RISKSORA

ENTERPRISE LOGO

INCIDENT INVESTIGATION REPORT

INCIDENT ID	INC-U4-2025-001/SC
Report	CSE Incident Investigation
Analysis date	2026-04-03
Severity	Major injury - hospitalisation
Location	Industrial facility - vessel maintenance area, Unit 4
Sector	Oil & Gas
Reporter	Safety Coordinator - Unit 4

CONFIDENTIAL

TABLE OF CONTENTS

Incident: INC-U4-2025-001/SC
Severity: Major injury — hospitalisation
Classification: 5 barriers · 3+ causal paths
Priority GFTs: IG (4), OR (3), MM (3)

EXECUTIVE SUMMARY

INC-U4-2025-001/SC | MAJOR INJURY — HOSPITALISATION | 2025-11-15 | Unit 4

4	5	3+	IG
SEVERITY	BARRIERS	CAUSAL PATHS	PRIORITY GFT

WHAT HAPPENED

On 15 November 2025 at approximately 08:30, a worker entered Vessel V-201 at the Unit 4 maintenance area to perform routine inspection. No independent atmospheric verification was conducted prior to entry. The worker relied on a portable gas detector that was 6 months overdue for calibration. Approximately 8 minutes after entry, the worker was overcome by toxic H2S atmosphere and lost consciousness. Co-workers raised the alarm, but the facility's single rescue team was deployed at an adjacent unit. 47 minutes elapsed before rescue arrived. The worker was extracted unconscious and transported to hospital with major injuries.

HOW IT HAPPENED — BARRIER FAILURES

Five barriers that should have prevented this incident either failed or were absent entirely. Three prevention controls failed: (1) no independent atmospheric verification existed as a PTW requirement, (2) the gas detector sensor had degraded past its calibration interval by 6 months, and (3) the supervisor authorised entry while managing 3 simultaneous confined space permits. Two recovery defences failed: the single rescue team was unavailable, and no backup rescue capability existed.

WHY IT HAPPENED — ORGANISATIONAL CAUSES

Each barrier failure traces to an organisational decision made weeks, months, or years before the incident. The staffing model allocated 1 supervisor to oversee up to 5 concurrent entries, creating production-driven workload that made inadequate oversight predictable. The calibration system was manual with no automated alerting, disconnected from the PTW authorisation process. The emergency response model had not been updated since the facility expanded from 3 to 7 operational units.

MANAGEMENT FAILURE — GFT CLASSIFICATION

Three management domains are responsible. Incompatible Goals (IG): production scheduling drove simultaneous entries beyond supervisory capacity. Maintenance Management (MM): calibration oversight was manual, invisible, and disconnected from operational authorisation. Organisation (OR): emergency resourcing was not scaled with facility growth. These are structural decisions, not individual failures.

WHAT WILL PREVENT RECURRENCE

TIER 1: MANAGEMENT INTERVENTIONS (LATENT FAILURES)

IG — Incompatible Goals:

Restructure supervisor-to-entry staffing ratio. Maximum 2 concurrent entries per supervisor as a hard limit in the PTW system.

MM — Maintenance Management:

Integrate calibration oversight directly into PTW. Overdue calibration must block permit issuance automatically.

OR — Organisation:

