OpsPilot

Safety Investigation — User Manual

Near Misses & Process Safety Events · Barrier Analysis · AI Engineering Co-Pilot

What this guide covers — what a safety investigation is (and how it differs from injury investigation and RCA), how the OpsPilot module applies barrier analysis, what to have ready, and the report you receive.

1. What is a safety investigation?

A safety investigation examines events where the harm was avoided or the system was challenged — near misses, dangerous occurrences and process safety events — to learn why the barriers that should have prevented it didn't hold. The value is enormous precisely because nobody was hurt: it's a free lesson before the event that does cause harm. The method is barrier analysis — mapping the controls that were supposed to prevent the top event, and explaining why each one failed.

It complements the other investigation modules: *Injury Investigation* is for events where a person was harmed; *RCA* is for equipment failures; this module is for near misses and process-safety events, using barrier analysis rather than fishbone.

2. What the OpsPilot module does

Role	Responsibility
🎯 **AI Coach (OpsPilot)**	Applies structured barrier analysis and 5-Why — pushing beyond the surface, challenging assumptions, and ensuring every failed barrier is explained rather than glossed over.
👷 **Investigation Lead (you)**	Provide the ground truth — what actually happened, what controls were in place, and what was different on the day. Your knowledge of the site and the people is essential.

3. How it works — the process

#	Stage
1	Event type classification — near miss, dangerous occurrence, or process safety event
2	Hazard and top-event identification
3	Barrier mapping — what was supposed to prevent this?
4	Failed-barrier analysis — why did each control not work?

#	Stage
5	5-Why to the systemic root cause
6	Safety-critical control assessment
7	Corrective action plan
8	Word report

4. What you will be asked — have this ready

- The event type and what actually happened.
- The hazard and the top event (the thing that nearly went badly wrong).
- The barriers that were supposed to prevent it — and which held, which failed.
- What was different on the day, and the context around the people and controls involved.

5. What you receive — the output

A formal investigation report (Word): event classification, the hazard and top event, the barrier map, the failed-barrier analysis, the 5-Why to systemic root cause, the safety-critical control assessment and the corrective action plan.

6. Worked example (illustrative)

A near miss: a relief valve lifted and released to atmosphere, but nobody was hurt. The top event is overpressure. Barrier mapping lays out what should have prevented it: the control system pressure alarm, the operator response, the high-pressure trip, and finally the relief valve. The failed-barrier analysis works each one — the alarm fired but was lost in alarm flood (barrier failed), the operator didn't respond in time (barrier failed), the high-pressure trip was found to be out of calibration (barrier failed), and only the relief valve — the last line — actually worked. The 5-Why on the trip miscalibration reaches a systemic root: no functional-test schedule for safety-critical trips. The lesson is free this time; the corrective actions make sure the next overpressure doesn't rely solely on the last barrier.

7. Getting the best result

- **Treat near misses as gifts.** They're the lesson before the injury — investigate them as seriously.
- **Map every barrier.** Understanding which held and which failed is the whole method.
- **Explain each failure.** “The alarm didn't work” isn't enough — why didn't it?
- **Find the systemic root.** A miscalibrated trip points to a missing test regime, not a one-off.