Safety Evaluation Kit: Emergency Stop & Safe Stop (ESTOP-SAFE-v1.0)

1 Kit Overview

1.1 Purpose

This kit evaluates whether the robot reliably enters and maintains a safe state when an emergency stop is triggered, and whether unintended motion is prevented during and after emergency stop release. The kit is designed to expose unsafe stop behavior, delayed stopping, and unintended restart under realistic operating conditions.

1.2 Applicable Robot Types

- Mobile Robots
- Arms and Manipulators
- Mobile manipulators

1.3 Scope

- Emergency stop response and latency
- Stopping distance under motion
- Stop priority under compute or command load
- Behavior during emergency stop release

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

The following safety invariants must always hold:

1. **Immediate Stop:** When an emergency stop is activated, all robot motion shall cease within a bounded time and distance.
2. **Override Priority:** Emergency stop shall override all motion commands, autonomy logic, and teleoperation inputs.
3. **No Automatic Resume:** After emergency stop release, the robot shall not resume motion without an explicit, deliberate re-arming action.

Violation of any invariant constitutes a **FAIL**.

4 Hazard Scope

This kit addresses the following hazards with reference to ISO 3691-4:2023, Clause 4.8.1:

- **H-01: Inadequate stopping behavior following emergency stop activation.**
  Robot motion does not cease within a bounded and repeatable time and distance after the emergency stop is actuated.
- **H-02: Emergency stop does not override all motion producing control sources.**
  Emergency stop fails to reliably override autonomous control, teleoperation commands, or maintenance mode inputs.

- **H-03: Actuator power is not fully removed upon emergency stop activation.** One or more motion-producing actuators remain energized or capable of generating motion after emergency stop activation.
- **H-04: Unintended restart or resumption of motion after emergency stop release.** Robot resumes motion automatically or without explicit re-arming following emergency stop release or fault recovery.
- **H-05: Emergency stop device is not clearly visible or accessible to the operator.** Emergency stop cannot be readily located or actuated by an operator during foreseeable operation or emergency conditions.

5 Roles and Responsibilities

The roles and responsibilities defined in this section apply uniformly to all assessments conducted under this report, unless explicitly stated otherwise.

Client Team

The Client Team is responsible for the preparation, collection, and submission of all required evidence related to the defined test cases, including but not limited to documentation, logs, test results, videos, and system descriptions. The Client Team shall ensure that all submitted information is accurate, complete, and representative of the evaluated system configuration.

Assessor

The Assessor is responsible for reviewing and evaluating the evidence submitted by the Client Team against the defined assessment criteria and scope. The Assessor identifies safety findings, observations, and recommendations based solely on the submitted evidence and stated assumptions. The Assessor does not perform independent system operation, testing, or modification unless explicitly agreed in writing.

6 Prerequisites and Setup

6.1 Required Tools

- Robot logging system (controller state, velocity, timestamps)
- Video recording device (phone acceptable)
- Ability to trigger emergency stop
- Method to apply computational or command load (if applicable)

6.2 Test Conditions

- Robot operating in normal autonomy or commanded motion
- Clear test area with exclusion zone
- Payload and speed representative of real deployment

7 Failure Scenarios

Scenario ES-1: Emergency Stop During Nominal Motion

Failure injection: Trigger emergency stop while the robot is moving at nominal operating speed.

Expected safe behavior: Robot stops within bounded time and distance and enters a latched safe state.

Evidence to record:

- Stop time (ms)
- Stopping distance (cm)
- Video of stop event
- Controller state log

Scenario ES-2: Emergency Stop Under High Compute Load

Failure injection: Trigger emergency stop while the robot is under high CPU load or command traffic.

Expected safe behavior: Emergency stop overrides all computation and stops motion without delay.

Evidence to record:

- Stop time
- CPU or system load indicator
- Video evidence

Scenario ES-3: Emergency Stop Release Near Human or Obstacle

Failure injection: Release emergency stop while a human surrogate or obstacle is within the safety zone.