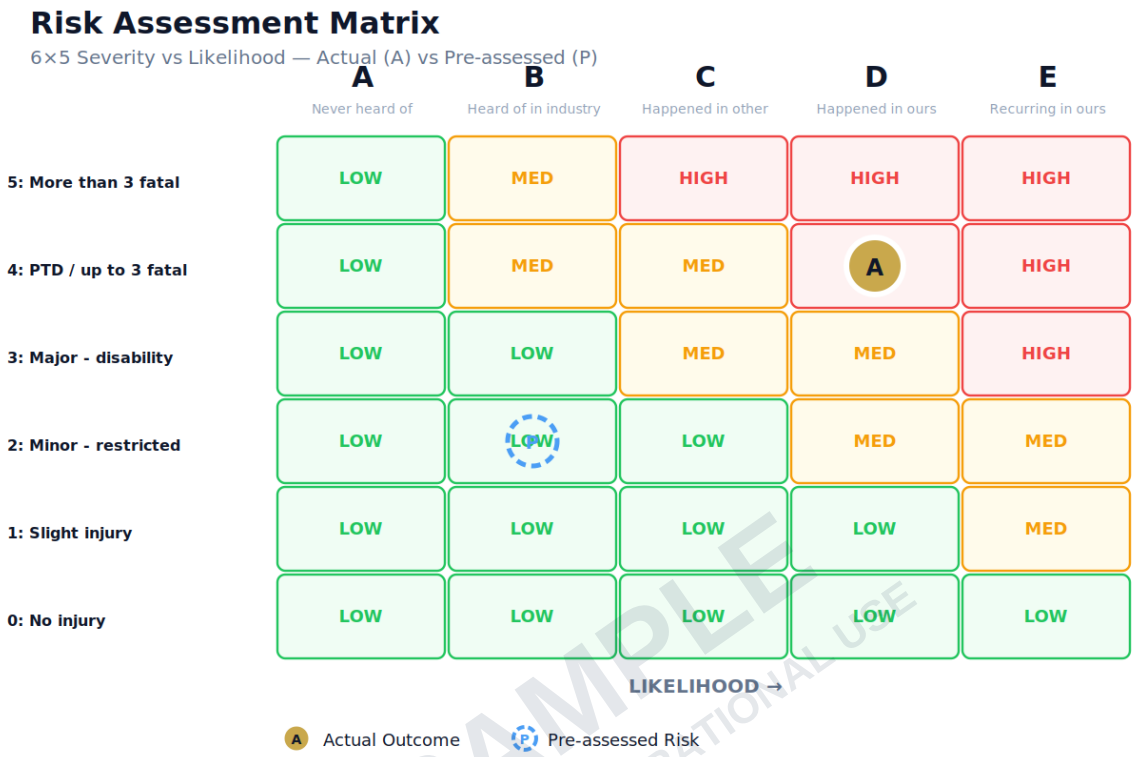
Scale emergency response to current facility footprint. Dedicated backup rescue team required, resourced independently.

TIER 2: OPERATIONAL CONTROLS (PRECONDITIONS + ACTIVE FAILURES)

- Mandatory independent atmospheric verification as a hard gate in PTW
- Automated calibration alerting at 30/14/1-day intervals
- Quarterly dual-team emergency response drills with measured response times

RISK ASSESSMENT MATRIX

6×5 Severity vs Likelihood — Actual (A) vs Pre-assessed (P)



INTERPRETATION

DEFICIENCY

The pre-assessed risk (P) classified this activity at Severity 2 × Likelihood B (LOW zone). The actual outcome (A) materialised at Severity 4 × Likelihood D (HIGH zone) — a gap of 2 severity levels and 2 likelihood levels. This is a fundamental failure of the risk assessment process.

IMPACT

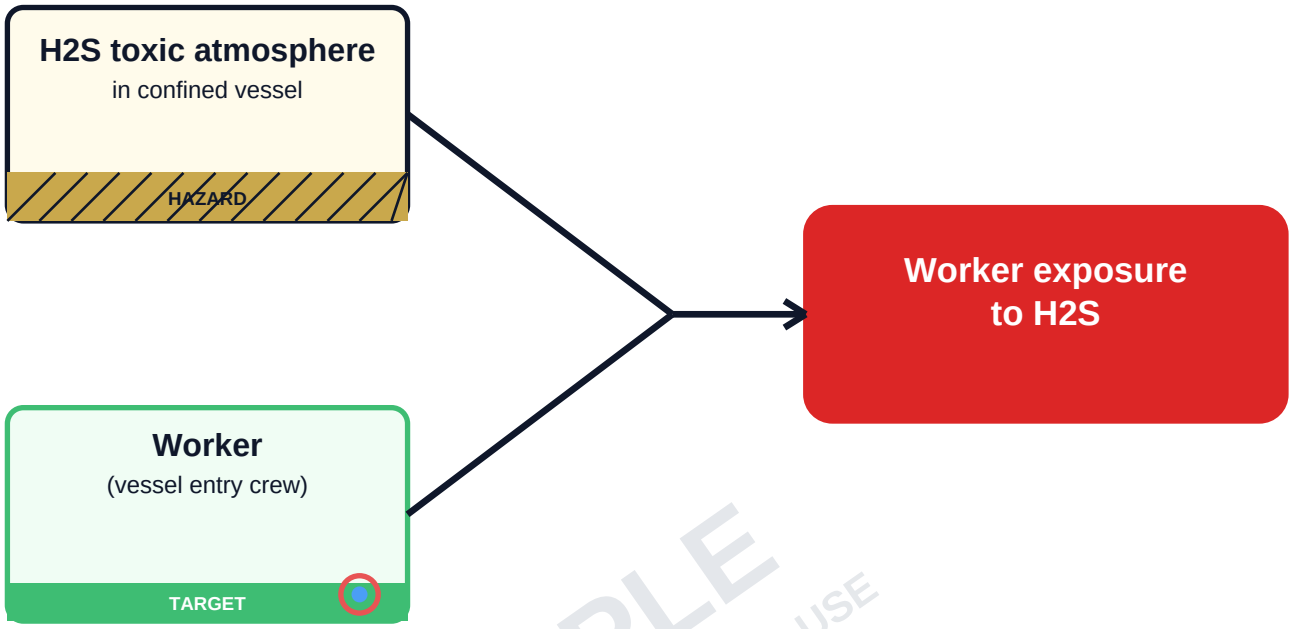
The risk assessment gap means the activity was permitted under controls appropriate for a LOW-risk task. Entry procedures, supervision ratios, emergency provisioning, and equipment checks were all calibrated to a risk level that bore no relationship to the actual hazard profile of the confined space.

