ROBOTICS CANON

2026-03-18

Dexter Hadley, MD/PhD

Hadley Lab CANONIC

Abstract

Example

Contents

No physical action MUST occur without governance verification at the required safety integrity level.

Example: ISO 10218-1:2011 (Industrial Robots Safety Requirements) defines performance levels for safety-related control systems. A collaborative robot (cobot) performing pick-and-place in a shared workspace MUST verify: (1) force/torque limits per ISO/TS 15066 (biomechanical load limits 150N max transient contact force for chest, 280N for upper arm), (2) speed limits (250mm/s max in collaborative mode), (3) workspace boundaries via safety-rated monitored stop or hand guiding. IEC 61508 SIL determination: SIL 1 (negligible), SIL 2 (marginal), SIL 3 (critical), SIL 4 (catastrophic). MAGIC gate: bitwise AND of required SIL dimensions before actuator command executes.

0.1 2. Sensor-Evidence Chain

All perception data MUST be logged as immutable evidence with timestamp, source, and confidence.

Example: A surgical robot (da Vinci Xi) captures: stereo endoscope video (30fps, timestamped), instrument kinematics (1kHz joint angles, torques), force feedback (6-axis force/torque sensor), patient registration (CT/MRI overlay). Evidence chain: sensor preprocessor fusion decision command actuator outcome. Each stage produces auditable artifacts. IEC 62304 Class C (life-sustaining/life-supporting) requires full traceability from hazard analysis through verification. ISO 13482:2014 covers personal care robots (physical assistant, mobile servant, person carrier).

0.2 3. Real-Time Temporal Integrity

Action timing MUST be verified against safety bounds with deterministic latency guarantees.

Example: Industrial robot safety response time: emergency stop 500ms (ISO 10218-1, 5.4.3). Automotive ADAS: braking reaction 150ms (ISO 26262 timing analysis). Surgical robot: instrument following 10ms latency (haptic transparency). Real-time operating systems (RTOS): VxWorks, QNX, FreeRTOS-SMP provide deterministic scheduling. Worst-case execution time (WCET) analysis per DO-178C for aviation. IEC 61508 requires proof of response time for each SIL level. Jitter bounds: SIL 3 requires <1ms jitter for safety-critical control loops.

0.3 4. Workspace Boundaries

Robot operating envelope MUST be enforced through safety-rated monitored zones with governance verification.

Example: ISO 10218-2:2011 (Robot Systems Integration) defines safeguarded spaces: (1) maximum space volume reachable by any moving part, (2) restricted space portion limited by devices, (3) operating space portion used during program execution. Safety-rated soft axis limiting (SLS) per IEC 61800-5-2. Virtual fencing via safety-rated 3D cameras (e.g., SICK microScan3, Keyence SZ series). Collaborative workspace per ISO/TS 15066: speed and separation monitoring (SSM), hand guiding, safety-rated monitored stop, power and force limiting (PFL). Geofencing for autonomous mobile robots (AMRs) per ISO 3691-4.

0.4 5. Autonomous Operation

Governance-verified control loops MUST maintain safety invariants across all operating modes.

Example: SAE J3016 autonomy levels adapted for robotics: Level 0 (manual), Level 1 (assisted single axis), Level 2 (partial multi-axis), Level 3 (conditional robot manages within ODD), Level 4 (high robot handles all scenarios in ODD), Level 5 (full no human needed). Operating Design Domain (ODD) specifies conditions under which autonomous operation is governed. Mode transitions (autonomous manual emergency stop) require governed state machine. ROS 2 lifecycle management: unconfigured inactive active finalized. ISO 13849-1 performance levels (PL a-e) for safety-related control.

0.5 6. System Architecture

Hardware, software, and safety systems MUST be architecturally separated with defined interfaces and governance at each layer.

Example: IEC 61508 reference architecture: sensors safety logic solver actuators, with independent safety monitoring. Redundancy patterns: 1oo1 (single channel), 1oo2 (dual with voting), 2oo3 (triple modular redundancy TMR). Hardware Fault Tolerance (HFT): SIL 3 requires HFT 1 (at least dual-channel). Software architecture per IEC 62443 zones and conduits: safety zone (SIL-rated), control zone (real-time), enterprise zone (IT). ROS 2 architecture: DDS middleware, lifecycle nodes, managed execution. URDF/SDF for robot description. MoveIt for motion planning with collision avoidance.

---

1. Constraints

```
MUST:     Cite ISO 10218, ISO/TS 15066, IEC 61508, or
MUST:     Map safety integrity level to MAGIC checkset
MUST:     Distinguish between industrial, collaborativ
MUST NOT: Present ungoverned autonomous operation as a
```

ROBOTICS | CANON | VERTICALS