Expected safe behavior: Robot remains stationary and requires explicit re-arming.

Evidence to record:

- Motion after E-stop release (yes/no)
- Controller mode/state
- Video evidence

Scenario ES-4: Repeated Emergency Stop Cycling

Failure injection: Perform multiple emergency stop / release cycles.

Expected safe behavior: Consistent stopping behavior with no degradation or unsafe state transition.

Evidence to record:

- Stop time across cycles
- Any anomalies or delayed response

Scenario ES-5: Emergency Stop Visibility and Accessibility

Failure injection: None (inspection and reachability verification).

Expected safe behavior: Emergency stop device is clearly visible and can be actuated immediately by an operator from foreseeable approach directions without repositioning the robot.

Evidence to record:

- Photographs showing emergency stop visibility from front, side, and rear
- Short video demonstrating operator reach and actuation from each direction
- Approximate time-to-actuation (s) from initial approach

Scenario ES-6: Emergency Stop Override of Active Control Commands

Failure injection: While autonomous navigation, teleoperation, or manual motion commands are actively being issued, trigger the emergency stop.

Expected safe behavior: Emergency stop overrides all motion-producing commands, and no actuator motion occurs while the emergency stop remains active.

Evidence to record:

- Controller command logs showing active motion commands
- Safety or drive-enable state indicating emergency stop activation
- Video showing absence of motion after emergency stop

Scenario ES-7: Actuator Power or Torque Removal Confirmation

Failure injection: Trigger emergency stop during motion and attempt to induce motion or command actuation while the emergency stop is active.

Expected safe behavior: All motion-producing actuators are de-energized or placed in a verified safe torque-off state, preventing any commanded or induced motion.

Evidence to record:

- Safety controller or drive-enable status logs
- Actuator power or torque state indicators (as applicable)
- Video demonstrating inability to produce motion while emergency stop is active

8 Evidence Submission Requirements

To support risk estimation and evaluation in accordance with ISO 12100:2010(E), the client shall submit a single, consolidated evidence package for each assessment run.

The evidence package shall include, at a minimum:

- All system logs referenced by the evaluated scenarios, including controller state, timestamps, and relevant safety or motion signals.
- All video recordings corresponding to the evaluated scenarios, clearly labeled by scenario identifier and synchronized, where feasible, with system logs.
- Brief run documentation describing the assessment context, including:
  - date of execution;

– robot hardware and software configuration;
– payload, speed limits, and operating mode.

Submitted evidence shall be sufficient to allow reliable interpretation of observed system behavior and its relevance to hazard exposure, occurrence of hazardous events, and the possibility of avoiding or limiting harm.

Where evidence is incomplete, unclear, or missing, risk estimation may be inconclusive and additional evidence or re-execution of scenarios may be required.

Incomplete evidence may result in an **INCONCLUSIVE** judgment.

9 Risk Estimation and Evaluation

Risk estimation and evaluation are performed in accordance with ISO 12100:2010, Clause 5.5. The objective is to determine whether the risks associated with identified hazards are acceptable or require risk reduction, taking into account the intended use and foreseeable misuse of the system.

Risk estimation and evaluation are qualitative and based on structured engineering judgment.

9.1 Severity of Harm

The severity of harm is estimated by taking into account the following (ISO 12100:2010, Clause 5.5.2.2):

a) the severity of injuries or damage to health, for example:
   - no harm;
   - slight;
   - medium;
   - high;
   - devastating.

b) the extent of harm, for example, to:
   - one person;
   - several persons.

For the purpose of risk estimation, the worst credible consequence is considered.

Severity Classes Severity is classified using the following qualitative categories:

- **No Harm:** No injury or damage to health is reasonably foreseeable.
- **Slight:** Minor, reversible injury not requiring medical treatment.
- **Medium:** Injury requiring medical treatment or resulting in temporary impairment.
- **High:** Serious injury resulting in permanent impairment or life-threatening harm.
- **Devastating:** Fatal injury or multiple serious injuries.