ROOT CAUSES

Three systemic deficiencies drove the under-assessment: (1) the risk assessment did not account for concurrent PTW operations increasing supervisor workload, (2) equipment reliability was assumed rather than verified — the expired calibration was invisible to the assessment, (3) emergency response capacity was benchmarked against the pre-expansion facility footprint.

CORE DIAGRAM — INCIDENT MECHANISM

Tripod Beta Hazard-Event-Target identification



TRAJECTORY SPLIT

PREVENTION (Controls) — 3 barriers

Atmospheric verification (MISSING) · Gas detector calibration (FAILED) · Supervisor PTW oversight (FAILED)

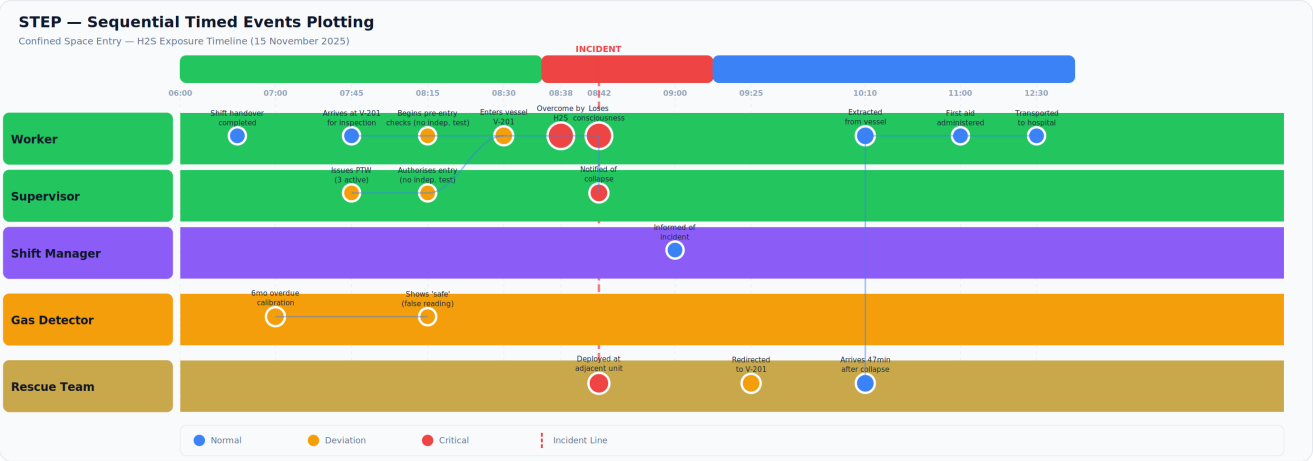
RECOVERY (Defences) — 2 barriers

Emergency rescue response (FAILED) · Backup rescue team (MISSING)

The core diagram defines what is being investigated. Prevention barriers stop the event from occurring — they are positioned between the hazard and the event. Recovery barriers limit the consequences once the event has occurred — they protect the target from the full impact. This incident had 3 failed or missing controls on the prevention trajectory and 2 failed or missing defences on the recovery trajectory, meaning the organisation had neither adequate prevention nor adequate consequence mitigation.

STEP — SEQUENTIAL TIMED EVENTS PLOTTING

Incident Timeline Reconstruction — 15 November 2025



TIMELINE ANALYSIS

The STEP chart reconstructs 18 events across 5 actors spanning 06:00 to 12:30. Three critical sequences demand management attention. First, the pre-entry phase (07:45-08:30) reveals the supervisor issued PTW while managing 3 concurrent confined space operations — the staffing model made inadequate oversight structurally inevitable. Second, the gas detector showed a 'safe' reading at 08:15 despite 6 months of expired calibration — the worker had no means of detecting the equipment failure. Third, the 47-minute gap between worker collapse (08:38) and rescue arrival (09:25) is the single factor that escalated this from a near-miss to a major injury. The rescue team was redeployed from an adjacent unit because no backup capability existed.

