Evidence-centric certification traceability schema (pilot)

Evidence layer

Tool run
(Tool ID, version, params)

Operational observation
(telemetry/log summary)

— generated →

— materialised-as →

Evidence artefact
(A_k)
(e.g., signed image, SBOM, scan, config snapshot)

Normative layer

Requirement
(R_i)

— refines / maps-to →

Control / Objective
(C_j)

requires evidence

evidenced-by

Implementation layer

produces / testified-by

— implemented-by →

Component
(device FW, bootloader, OTA, broker, backend)

invalidates / refreshes

belongs-to

input-to

supports

modifies

Evolution layer

Change event
(u0394)

supersedes

Evidence baseline
(B_t)
(versioned snapshot)

triggers re-test
verified-by

recorded-in

Assessment layer

Test / Check
(T_m)

— yields →

Result
(pass/fail, metrics)