Safety Evaluation Kit: Load Handling and Transfer (LOAD-HANDLE-v1.0)

1 Kit Overview

1.1 Purpose

This kit evaluates whether a robotic system maintains safe and stable behavior while loading, transporting, and unloading objects under normal operation and foreseeable disturbances. The objective is to identify load instability, unintended object release, unsafe motion induced by load dynamics, and unsafe interaction with humans or obstacles during load handling tasks.

1.2 Terminology

For the purposes of this document:

- **Loading:** Picking (manipulators) or acquiring a payload (mobile robots).
- **Unloading:** Placing (manipulators) or releasing a payload (mobile robots).
- **Object:** The item being handled, including parcels, packages, tools, or parts.

1.3 Applicable Robot Types

- Mobile robots
- Arms and manipulators
- Mobile manipulators

1.4 Scope

- Object stability during loading and unloading
- Object stability during nominal motion (translation and turning)
- Object stability during emergency stop or fault-induced stopping

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. **Object Retention:** During loading, transport, stopping, and unloading, the object shall not be unintentionally released or dropped.
2. **Load Stability:** Under nominal motion and foreseeable fault or stop conditions, the object shall remain mechanically stable relative to the robot.
3. **Safe Interaction During Load Handling:** While handling a load, the robot shall detect humans or obstacles in its workspace and transition to a safe state without causing object drop or collision.

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

4 Hazard Scope

This kit addresses the following hazards with reference to ISO 3691-4:2023, Clause 4.5:

- **H-01: Loss of object retention during operation**
  Loss of object retention during loading, transport, emergency stopping, or fault conditions, resulting in dropped loads that may injure nearby humans or damage property.
- **H-02: Failure to detect humans or obstacles during load handling**
  Inadequate detection of humans or obstacles while carrying a load, leading to collision between the robot, the load, and surrounding entities.
- **H-03: Unstable or jerky motion induced by faults**
  Control, sensing, or actuator faults producing unstable or jerky motion, resulting in load instability or unintended object release.
- **H-04: Unsafe handling of sharp, small, or fragile objects**
  Excessive speed or abrupt motion during handling of sharp, small, or fragile objects, resulting in object damage or secondary hazards.

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)
- Representative test objects or parcels of varying size and mass
- Ability to perform loading and unloading operations

6.2 Test Conditions

- Robot operating in nominal autonomy or commanded motion
- Clear test area with an exclusion zone
- Payload mass and speed representative of intended deployment

7 Failure Scenarios

Scenario LH-1: Load Stability During Nominal Motion

Failure injection: Introduce controlled disturbances (e.g., abrupt velocity changes or minor external perturbations) during nominal loading, transport, or unloading motion.

Expected safe behavior: The controller stabilizes the robot and the object remains retained and mechanically stable.

Evidence to record:

- Commanded and measured velocity logs
- IMU and actuator data
- Object retained (yes/no)
- Controller mode/state
- Video evidence

Scenario LH-2: Emergency Stop While Carrying a Load

Failure injection: Trigger emergency stop while the robot is moving with a loaded object.

Expected safe behavior: Robot stops within bounded behavior and the object remains retained.

Evidence to record:

- Object retained (yes/no)
- Controller mode/state
- Velocity logs
- Video evidence

Scenario LH-3: Fault Induction During Load Handling

Failure injection: Introduce representative faults (e.g., sensor degradation, control faults) during load transport.

Expected safe behavior: Robot either maintains stable motion or transitions to a safe stop without object drop.

Evidence to record: For at least five distinct fault cases:

- Fault type
- Controller mode/state
- Object retained (yes/no)
- Velocity logs
- Video evidence

Scenario LH-4: Handling of Sharp, Small, or Fragile Objects

Failure injection: Command handling of sharp, small, or fragile objects at representative operating speeds.

Expected safe behavior: Robot operates at appropriately reduced speed and maintains object stability without drop.

Evidence to record: For each object type:

- Object type
- Controller mode/state
- Object retained (yes/no)
- Velocity logs
- Video evidence

Scenario LH-5: Human or Obstacle Intrusion During Load Handling

Failure injection: Introduce a human surrogate or obstacle into the robot workspace during load handling.

Expected safe behavior: Robot transitions to a safe state and the object remains retained.

Evidence to record:

- Controller mode/state
- Object retained (yes/no)
- Velocity logs
- Video evidence

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
- Load handling or retention mechanism changes
- Speed, payload, or operating environment changes