FAILED AND MISSING BARRIERS

5 barriers identified across prevention (controls) and recovery (defences)

Independent atmospheric verification

Control — MISSING

What: What: No requirement for independent atmospheric testing before confined space entry existed in the PTW system.

How: How: The PTW form did not include an independent verification field. Entry was authorised solely on the basis of the worker's portable gas detector reading.

Why: Why: The hazard identification process that designed the PTW system never identified the need for redundant atmospheric verification — a gap in the original hazard assessment.

Gas detector calibration (6 months overdue)

Control — FAILED

What: What: The portable gas detector's sensor had degraded beyond its calibration interval, producing false 'safe' readings.

How: How: Calibration tracking was manual. No automated alert existed. The PTW system did not check calibration status before authorising entry.

Why: Why: The calibration management system was disconnected from operational authorisation — a systemic gap between maintenance and operations.

Supervisor PTW oversight

Control — FAILED

What: What: The supervisor authorised entry while simultaneously managing 3 confined space permits across different locations.

How: How: Production schedule required 3 concurrent confined space entries. The staffing model allocated 1 supervisor to oversee up to 5 concurrent operations.

Why: Why: Staffing ratios were set for throughput, not safety oversight. The conflict between production and safety was structural and predictable.

Emergency rescue response

Defence — FAILED

What: What: The facility's single rescue team was deployed at an adjacent unit when the emergency occurred. 47 minutes elapsed before rescue.

How: How: No prioritisation protocol existed for competing emergency demands. The rescue team had no visibility of concurrent confined space operations.

Why: Why: The emergency response model had not been updated since the facility expanded from 3 to 7 operational units.

Backup rescue team

Defence — MISSING

What: What: No backup rescue capability existed anywhere in the facility's emergency response architecture.

How: How: The entire facility relied on a single rescue team with no contingency for simultaneous emergencies.

Why: Why: Emergency response resourcing was never scaled to match facility growth — a conscious organisational design decision.

CAUSATION PATHS

Each path traces: barrier → active failure → precondition → latent failure → GFT

Path 1: Atmospheric verification

GFT: IG

ACTIVE FAILURE Supervisor authorised entry without independent atmospheric test

↓

PRECONDITION Managing 3 simultaneous entries under production schedule pressure

↓

LATENT FAILURE Staffing model: 1 supervisor allocated for up to 5 concurrent entries

Evidence: PTW log #2025-V201, shift roster Nov-15, supervisor workload records

Why this matters:

This is a workload issue, not a training issue. The supervisor was competent but structurally overloaded. Retraining does not fix the staffing model — it was designed for throughput, not safety. The failure was predictable from the day the staffing ratio was set.

Path 2: Gas detector calibration

GFT: MM

ACTIVE FAILURE Sensor degraded past calibration interval by 6 months

↓

PRECONDITION Manual tracking system with no automated alerts to maintenance or operation

↓

LATENT FAILURE No integration between calibration management and PTW authorisation systems

Evidence: Calibration records (V-201 detectors), maintenance log, PTW system configuration

Why this matters:

Even if every procedure had been followed perfectly, the equipment would have produced a false 'safe' reading. Correct procedure + faulty equipment = false safety. The barrier was compromised before the worker entered the vessel — and invisibly so.

Path 3: Emergency rescue response

GFT: OR

ACTIVE FAILURE Single rescue team deployed at adjacent unit; no team available for V-201

↓

PRECONDITION No backup rescue capability; no prioritisation protocol for competing emerg

↓

LATENT FAILURE Emergency response model not updated since facility expansion from 3 to 7 u

