

Level Instrumentation & Alarm Safety: Safety-Critical Vessel Level Protection

A verification checklist for level redundancy, diagnostics, and alarm management

When a single level transmitter freezes and the backup trip has been left out of service, the control screen lies and a tower fills past full with nobody watching. This checklist captures the verification steps that prevent the failure mode behind a documented refinery overfill — a stuck displacer, a dead high-level switch, and an alarm flood that buried the one alarm that mattered.

Use it when commissioning or auditing level protection on safety-critical vessels, and during startup readiness reviews. Sign each line. Treat a flatlined signal as a fault until proven otherwise.

COMPANION RCA

Blinded by the HMI: The Splitter
Tower Level Transmitter Failure

AUDIENCE

Process control engineers, I&E
technicians, operations supervisors

STANDARDS

IEC 61511 / ISA-84, ISA-18.2, API
RP 551, OSHA 1910.119

Use this checklist to verify level protection on any safety-critical vessel. Each item must be verified by the responsible engineer or qualified technician. If you cannot verify an item, the protective function is not credited.

1. LEVEL REDUNDANCY AND DIVERSITY

☐ **High-hazard vessels use diverse level technologies.**

Two independent measurement physics (for example, guided-wave radar plus a mechanical displacer) to defeat common-mode failure.

☐ **Safety high-level trip is independent of the control transmitter.**

The protective high-level switch is a separate device wired directly to the emergency shutdown system, not shared with control.

☐ **Backup trip proof-tested within its defined interval.**

Functional proof test performed and recorded on schedule. An untested trip is not a credited protection layer.

PASS CRITERIA – PROOF TESTING

Proof-test interval set from the LOPA / SIL calculation, not convenience. Record the **as-found** and **as-left** state of every safety trip. A device left out of service is bypassed only under a documented MOC.

2. CONTROL SYSTEM AND HMI DIAGNOSTICS

☐ **Flatline / rate-of-change diagnostics active on critical transmitters.**

Logic raises a diagnostic alarm when a signal stays mathematically constant during active filling or transfer.

☐ **HMI distinguishes safety-critical alarms from process alerts.**

Priority, colour, and audible coding make the critical alarm unmistakable against routine alerts.

☐ **Active alarm count managed within ISA-18.2 limits.**

Stale and chattering alarms suppressed; alarm rationalization in place so operators can see what matters.

PASS CRITERIA – ALARM RATE

Target an average of fewer than 1 alarm per 10 minutes per operator under normal operation (ISA-18.2). Investigate any standing alarm flood before crediting operator response as a layer.

3. OPERATIONS & BYPASS CONTROLS

☐ **Formal authorization required to bypass a level transmitter or trip.**

Bypasses logged, time-limited, alarmed, and removed under a controlled procedure.

☐ **Operators verify suspect readings with an independent check.**

A flatlined or doubtful level is confirmed by a diverse instrument or physical check before continuing to fill.

☐ **Safety-critical instrument status reviewed at shift handover.**

Out-of-service trips and known instrument faults are communicated and acknowledged at every shift change.

4. MECHANICAL INTEGRITY & RELIEF PATH

☐ **Safety-critical instruments in the mechanical-integrity program.**

Transmitters, switches, and final elements inspected and tested under PSM mechanical integrity (OSHA 1910.119).

☐ **Overfill relief routed to a safe destination.**

Relief and blowdown directed to a closed flare or safe containment — not an atmospheric vent stack near occupied areas or ignition sources.

REFERENCE STANDARDS

- **IEC 61511 / ISA-84** — Functional safety; independent protection layers and proof testing
- **ANSI/ISA-18.2** — Alarm management lifecycle; elimination of alarm floods
- **API RP 551** — Process measurement; diverse/redundant level for high-level trips
- **API RP 754** — Process safety performance indicators
- **OSHA 29 CFR 1910.119** — Process Safety Management; mechanical integrity of safety devices

DISCLAIMER & LIMITATION OF LIABILITY

This checklist is provided for educational and informational purposes only. It is a general industry reference, not a site-specific procedure, engineering specification, or legal compliance document. It does not replace the judgement of a qualified person, professional engineer, or authority having jurisdiction (AHJ).

Codes, standards, and regulations are revised periodically and vary by jurisdiction. **Verify the current edition of all referenced codes (CEC, NEC, CSA, NFPA, API, OSHA) and any provincial, state, or local amendments that apply to your work site before relying on the items listed here.** Where any

conflict exists between this checklist and the applicable code, regulation, or your employer's safe work procedure, the code, regulation, or procedure governs.

ELI Intelligence and the authors of this material disclaim all liability for any loss, injury, or damage arising from the use of, or reliance on, this checklist. Use at your own risk and only under the supervision of competent persons trained for the work being performed.

GET THE FULL RCA AND THE NEXT CHECKLIST

This checklist accompanies the full incident analysis at safetyblog.eli-intelligence.com. New incident RCAs and field checklists publish every Friday. Subscribe at the site footer to get them in your inbox the morning they go live.