Safety Findings Report
Emergency Stop & Safe Stop Evaluation (ESTOP-SAFE v1.0)

Independent Safety Assessment

1 Assessment Summary

This report presents the results of an independent safety evaluation of emergency stop and safe stop behavior using the **ESTOP-SAFE v1.0** Safety Evaluation Kit.

The assessment evaluates whether the robot reliably enters and maintains a safe state when an emergency stop is activated or released, in accordance with the defined safety intent and hazard scope of the kit. Risk estimation and evaluation are performed qualitatively in accordance with ISO 12100:2010(E), Clause 5.5.

- **Robot Platform:** [Robot name / model]
- **Assessment Scope:** Emergency Stop & Safe Stop behavior
- **Evidence Package ID:** [RUN-ID]

Overall Risk Evaluation: **Risk Not Acceptable**

Based on the collected evidence and qualitative risk evaluation in accordance with ISO 12100:2010, one or more identified hazards were evaluated as having risks that are **not acceptable** under the assessed conditions. Risk reduction measures are required prior to deployment.

2 What This Assessment Is Not

This assessment is conducted solely for the purpose of identifying and documenting potential safety hazards and associated risks related to the evaluated system, based on the information made available at the time of assessment and within the defined scope, assumptions, and operating conditions. The following clauses explicitly define the limitations of this assessment.

Exclusions and Limitations

C1. No Certification or Regulatory Approval
This assessment does not constitute certification, regulatory approval, compliance sign-off, or formal conformity assessment under any national, international, or industry-specific standard, directive, regulation, or law.

C2. No Guarantee of Overall System Safety
This assessment does not guarantee the overall safety, reliability, performance, robustness, or fitness for use of the evaluated system, whether in isolation or as part of a larger system.

C3. No Replacement for Statutory or Third-Party Evaluation
This assessment does not replace, supersede, or invalidate evaluations, inspections, approvals, or certifications performed by notified bodies, statutory authorities, regulators, or other authorized third parties.

C4. No Exhaustive Verification or Validation
This assessment is not limited to a checklist-based or documentation-only review; however, it does not constitute exhaustive testing, full system verification, validation, fault injection testing, or lifetime operational analysis.

C5. Limited Scope of Responsibility
The assessment is limited to safety risk identification and qualitative or semi-quantitative risk analysis within the agreed scope. The occurrence of any hazardous event, incident, injury, damage, or loss arising from the use, misuse, modification, integration, or deployment of the system remains the responsibility of the system owner, manufacturer, integrator, or operator.

C6. No Assumption of Liability
This assessment does not constitute a warranty, guarantee, or assumption of liability, whether express or implied, by the assessing organization for any outcomes resulting from system operation or decision-making based on this assessment.

This section shall be interpreted in conjunction with the defined scope, assumptions, and limitations stated elsewhere in this report. Any use of this assessment beyond its stated purpose or scope is undertaken at the sole discretion and responsibility of the owner.

3 Safety Intent Evaluation

The following safety invariants were evaluated:

1. Emergency stop reliably halts all robot motion within bounded time and distance.
2. Emergency stop overrides all motion-producing control sources.
3. Robot does not resume motion after emergency stop release without explicit re-arming.

Evaluation Summary: One or more safety invariants were not consistently satisfied under foreseeable operating conditions, contributing to an increased probability of occurrence of harm.

4 Scenario Results Summary

Scenario outcomes are reported as evidence-oriented observations (not as pass/fail judgments). Each scenario contributes evidence for the risk evaluation of associated hazards.

Scenario ID	Description	Observation
ES-1	Emergency stop during nominal motion	Observed behavior consistent with expected safe behavior
ES-2	Emergency stop under high compute load	Observed behavior consistent with expected safe behavior
ES-3	Emergency stop release near human/obstacle	Observed behavior deviated from expected safe behavior

ES-4	Repeated emergency stop cycling	Observed behavior consistent with expected safe behavior
ES-5	Emergency stop visibility and accessibility	Observed behavior consistent with expected safe behavior
ES-6	Emergency stop override of active commands	Observed behavior deviated from expected safe behavior
ES-7	Actuator power / torque removal confirmation	Insufficient evidence to determine behavior

5 Key Safety Findings

Findings are stated in terms of observed behavior, potential contribution to severity and probability of harm, and risk acceptability in accordance with ISO 12100:2010(E), Clause 5.5.3.

Finding F-01: Unintended motion after emergency stop release

Severity (worst credible): High / Devastating
Probability (qualitative): Likely
Risk Evaluation: Not Acceptable

Observed behavior: Following emergency stop release, the robot resumed motion without an explicit operator re-arming action when autonomy commands were still active.

Associated scenario(s): ES-3

Why this matters: Operators may reasonably assume the robot remains safe after releasing the emergency stop. Automatic motion resumption increases the probability of occurrence of harm, including collision or injury, particularly in the presence of humans.

Required risk reduction: Implement a latched safe state requiring deliberate and explicit re-arming before motion can resume. Demonstrate the behavior under foreseeable operating conditions and re-run the associated scenario(s).

Finding F-02: Emergency stop does not override all active control commands

Severity (worst credible): High / Devastating
Probability (qualitative): Possible to Likely
Risk Evaluation: Not Acceptable

Observed behavior: During emergency stop activation, teleoperation commands continued to be processed by the motion controller, resulting in delayed stop behavior.

Associated scenario(s): ES-6

Why this matters: Emergency stop must dominate all control sources. Partial override introduces ambiguity in control authority and can increase both the occurrence of a hazardous event and the probability of harm under foreseeable conditions.

Required risk reduction: Ensure emergency stop input has highest priority and suppresses all motion-producing commands at the safety controller level. Provide evidence that command processing and actuation are inhibited while emergency stop is active.

Finding F-03: Actuator power removal not verifiable

Severity (worst credible): Medium to High
Probability (qualitative): Uncertain (insufficient evidence)
Risk Evaluation: Requires further analysis / evidence

Observed behavior: Submitted evidence did not conclusively demonstrate removal of actuator power or transition to a verified safe torque-off state.

Associated scenario(s): ES-7

Why this matters: A stopped robot that remains energized may still pose a motion hazard, and insufficient evidence prevents reliable estimation of probability of harm.

Required action: Provide clear actuator power or torque-state indicators in logs or status interfaces and re-run ES-7 to support risk evaluation.

6 Evidence Quality Assessment

- Logs: **Sufficient**
- Video evidence: **Sufficient**
- Timing data: **Partial**
- Actuator power / torque state evidence: **Insufficient**

Where evidence is insufficient, risk evaluation cannot be completed and additional evidence is required in accordance with ISO 12100:2010(E), Clause 5.5.

7 Deployment Recommendation

Based on the identified findings and the overall risk evaluation outcome of **Risk Not Acceptable**, deployment of the evaluated system in environments involving human presence is **not recommended** at this time.

Risks evaluated as **not acceptable** require risk reduction measures in accordance with ISO 12100:2010(E), Clause 6, followed by re-evaluation with sufficient supporting evidence.

8 Re-evaluation Requirements

Re-execution of this kit (or the relevant scenarios) is required after:

- Emergency stop logic, wiring, or device changes
- Controller authority/arbitration changes (autonomy/teleop/manual)
- Safety controller configuration updates
- Changes to speed, payload, or operating conditions that affect stop behavior

9 Limitations and Disclaimer

This assessment is limited to the scope of the ESTOP-SAFE v1.0 kit and the evidence provided under the stated operating assumptions. It does not constitute certification, regulatory approval, or a guarantee of overall system safety.