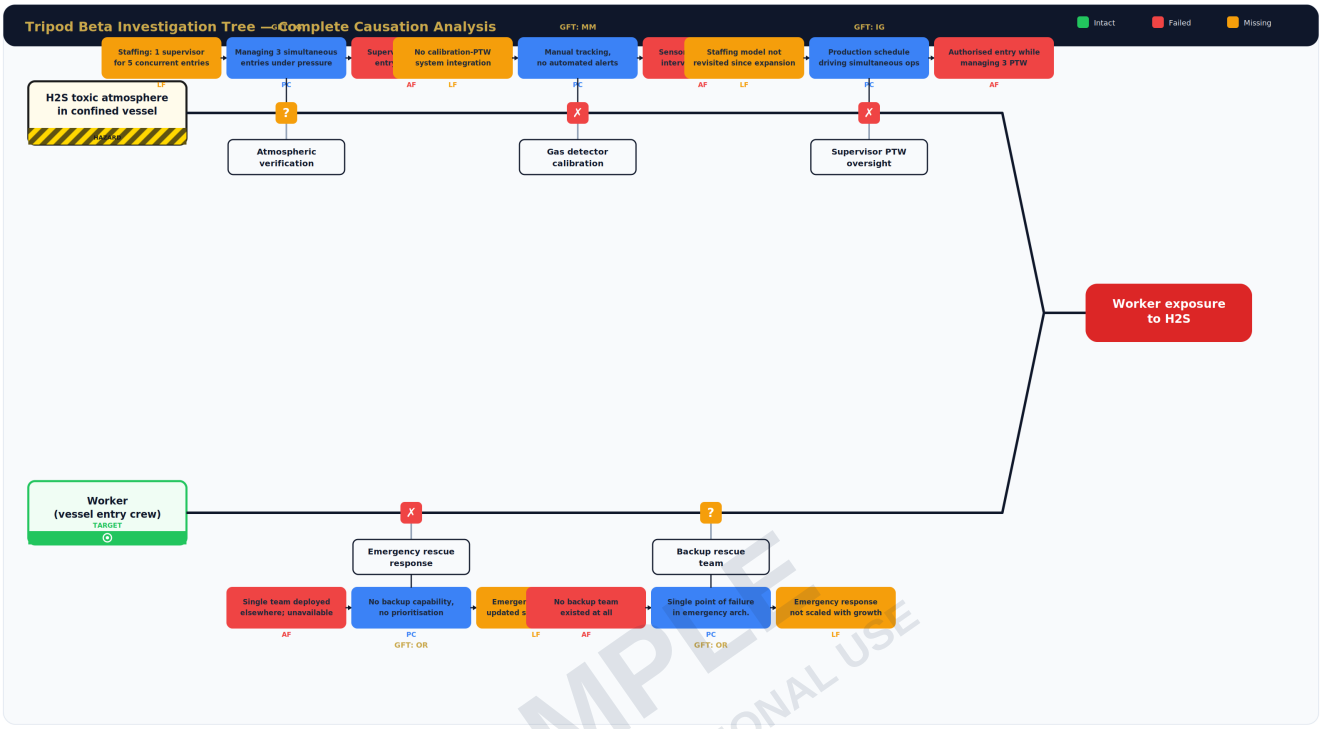
Evidence: Rescue deployment log, facility expansion records, emergency response plan v2.1

Why this matters:

The severity of this incident was directly determined by a resourcing decision made years before the event. The worker's injuries escalated from minor to major during the 47-minute rescue delay. This is not a failure of response execution — the team performed well once deployed. This is a failure of organisational design.

