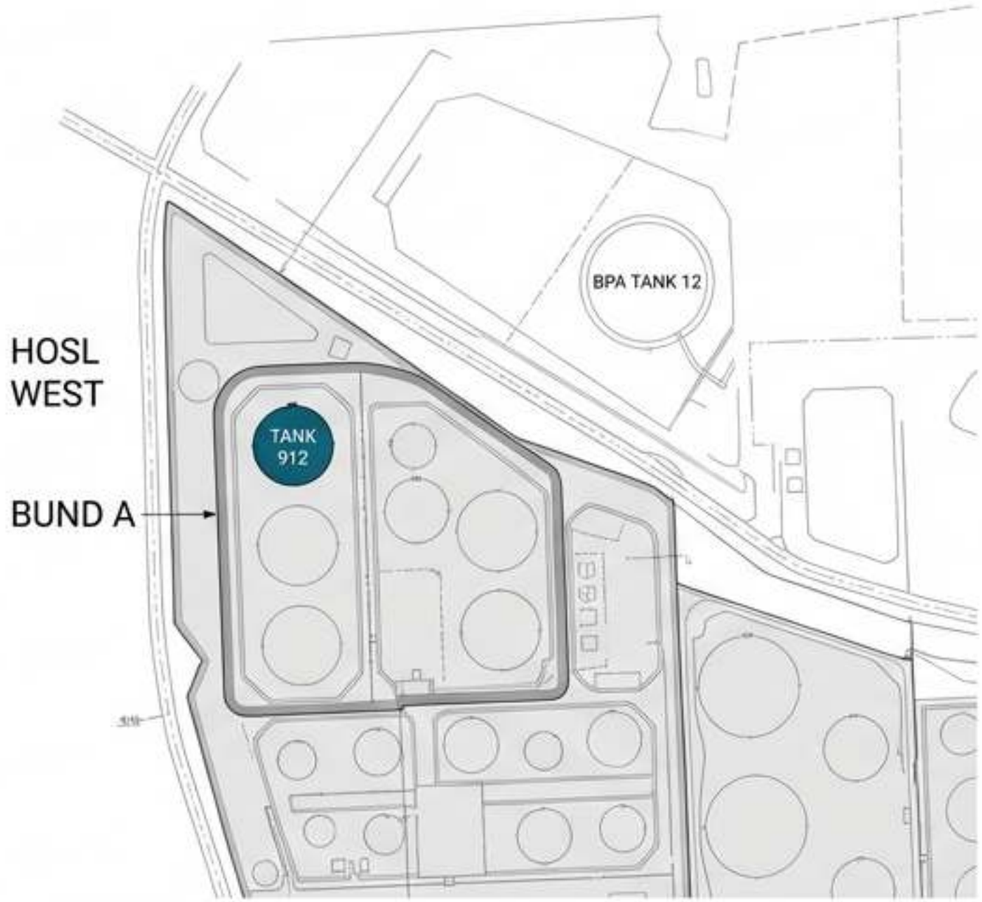
Buncefield Oil Storage Depot Explosion

A system-level examination of storage control, protection, and escalation.

