

Industrial Robot Safety Beyond Binary Permit-Suppress

by [Nick Clark](#) | Published April 25, 2026

What Industrial Robotics Safety Currently Provides

Industrial robotics has been built on a fenced-cell model: high-power industrial robots (FANUC, ABB, KUKA, Yaskawa) operate inside light-curtained or hard-fenced cells with humans excluded during operation. ISO 10218 specifies the safety integrity. The safety logic is binary: the cell is operating, the cell is halted, transitions between the two require explicit safe-state confirmation.

Collaborative robots (Universal Robots, FANUC CR series, ABB YuMi, Doosan, Techman) extend operation outside fenced cells under ISO/TS 15066 power-and-force-limiting. The safety logic remains binary: the robot operates within force limits, or it halts on contact. The model works for the constrained collaborative regime it was specified for; it does not scale to broader autonomous-mobile, autonomous-manipulation, or human-collaborative-manipulation use cases.

Why Binary Architecture Limits Human-Collaborative Robotics

The economic case for human-collaborative robotics depends on robots performing meaningful work in shared spaces. The binary architecture supports this only at the

most constrained envelope: low force, low speed, contact-stop, with force-limiting hardware doing most of the safety work. Performance in this envelope is structurally limited because the architecture cannot distinguish between 'unexpected contact requiring halt' and 'expected contact requiring graceful continuation.'

Graduated modes change this. The same robot can operate in full mode in a fenced configuration, in stage-gated mode during human-collaborative manipulation (each contemplated motion verified against the human's observed state), in shadowed mode during teleoperation skill transfer, and in advisory mode during programming-by-demonstration. The modes are governance-credentialed and configurable per use case.

How Confidence Governance Sits Above ISO Safety

Confidence-governed actuation does not replace ISO 10218 / 13849 / 15066. It sits above them. The ISO-specified safety logic remains the floor — the absolute bound below which actuation is unconditionally suppressed. Above that floor, the graduated modes operate, with the mode selection consuming the human-presence observations, the planned-motion details, the operating envelope, and the credentialed governance policy.

The integration is structural. ISO logic gates the worst-case fault response. Graduated modes shape the routine operation. The two compose: the robot operates in stage-gated mode during human-collaborative manipulation, with the ISO floor still gating any contemplated motion that would exceed force limits. The architecture is additive, not replacing; existing safety certification remains valid.

What This Enables for Industrial Automation

The economic potential of human-collaborative robotics is large but constrained by the binary architecture. Symbotic, Locus Robotics, Boston Dynamics' Stretch, Agility Robotics' Digit — all are building toward broader autonomous-manipulation roles in shared human spaces. Each faces the same architectural mismatch between binary safety and graduated operational requirements.

Graduated modes plus reversibility-aware commitment plus post-actuation verification provide the architectural primitive that supports the shared-space autonomous-manipulation regime. The patent positions the primitive at the layer above ISO safety, applicable across the FANUC / ABB / KUKA / Yaskawa industrial layer, the UR / Doosan collaborative layer, and the emerging humanoid / mobile-manipulator layer. The competition shifts from safety-integrity certification to architecture-fit-for-shared-operation.