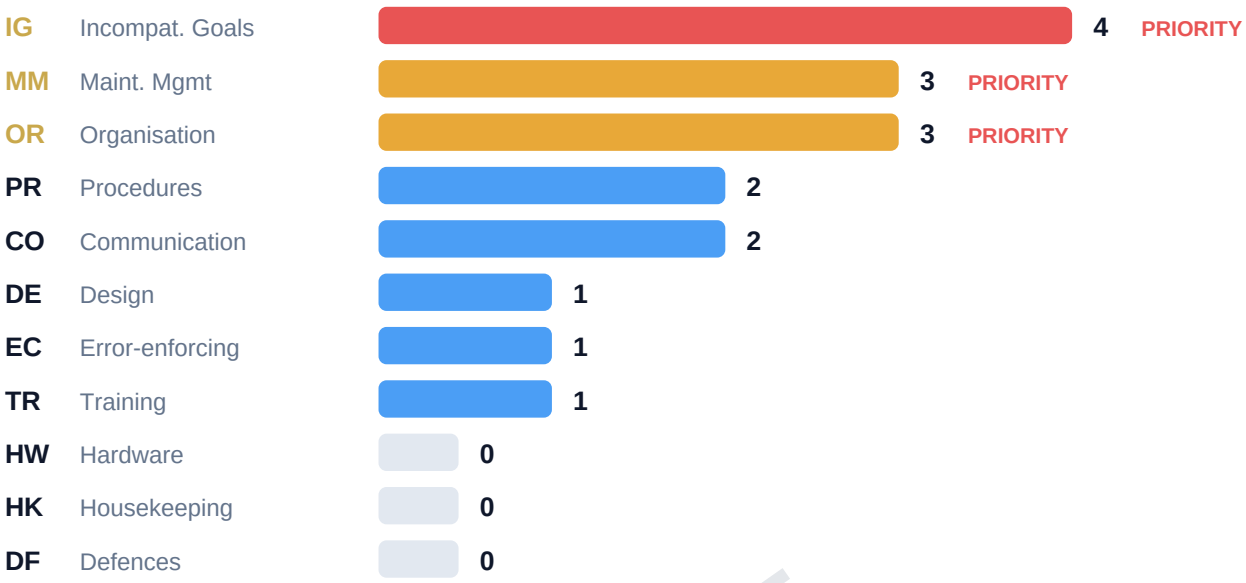
TRIPOD BETA CAUSATION TREE

Complete causation analysis — 5 barriers with full AF → PC → LF trajectories



RISK PROFILE — GENERAL FAILURE TYPES (GFT)

11 management domains classified by barrier failure origin



EXECUTIVE INTERPRETATION

The GFT profile reveals a concentrated failure pattern across three management domains that account for 77% of identified organisational weaknesses. This concentration indicates systemic rather than isolated issues.

IG — Incompatible Goals (Score: 4 — CRITICAL)

Production scheduling systematically overrides safety controls. The 1:5 supervisor ratio and concurrent confined space operations create structural conflicts where production throughput is prioritised over verification rigour. REQUIRED ACTION: Executive directive establishing maximum concurrent entry ratios as non-negotiable hard limits, with staffing model redesign within 30 days.

OR — Organisation (Score: 3 — PRIORITY)

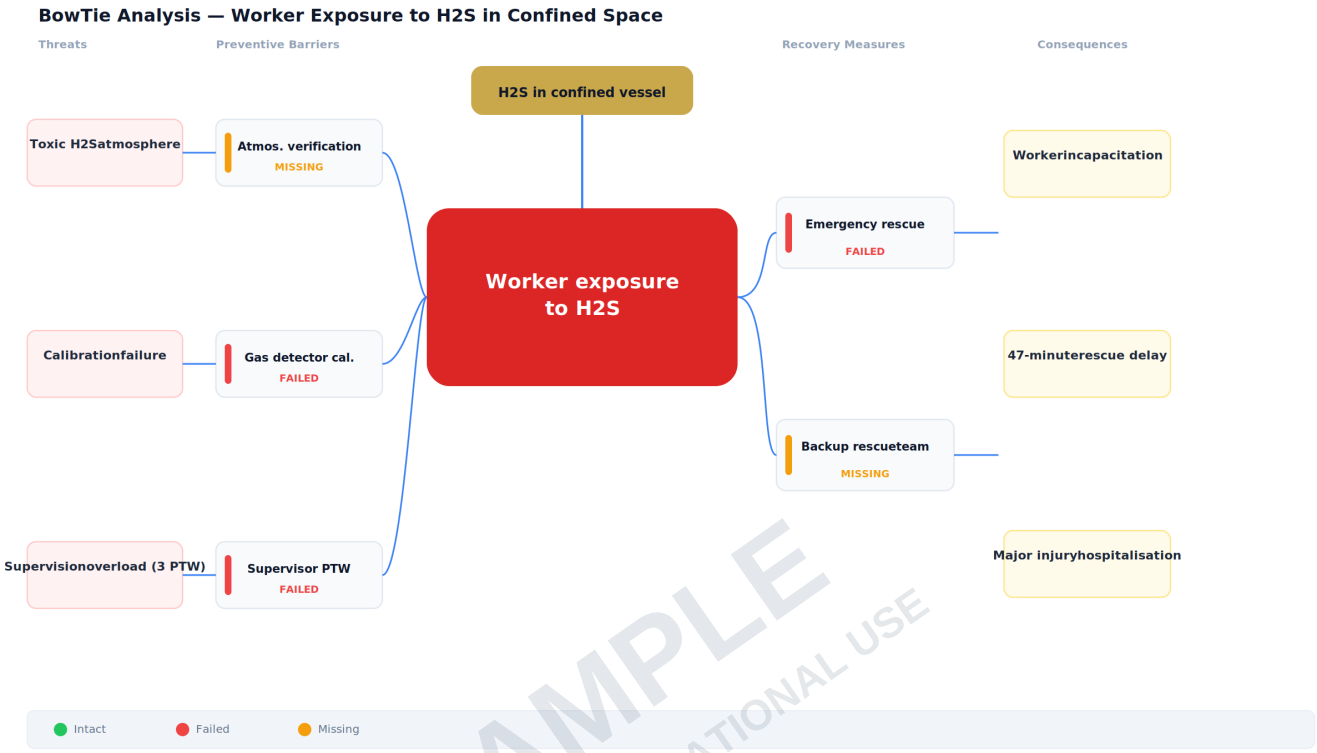
Emergency response architecture has not been updated since facility expansion from 3 to 7 units. The single rescue team model creates a single point of failure. The 47-minute rescue delay directly escalated injury severity. REQUIRED ACTION: Dedicated backup rescue team deployment within 60 days, with quarterly dual-team drills.