SOURCE: MAJOR INCIDENT INVESTIGATION BOARD FI

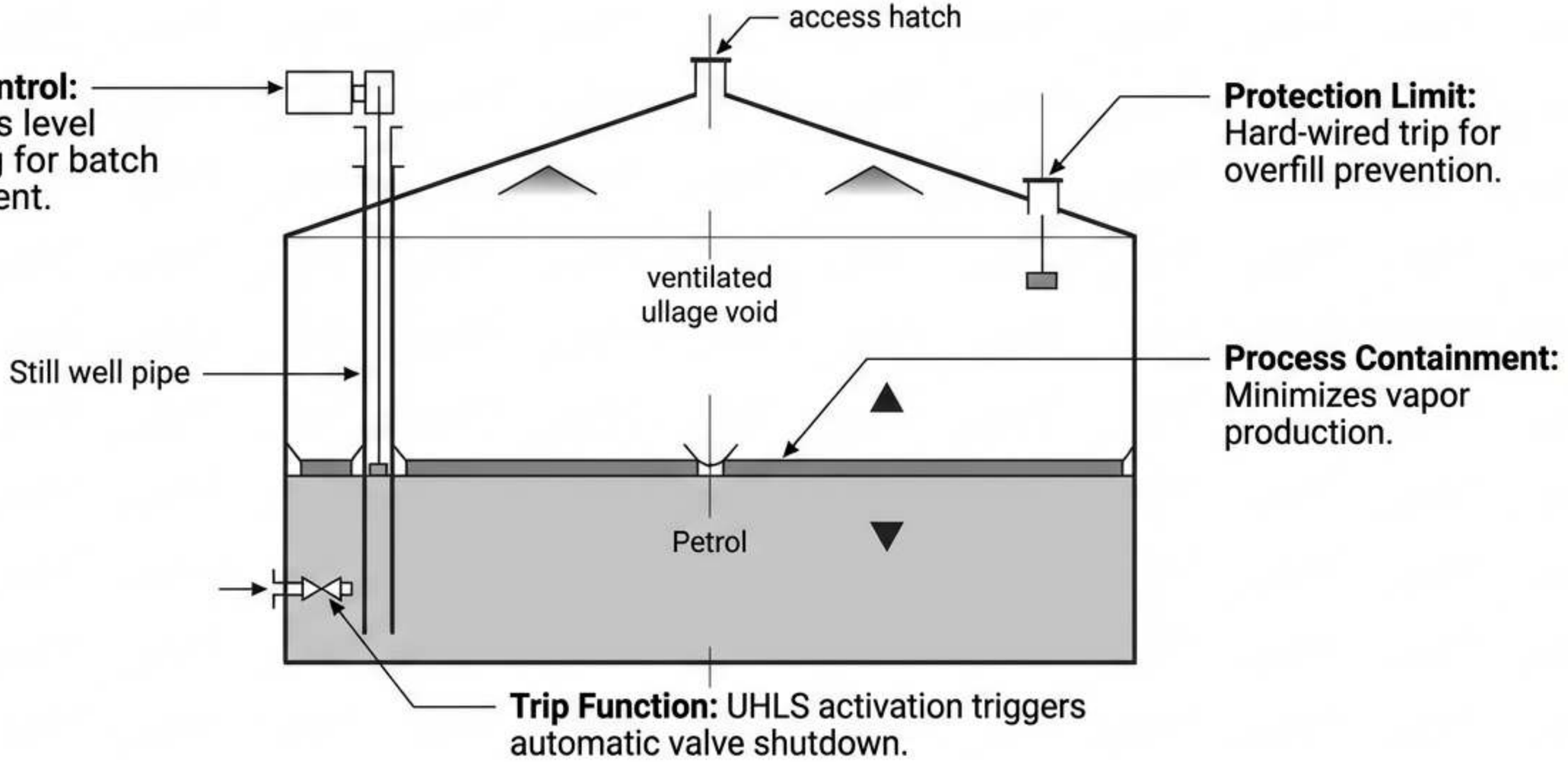
HOSL West: System Boundaries and Critical Components



System Architecture and Boundaries

- Primary Inputs: Three major pipeline systems (FinaLine, M/B North, T/K South).
- Storage Node: HOSL West containment area / Tank 912.
- Control Layer: Automatic Tank Gauging (ATG) with servo-operated level gauges.
- Protection Layer: Independent Ultimate High-Level Switches (UHLS).
- Criticality: High-flow transfer management (up to 890 m^3/hour) within finite containment.

Intended System Function



Operating Context: Night of Dec 10–11, 2005

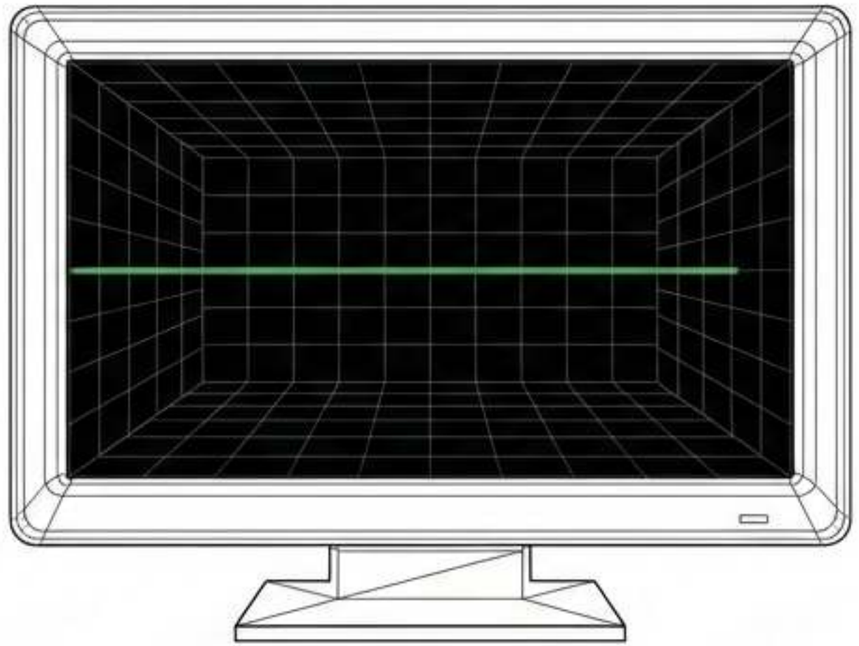
Activity: Tank 912 receiving split-stream delivery.

