EVIDE · TECHNICAL SCOPE NOTE

Robotic Safety Decisions and Evidentiary Boundaries

Version 1.0 · 14 November 2026 · Emanuel Celano, EVIDE (External Evidentiary Deposit)

Purpose and scope

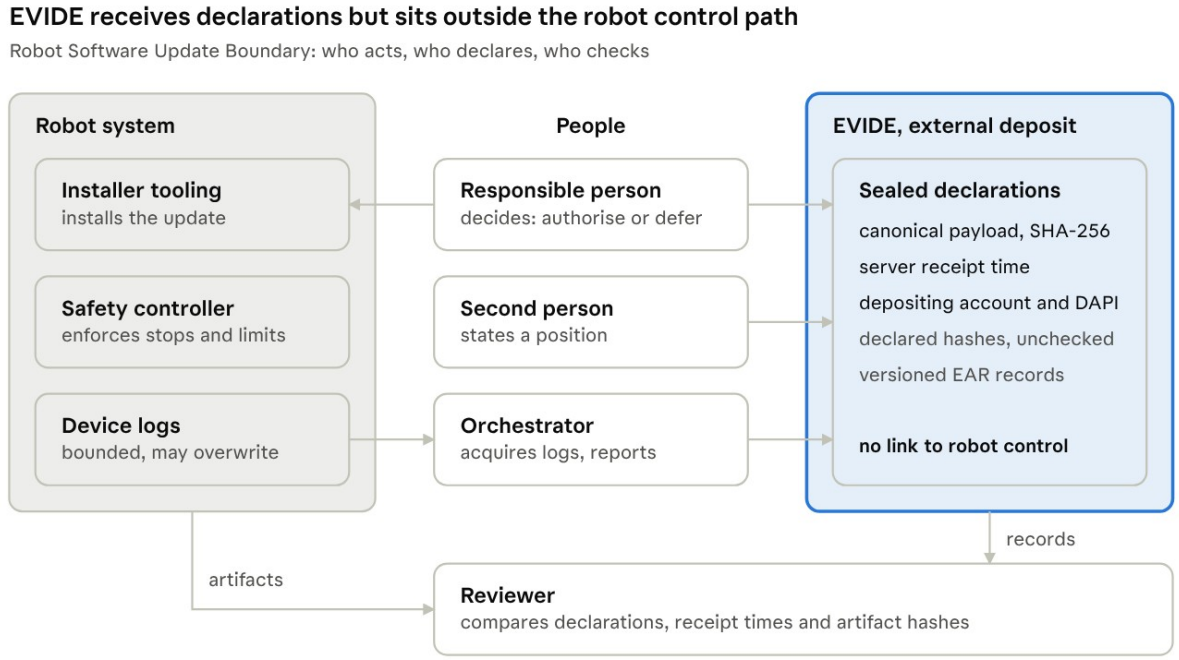
> **Safety systems enforce operational safety constraints. Evidentiary records preserve what was declared, which artifacts were referenced, when those declarations reached EVIDE, and what was not verified.**

This note describes where an external evidentiary deposit (EVIDE) sits around a robotic safety decision, and where it stops. It uses one scenario: a software update to a non-safety-critical application component of a robot.

The note is vendor-neutral. It describes no existing integration with any robot, controller or safety product, and it makes no claim of conformity with any standard.

Standards context, scope only. ISO 10218-1:2025 and ISO 10218-2:2025 cover industrial robots and their integration; their scope excludes mobility when the robot is part of a mobile platform. ISO/CD 25785-1 (dynamically stable industrial mobile robots, including bipedal and quadrupedal forms) is a committee draft whose CD comment period closed on 8 July 2026; a Part 2 on integration is to be developed separately. ISO 31101:2023 sets requirements for safety management systems of services provided by service robots and is not a product safety standard. This note reflects the public scope statements of these documents, not a clause-by-clause reading of their text.

Boundaries at a glance



Only people and the orchestrator write to EVIDE, and nothing flows from EVIDE back to the robot. The responsible person authorises the installation outside EVIDE. The reviewer checks referenced artifacts against their declared hashes, outside EVIDE.

Scenario: Robot Software Update Boundary

A responsible person decides whether to install a new version of an application component (for example a speech-pipeline node). Firmware, safety functions, motion parameters, brakes and stop functions are out of scope. The robot is stationary or in a controlled area during installation.

1. **Before the update.** The responsible person deposits a structured human decision: authorise or defer, installed and planned version, purpose, known risks, declared role, declared uncertainties. The deposit references by declared hash the package, release notes, pre-update version report, backup and test plan with a minimum observation window. A second person, holding a DAPI-identified account, may deposit a linked response to a frozen summary of the record (FAST REVIEW): a position on the decision, not an approval. In the current production version, the fixed text of the FAST REVIEW representation is available only in Italian (`fr-it-1.0`). The surrounding interface and notices support five languages, but they do not translate the frozen representation or the source content.
2. **During the update.** The robot's own tooling installs the software. Safety controllers and device logs record their own events. EVIDE is not in this path: it does not authorise, trigger, delay or block the installation, and no deposit is a precondition for it.
3. **After the update.** An orchestrator deposits, through the machine channel (REST API or a local MCP client), the declared outcome and declared installation time, chained to the decision record. The chain is accepted only if the API key belongs to the same evidentiary domain as the decision record (the same personal account, or the same organization) and the decision record has been received or certified. It references by declared hash the installation log extract, the post-update version report and a statement on the robot's clock. An observation window then records declared observations and test results, and closes with a declared verdict. The minimum duration comes from the declared test plan; EVIDE does not enforce it. The verdict is not a safety judgement.
4. **Review or incident.** A reviewer receives the EVIDE outputs and, separately, the referenced artifacts from whoever holds them. EVIDE does not retrieve or assemble those artifacts. The reviewer can separate what was declared, which artifacts were referenced and with which declared hash, when each declaration reached EVIDE, and which artifacts actually match their declared hash.