MM — Maintenance Management (Score: 3 — PRIORITY)

Calibration management operates in isolation from operational authorisation. Equipment with expired calibration can pass through PTW checks undetected. REQUIRED ACTION: System integration between calibration and PTW within 90 days — overdue calibration must block permit issuance.

BOWTIE DIAGRAM

Confined Space Entry — H2S Exposure — Formal Hazard Bow-Tie View



RECOMMENDATIONS

SMARTER framework: Specific · Measurable · Achievable · Relevant · Time-bound · Evidenced · Reviewed

PRIORITY DISTRIBUTION

4 HIGH
1 MEDIUM

4 of 5 require immediate management attention.

PRIORITY × BARRIER

Atmospheric verification	HIGH
Gas detector calibration	HIGH
Emergency rescue	HIGH
Supervisor oversight	HIGH
Gas detector	MEDIUM

RACI MATRIX

TIER	R	A	C	I
1: Mgmt Sys	OM	OD	HSE	Board
2: Latent	MM	OD	IT	HSE
3: Oper.	HSE	OM	Sup	MM

R=Responsible A=Accountable
C=Consulted I=Informed

TIER 1: MANAGEMENT SYSTEM INTERVENTIONS (GFT-DRIVEN)

REC-1 GFT: IG TIER 1 HIGH

Action: Restructure supervisor-to-entry staffing ratio. Establish maximum 2 concurrent confined space entries per supervisor as a non-negotiable hard limit designed into the PTW system.

Due: 30 days
Review: 90 days
Responsible: Operations Manager
Accountable: Operations Director
Evidence: Revised PTW system config + updated staffing policy

LEADING INDICATORS:

1. % of entries with ≤2 concurrent PTW per supervisor (target: 100%)
2. Monthly supervisor workload hours vs capacity limit
3. PTW rejection rate due to supervisor capacity (should increase initially)

REC-2 GFT: OR TIER 1 HIGH

Action: Scale emergency response to current facility footprint. Deploy dedicated backup rescue team resourced independently of the primary team. Quarterly dual-team response drills required.

Due: 60 days
Review: 120 days
Responsible: Operations Director
Accountable: Site General Manager
Evidence: Backup team deployment records + drill completion ce

LEADING INDICATORS:

1. Dual-team rescue availability rate (target: 100% during CSE ops)
2. Emergency response time to any unit (target: <10 minutes)
3. Quarterly drill completion rate + mean response time trend

TIER 2: LATENT FAILURE CORRECTIONS (ORGANISATIONAL CONDITIONS)

REC-3 GFT: MM TIER 2 HIGH

Action: Integrate calibration management directly into PTW authorisation. Overdue calibration must automatically block permit issuance. No manual override without HSE Manager sign-off.

Due: 45 days
Review: 90 days
Responsible: Maintenance Manager + IT
Accountable: Operations Director
Evidence: System integration test report + PTW block verificat

LEADING INDICATORS:
1. % of PTW checks with automated calibration verification (target: 100%)
2. Number of permits issued against expired equipment (target: 0)
3. Mean time from calibration expiry to equipment withdrawal

REC-4 GFT: IG TIER 2 HIGH

Action: Establish formal conflict resolution protocol for production vs safety. Any scheduling decision that requires >2 concurrent CSE operations must be approved by Operations Director with documented risk acceptance.

Due: 30 days
Review: 60 days
Responsible: Operations Manager
Accountable: Operations Director
Evidence: Conflict resolution protocol document + risk accepta

LEADING INDICATORS:
1. Number of >2 concurrent CSE operations requiring escalation
2. Production schedule compliance with CSE concurrent limits
3. Monthly safety-vs-production conflict log entries

TIER 3: OPERATIONAL CONTROLS (BARRIERS + PRECONDITIONS)

REC-5 GFT: MM TIER 3 MEDIUM

Action: Implement automated calibration alerting at 30-day, 14-day, and 1-day intervals. Alerts sent to both Maintenance and Operations. Equipment auto-flagged in PTW system at 1-day alert.