↓

Flow Dynamics: Rate increased from 550 to 890 m^3/hour (Kingsbury line closure).

↓

Monitoring: Operators relied on remote ATG display.



SYSTEM STATE: SILENT

Absence of high-level alarm interpreted as confirmation of safety.

Functional Failure Analysis

✗ Loss of Observability

(ATG failed to track rising level).

✗ Loss of Protection

(UHLS failed to trip).

✗ Loss of Vapor Control

(Floating deck bypassed; fuel exited roof vents).

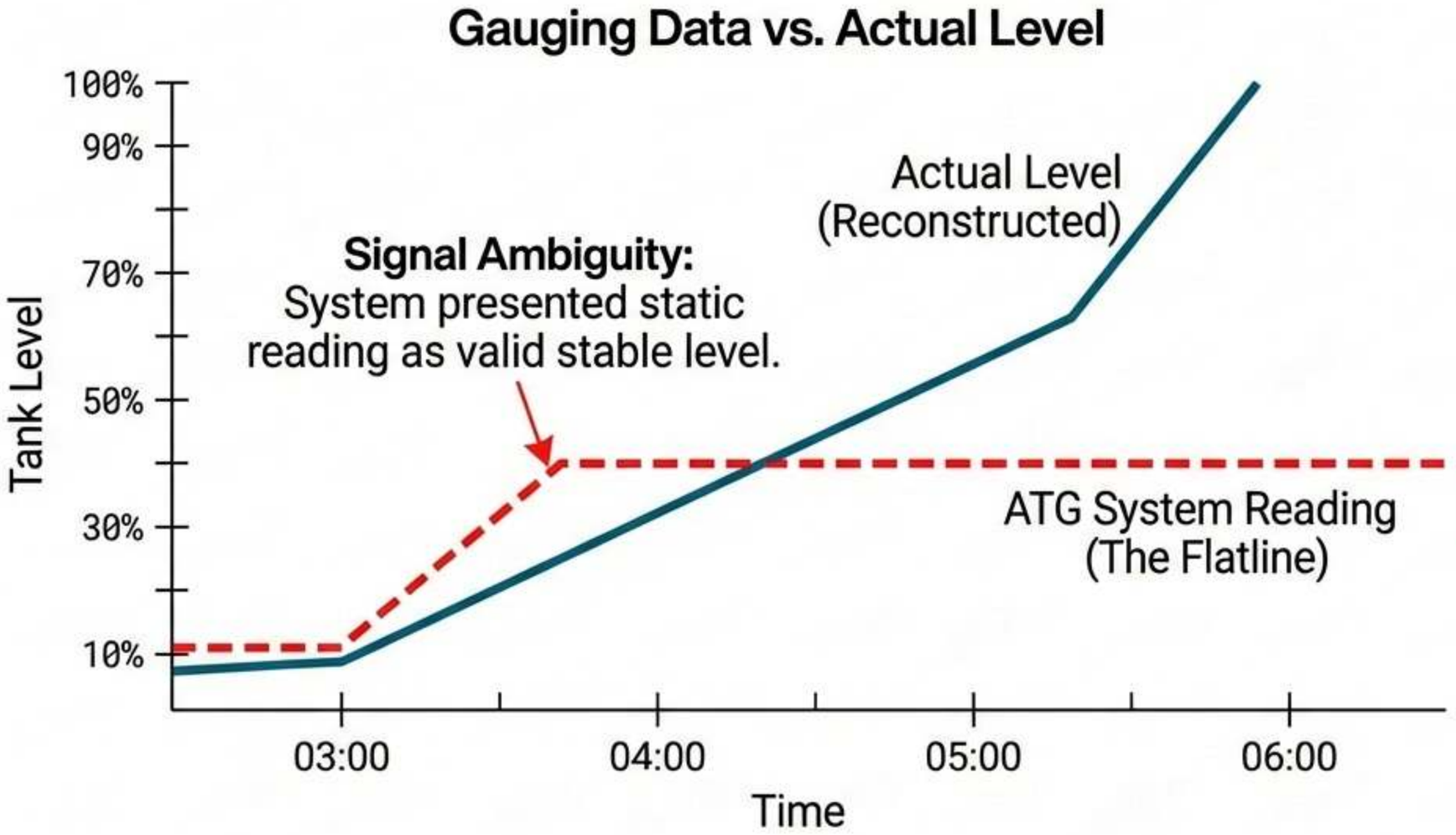
Roboto Mono

