SAFETY CANON

2026-03-18

Dexter Hadley, MD/PhD

Hadley Lab CANONIC

Abstract

Example

Contents

Hazards MUST be identified, assessed, and mitigated through systematic risk analysis.

Example: Risk assessment matrices severity (catastrophic, critical, marginal, negligible) Œ probability (frequent, probable, occasional, remote, improbable). FMEA/FMECA (Failure Mode and Effects Analysis/Criticality Analysis) identifies potential failure modes, their causes, effects, and severity. HAZOP (Hazard and Operability Study) systematic examination of deviations from design intent in process systems. ISO 14971 (medical devices) risk management process: risk analysis, risk evaluation, risk control, overall residual risk evaluation, risk management review, production/post-production monitoring.

0.1 2. Functional Safety

Critical systems MUST achieve safety integrity levels appropriate to the risk of the application.

Example: IEC 61508 foundational functional safety standard for electrical/electronic/programmable electronic safety-related systems. SIL (Safety Integrity Level) 1-4 quantitative reliability targets. ISO 26262 (automotive) ASIL A-D (Automotive Safety Integrity Level), covering concept through decommissioning. DO-178C (avionics software) and DO-254 (airborne electronic hardware) DAL A-E (Design Assurance Level). IEC 62443 (industrial automation and control systems) security levels for OT environments. Each domain defines its own levels but the principle is universal: higher risk = higher integrity requirement = more rigorous verification.

0.2 3. Occupational Safety

Workplaces MUST protect workers from recognized hazards through engineering controls, administrative controls, and PPE.

Example: OSHA (29 CFR 1910 general industry, 1926 construction) General Duty Clause (Section 5(a)(1)) requires employers to provide workplaces free from recognized hazards likely to cause death or serious physical harm. NIOSH (National Institute for Occupational Safety and Health) research and recommendations. Hierarchy of controls: elimination, substitution, engineering controls, administrative controls, PPE (least effective). PSM (Process Safety Management, 29 CFR 1910.119) 14 elements for highly hazardous chemicals. Permissible Exposure Limits (PELs), Threshold Limit Values (TLVs), and Recommended Exposure Limits (RELs) for workplace chemical exposure.

0.3 4. Product Safety

Products MUST meet applicable safety standards before market entry. Recalls MUST be executed when safety defects are identified.

Example: CPSC (Consumer Product Safety Commission) administers CPSIA (Consumer Product Safety Improvement Act). Mandatory reporting under Section 15(b) manufacturers must report products presenting substantial hazard. UL (Underwriters Laboratories), CSA (Canadian Standards Association), CE marking (EU Declaration of Conformity). Product liability theories: strict liability (Restatement 3rd, Torts), negligence (failure to exercise reasonable care), breach of warranty (express/implied). Recall management: effectiveness checks, consumer notification, remedy (repair, replacement, refund). RAPEX (EU rapid alert system for dangerous non-food products).

0.4 5. Root Cause Analysis

Failures MUST be investigated to identify root causes, not just proximate causes.

Example: TapRooT structured root cause analysis methodology with human factors consideration. AcciMap sociotechnical accident analysis mapping organizational factors across system levels. STAMP/STPA (Systems-Theoretic Accident Model and Processes) Levesons method treating safety as a control problem, not just component reliability. Swiss cheese model (Reason, 1990) accidents result from alignment of holes in multiple defensive barriers. Just culture (Dekker) distinguishes human error (consolable), at-risk behavior (coachable), and reckless behavior (punishable). Blame-free reporting systems increase incident reporting rates by 3-5x.

0.5 6. Incident Investigation

Safety incidents MUST be reported, investigated, and result in documented corrective actions.

Example: OSHA recordkeeping (29 CFR 1904): Form 300 (Log of Work-Related Injuries/Illnesses), 300A (Summary, posted Feb 1 - April 30), 301 (Incident Report). Severe injury reporting: fatality within 8 hours, hospitalization/amputation/eye loss within 24 hours. Near-miss reporting captures precursor events before harm occurs. Sentinel event review (Joint Commission) patient safety events requiring root cause analysis and action plan within 45 days. NTSB methodology (transportation) independent investigation, probable cause determination, safety recommendations. Aviation Safety Reporting System (ASRS/NASA) confidential, voluntary, immunity-providing incident reporting.

---

1. Constraints

```
MUST:     Cite specific safety standard or regulation
MUST:     Distinguish between safety integrity levels
MUST NOT: Present compliance with one domain's safety
```

SAFETY | CANON | HORIZONTAL