Due: 45 days
Review: 90 days
Responsible: Maintenance Manager
Accountable: Operations Manager
Evidence: Alert system configuration + quarterly audit of aler

LEADING INDICATORS:
1. % of calibration renewals completed before expiry (target: >95%)
2. Mean days between alert and calibration action
3. Number of 1-day alerts triggered per quarter (should trend to 0)

OVERALL RACI MATRIX

Recommendation	Ops Director	Ops Manager	HSE Manager	Maint Mgr	IT Manager
REC-1: Staffing ratio	A	R	C	I	I
REC-2: Backup rescue	A	C	C	I	I
REC-3: Cal-PTW integration	A	C	C	R	R
REC-4: Conflict protocol	A	R	C	I	I
REC-5: Cal alerting	I	A	C	R	C

R Responsible — does the work
A Accountable — owns the outcome
C Consulted — provides input
I Informed — kept updated

EVIDENCE TRACEABILITY

EVIDENCE QUALITY SCORE

68%

≥70 Strong | 40-69 Moderate | <40 Insufficient

EVIDENCE ITEMS

✓ **PTW Log #2025-V201** — Collected
Permit-to-Work · Links: atmospheric verification
Finding: No independent test field on permit form

✓ **Calibration records (V-201)** — Collected
Maintenance Log · Links: gas detector calibration
Finding: Last calibration 6 months prior to incident

■ **Rescue team deployment log** — Pending
Incident Record · Links: emergency rescue response
Finding: Awaiting extraction from operations system

✗ **Shift roster (Nov 15 coverage)** — Unavailable
Training Record · Links: supervisor oversight
Finding: Roster system archived monthly; November deleted

EVIDENCE GAPS

■ **Barrier: Backup rescue team**
Gap: No documentation of backup rescue capability
Recommended: Emergency response plan, resource allocation records, facility expansion audit

■ **Barrier: Atmospheric verification**
Gap: No PTW design review records
Recommended: Original PTW system design documents, hazard identification records

GLOSSARY & TERMINOLOGY

TRIPOD BETA METHODOLOGY

Active Failure	An unsafe act or omission by a person at the point of incident, traceable to pre conditions and latent failures.
Barrier	A control or defence designed to prevent or mitigate an unwanted event.
Causation Path	The trace from barrier failure through AF → PC → LF to organisational origin.
Control	A prevention barrier on the hazard side — stops the event from occurring.
Defence	A recovery barrier on the target side — limits consequences after the event.
HET Trio	Hazard-Event-Target: the incident mechanism model defining what is investigated.
Latent Failure	An organisational decision or condition that existed before the incident.
Precondition	A state or circumstance created by latent failures that enabled the active failu re.
Trajectory	The causal chain from latent failure through precondition to active failure.

GFT CATEGORIES (11 management domains)

CO	Communication	Clarity of operational information
DE	Design	Engineering of hardware and workplace
DF	Defences	Adequacy of recovery provisions
EC	Error-enforcing	Conditions that provoke human error
HK	Housekeeping	Order and cleanliness of workplace
HW	Hardware	State and suitability of equipment
IG	Incompat. Goals	Conflict between production and safety
MM	Maint. Mgmt	Quality of maintenance regime
OR	Organisation	Structure, staffing, and resourcing
PR	Procedures	Quality and availability of procedures
TR	Training	Competence development and assurance

ABBREVIATIONS

AF	Active Failure	BRF	Barrier Risk Factor	GFT	General Failure Type	HET	Hazard-Event-Target
LF	Latent Failure	PAER	People-Assets-Env-Rep	PC	Precondition	PTW	Permit to Work
RAM	Risk Assessment Matrix	STEP	Seq. Timed Events Plotting				

DISCLAIMER

This analysis was produced using the RISKSORA Investigation Copilot, powered by Tripod Beta methodology and AI-driven causation analysis. It should be reviewed by qualified investigators before inclusion in formal reports. It does not constitute a legal determination, assign liability, or replace professional engineering or safety judgment. All personally identifiable information has been redacted. Facility and company names have been generalised for confidentiality.

METHODOLOGY

Tripod Beta is a scientifically developed incident investigation methodology maintained by the Stichting Tripod Foundation and published by the Energy Institute. It traces barrier failures through active failures, preconditions, and latent failures to classify organisational weaknesses using 11 General Failure Types (GFTs). This approach ensures investigations reach the organisational conditions that allowed harm, rather than stopping at individual behaviour.

RISKSORA
risksora.com
HSESKILLS Ltd