✗ Loss of Containment

(Tank structure breached).

Roboto Mono

Warning Signs That Were Present

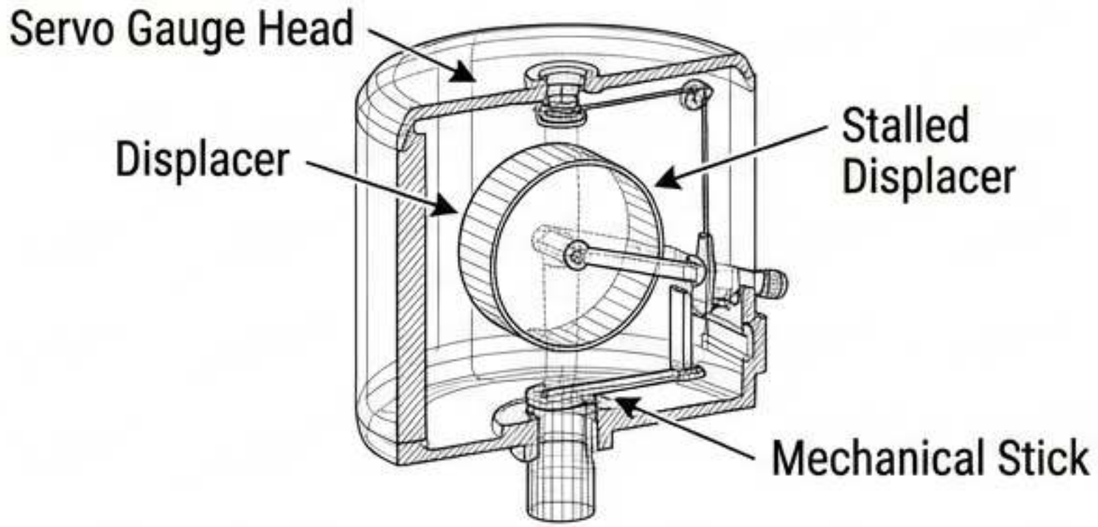


Lack of Correlation:
No logic alarm generated for "Inlet Valve Open" + "Level Static".

Lack of Correlation:
No logic alarm generated for "Inlet Valve Open" + "Level Static".

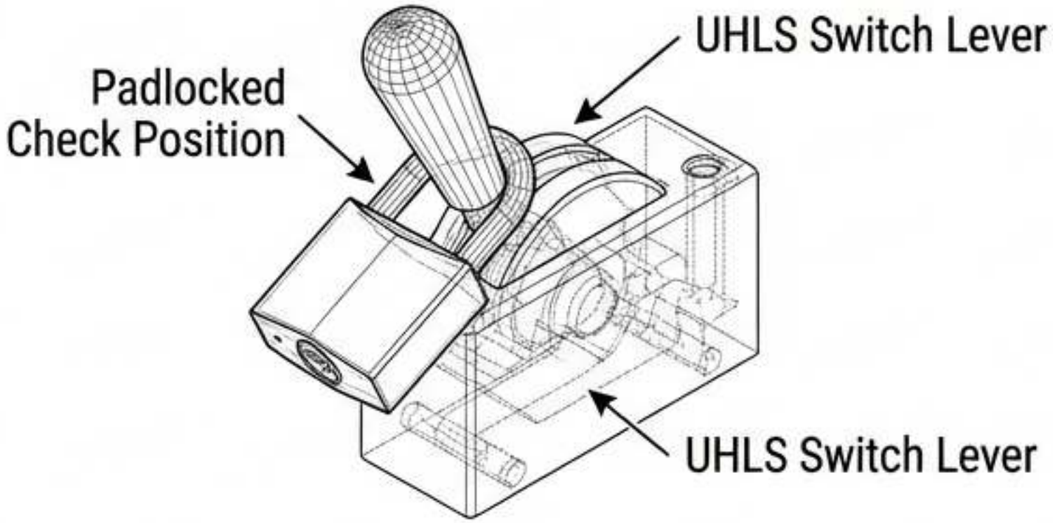
Roboto Mono

Plausible Failure Mechanisms



Control Failure (ATG)

Consistent with mechanical stick of servo gauge or stalled displacer. Feedback loop open.

