented at the 11th Global Congress of Process Safety in Austin, Texas, in 2015. He co-authored two CCPS publications that define the standard of care in process safety governance: Process Safety Leadership from the Boardroom to the Front Line (2019) and Guidelines for Process Safety in Outsourced Manufacturing Operations, Second Edition (2026). He is a Fellow of CCPS (2015) and holds the CCPS Certified Process Safety Professional (CCPSC) designation.

This grey paper draws on concepts and frameworks developed during Kenan Stevick's tenure as Chief Process Safety Engineer at Dow Chemical and presented at the 11th Global Congress of Process Safety (Austin, TX, 2015), as well as the CCPS process safety leadership framework and Risk Based Process Safety (RBPS) framework. It is intended for informational purposes and does not constitute legal advice.