9.2 Probability of Occurrence of Harm

The probability of occurrence of harm is estimated by considering the combined influence of the following aspects, in accordance with ISO 12100:2010, Clause 5.5.2.3.

Exposure of persons to the hazard

The exposure of persons to the hazard is estimated by taking into account, among others:

a) the need for access to the hazard zone (for example, during normal operation, correction of malfunction, maintenance, or repair);

b) the nature of access (for example, manual interaction);

c) the time spent in the hazard zone;

d) the number of persons requiring access; and

e) the frequency of access.

Occurrence of a hazardous event

The occurrence of a hazardous event is estimated by taking into account, among others:

a) reliability and other relevant technical or statistical data;

b) accident or incident history, where available;

c) history of damage to health; and

d) comparison with similar machinery or applications.

The occurrence of a hazardous event may be of technical or human origin.

Possibility of avoiding or limiting harm

The possibility of avoiding or limiting harm is estimated by taking into account, among others:

a) the different persons who can be exposed to the hazard(s), for example:

- skilled;
- unskilled;

b) how quickly the hazardous situation could lead to harm, for example:

- suddenly;
- quickly;
- slowly;

c) any awareness of risk, for example:

- by general information, in particular information for use;
- by direct observation;
- through warning signs and indicating devices on the machinery;

d) the human ability to avoid or limit harm (for example, reflex, agility, or possibility of escape);

e) practical experience and knowledge, for example:

- of the machinery;
- of similar machinery;
- no prior experience.

Probability Classes The probability of occurrence of harm is classified qualitatively using the following descriptive categories:

- **Very Unlikely:** Exposure to the hazard is exceptional or rare, the occurrence of a hazardous event is improbable, and there is a high possibility of avoiding or limiting harm.
- **Unlikely:** Exposure to the hazard is infrequent, hazardous events are possible but not expected under normal conditions, and avoidance or limitation of harm is generally feasible.
- **Possible:** Exposure occurs occasionally, a hazardous event is reasonably foreseeable under certain conditions, and the possibility of avoiding or limiting harm may be limited.
- **Likely:** Exposure to the hazard is frequent, hazardous events are expected to occur under foreseeable conditions, and the possibility of avoiding or limiting harm is low.
- **Frequent:** Exposure to the hazard is continuous or near continuous, hazardous events occur repeatedly or persistently, and there is little or no possibility of avoiding or limiting harm.

9.3 Risk Evaluation

Based on the qualitative estimation of the severity of harm and the probability of occurrence of harm, each identified risk is evaluated as either **acceptable** or **not acceptable** (ISO 12100:2010, Clause 5.5.3).

Where risk is evaluated as not acceptable, risk reduction measures shall be identified and applied in accordance with the hierarchy defined in ISO 12100:2010, Clause 6.

9.4 Insufficient Information

If available evidence is insufficient to reliably estimate the severity or probability of harm, the risk evaluation cannot be completed and shall be treated as requiring further analysis or additional evidence.

10 Output Artifacts

The assessor will return the following artifacts upon completion of the assessment:

- **Safety Findings Report (PDF)** documenting identified hazards, supporting evidence, and risk evaluation results.
- **Scenario-Level Observations** describing observed system behavior relative to expected safe behavior for each evaluated scenario.
- **Risk Evaluation Summary** indicating, for each identified hazard, whether the associated risk is considered acceptable or not acceptable under the evaluated conditions, in accordance with ISO 12100:2010.
- **Identified Safety Concerns and Required Risk Reduction Measures** for hazards where risk is evaluated as not acceptable.
- **Re-evaluation Guidance** describing conditions under which the assessment should be repeated following design changes, mitigations, or additional evidence.

11 Re-run Conditions

This kit must be re-run if any of the following change:

- Motion controller or safety controller changes
- Emergency stop hardware or wiring changes
- Speed, payload, or operating environment changes