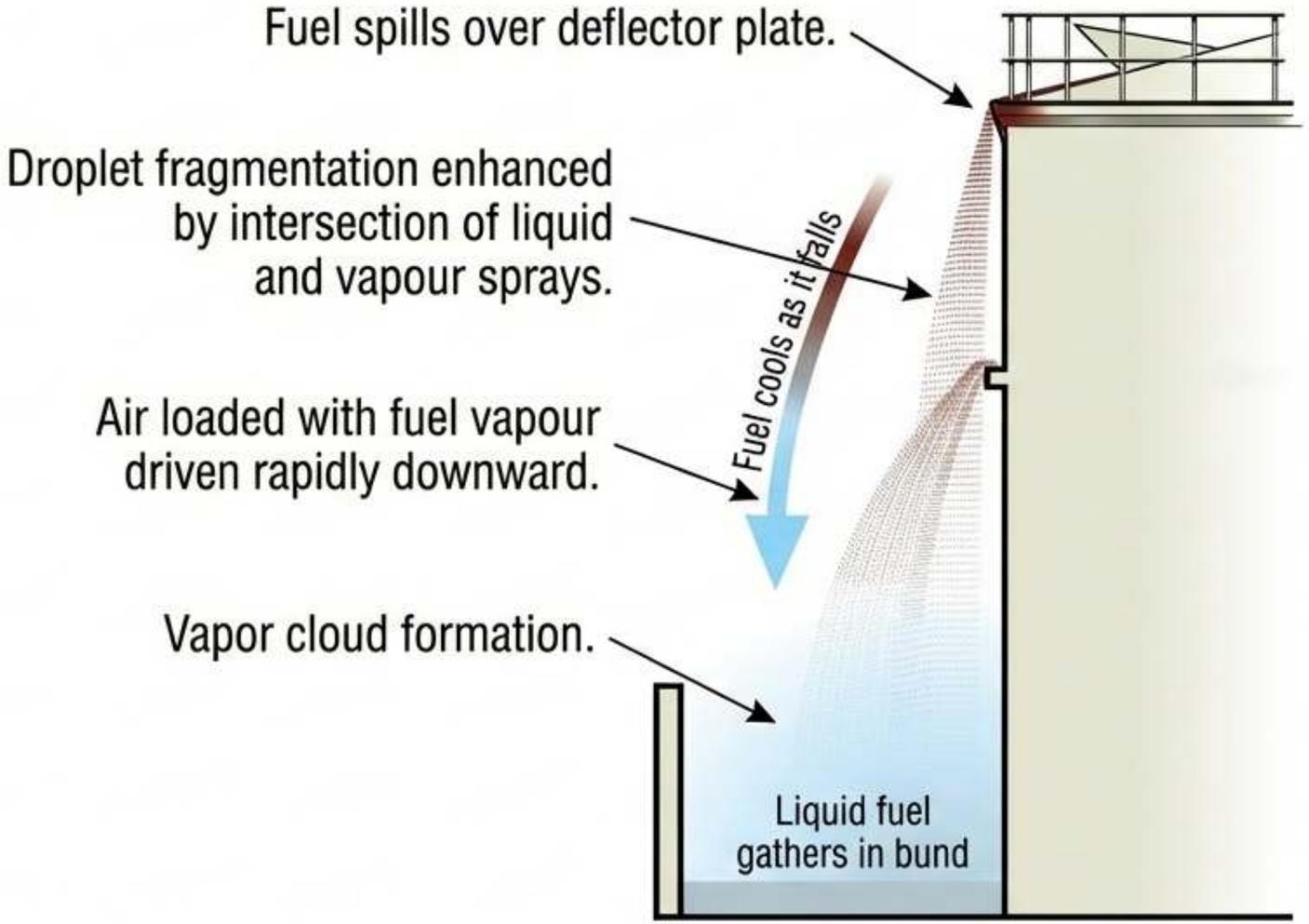


Protection Failure (UHLS)

Consistent with switch lever left in “padlocked check” position. Mechanically inhibited.