If the update is deferred, the decision and its reasons are deposited and no record represents an installation. A later review is a new decision, chained to the first.

Three times that are not the same

The time of an event, the time its artifact was acquired and the time a declaration reached EVIDE may originate from distinct clock sources and must not be treated as one.

Time	Clock	What it shows	What it does not show
Event time	robot, controller or device	when the source system says the event happened	that the source clock was correct
Acquisition time	the tool or person that retrieved the log	when an export was taken, as declared by whoever took it	that the export is complete
Deposit time	EVIDE server	when the declaration was received, from the EVIDE server clock, to the second. EVIDE also generates server-side UTC timestamps for observation-window opening and closing and EAR generation; these are distinct recorded events	that the declaration is true; it is not a qualified timestamp

Example: a bounded on-device log. Many safety devices keep a limited event log on the device and overwrite the oldest events when it is full. A management database then holds only the events already

retrieved. At any moment there are three sets: events still on the device, events already retrieved, and events overwritten before anyone retrieved them.

A deposit can state which export was acquired, when, from which source, with which declared hash, and a declared retention status of the source (`persistent_storage`, `rolling_buffer` or `unknown`). It cannot show that no events were overwritten before acquisition, or that the export is the whole log.

Clocks. Before and after the update the orchestrator deposits the robot's local time as read at sending. The difference from the deposit time gives only an order of magnitude of clock agreement at those two moments, including network delay. Below one second it is not meaningful. If it exceeds a tolerance set in advance, the order between installation time and deposit times is not asserted.

Records and their evidentiary limits

Except for files given to it directly, EVIDE seals the declaration, not the artifact. Every structured record, human or machine, is stored as its accepted payload with a SHA-256 hash of its canonical form and the server's receipt time, so anyone holding the JSON can recompute the hash. A SHA-256 comparison establishes consistency with a reference digest, such as the one on the record's EAR; detecting a later alteration depends on that reference digest being preserved reliably. It does not establish whether the declaration is true.

Record	Channel	What EVIDE establishes	What remains declared
Human decision (authorise or defer)	web or mobile structured intake	content, receipt time, the depositing account and its DAPI (taken from the account, not declared)	the decision's merits, the stated role and authority, the declared decision time
Linked response	shared from the decision record	that a DAPI-identified account holder deposited a response to a frozen FAST REVIEW representation, whose SHA-256 is recorded, and when (representation currently in Italian only)	that they read or understood it; a response is not an approval
Update outcome	REST API or local MCP client	content, receipt time, authenticated API-key/account association, and confirmation that the declared DAPI number matches the DAPI recorded for the account holding that key; the parent record's identifier in the hashed payload	installation, versions, installation time, test results
Clock check (before and after)	REST API or local MCP client	content and receipt time	the robot's local time
Observation window	REST API or local MCP client	server-side UTC opening and closing times; the first EAR version stays unchanged and a second version is issued at close	the observations, the verdict and any stabilization score; the verdict is not a safety judgement
Evidence reference (inside a record)	structured human intake and machine channel (REST API, MCP)	form only: allowed fields, types, values, a complete hash group; on the human channel the declared value must also have the form of a SHA-256 digest	that the artifact exists, matches the declared hash, was hashed by whom it says, is kept as stated
File given directly to EVIDE	web or mobile only	the file's hash, computed by EVIDE on the file received	the file's meaning and origin; for a URL only the address string is hashed, not the page

Chains. A machine-channel record can name a parent record; the parent's identifier enters its hashed payload, but the parent's content does not. A link from a human record to an earlier record is held in the database only. Chains do not appear on the EAR (the receipt document of each record), so a relation that must be visible there is also declared as an evidence reference.

What EVIDE does not do

- It does not stop, slow, command or authorise a robot. It is not in the control path or the safety path.
- It does not measure or certify safety, and it does not establish conformity with ISO 10218, ISO 25785, ISO 31101 or any regulation.
- It does not replace or retrieve device, controller or safety logs, and it cannot tell whether events were overwritten before an export.
- It does not open referenced artifacts or verify declared hashes, versions, test results or clocks.
- It does not verify that declarations are true or that a declared authority is legitimate. On the machine channel it checks that the declared DAPI number matches the DAPI recorded for the account that owns the key; on the human channel the DAPI is taken from the authenticated account, not declared.
- It does not turn a linked response into an approval, or a closed observation window into a safety verdict.
- Its receipt time is the server's clock, not a qualified timestamp.

Status and references

Version 1.0. Technical statements were checked on 14 November 2026 against a copy of the EVIDE production code taken on 13 November 2026. The scenario comes from an EVIDE Governance Lab protocol (v1.0, November 2026). Its Phase 0 tested platform behaviour (chaining, domain rules, receipts) on an isolated copy with synthetic accounts, and a dry run of the full scenario, including declared references in a human record and a linked response, was executed on the same copy. Linked responses have been available in production since 2 November 2026. No test has been run on a physical robot; the protocol is neither a safety test nor a standards validation.

- ISO 10218-1:2025, Robotics: safety requirements, Part 1: Industrial robots
- ISO 10218-2:2025, Robotics: safety requirements, Part 2: Industrial robot applications and robot cells
- ISO/CD 25785-1, Safety requirements for dynamically stable industrial mobile robots, Part 1: Robots
- ISO 31101:2023, Application services provided by service robots: safety management systems requirements

emanuel
celano
14.11.2026
10:57:34
GMT+01:00