Dormant Failure: The protection layer was physically disabled (testing gap) without annunciating “disabled” status to the control room.

Dynamics of Containment Loss



Escalation Mechanism: Interaction with wind wind girders turned liquid stream into fine mist/vapor. Defeated “pool fire fire” containment models.

Consequences: Impact and Magnitude

Human Impact: 43 injuries.

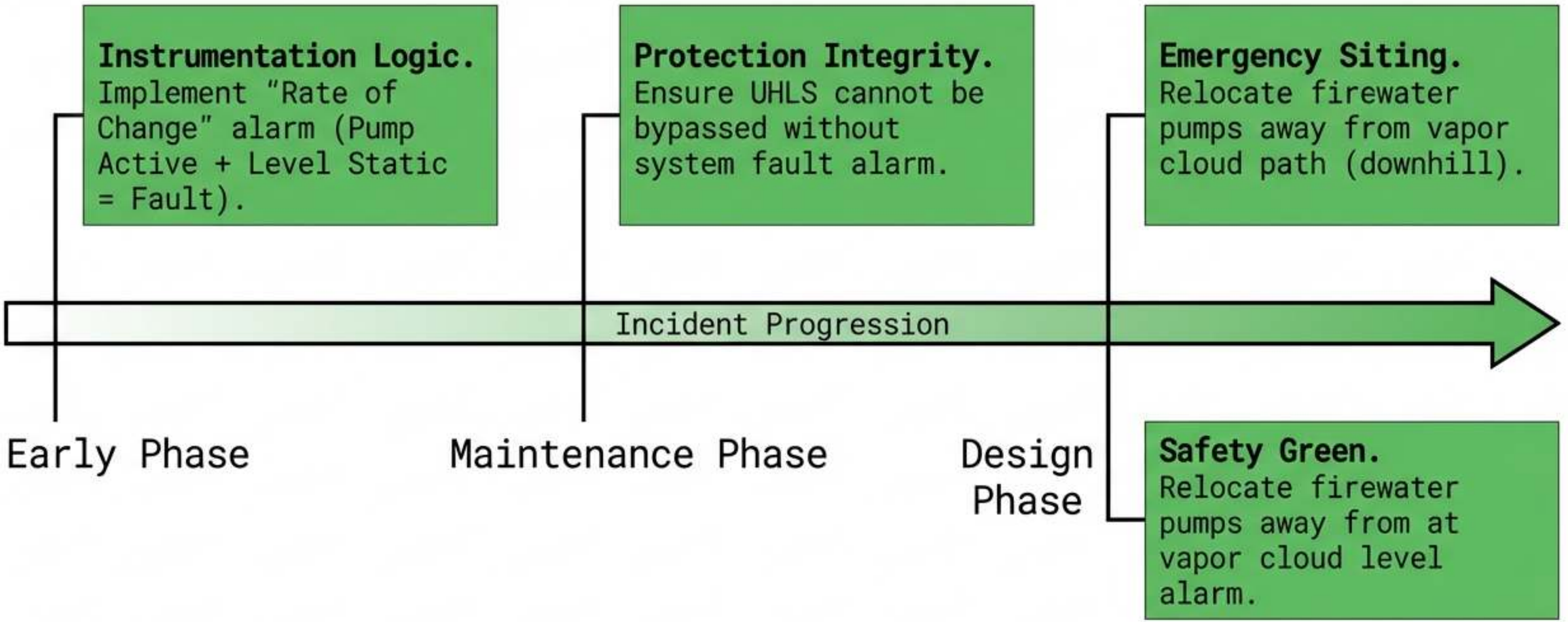
Asset Destruction: Total loss of 20+ fuel storage tanks.

Infrastructure: Loss of strategic supply to Heathrow/Gatwick. M1 Motorway closed.

Environmental: Pollution plume over Southern England. Risk to chalk aquifer.

Economic: Major disruption to Maylands Industrial Estate.

System Vulnerabilities and Intervention Points



Transferable Insight

The Trap of Silence.

Absence of evidence (no alarm) is often mistaken for evidence of absence (no danger).

Dormant Failures.

Protection layers often fail silently and remain failed until a demand is placed upon them.

Independence vs. Diversity.

Physical separation does not guarantee independence if maintenance procedures or failure modes are common.

Change of State.

High-rate transfers introduce dynamic risks (vapor generation) not predicted by static models.

Which of our protection systems give us confidence — and which give us evidence?