WISL™ No.90

ISBN: 978-981-17970-1-9

HSA 8-Bed Ward with IT Implementation — Study Proposal

A7 Bridge Layer · Hospital Ward Deployment

Non-Agentic AI Governance Singapore [UEN 53522354D] Parent Patent SG020603109STW · NAIGE (NAI 4.0) Edition: Draft for site survey and stakeholder review, 2026

---

1. Purpose

This proposal sets out the validation pathway for the **A7 hospital-ward deployment** — an 8-bed ward integrated with enterprise clinical IT. It is the upstream counterpart to the A8 nursing-home study (No.89): same architecture, higher-acuity setting, and a networked IT surface the nursing-home deployment does not have.

It is a **validation study**, not a deployment. No autonomous clinical operation is proposed.

---

2. Relationship to the A8 Study

	A8 — No.89	A7 — this proposal
Setting	Nursing home (Toa Payoh RTS)	Hospital 8-bed ward
Bridge	A8 Bridge Layer	A7 Bridge Hub / Translation Layer
IT surface	Air-gapped from facility IT	Integrated with enterprise clinical IT
Class	B (SaMD), [P+N]	B rising toward C where advisory informs acute management

The two share the deterministic spine — A12 core, N12 drift kernel, WD117 ledger — and the sensing lane. **A7 does not add an actuator.** Any kinetic capability remains the separate [P+N+D] / Class C track.

---

3. Study Stack

Component	Application	Function
A7 Bridge Hub	10202602213U	Sole ingress chokepoint; deterministic translation of advisory data; EMF-drift screening
A11	—	IT connector enclosure; air-gapped IT-to-OT boundary A7 interfaces with
A13b sensing lane	10202602177W	905nm LiDAR, node-local voxelisation, CoM vectors only
WD117 ledger	10202602223T	Write-once forensic record incl. clinician response / non-response

Component	Application	Function
Non-B1 advisory shell	10202602270V	Alerts only; zero actuation

---

4. The Central Question — IT Integration vs Isolation

The A8 study rests on a clean air-gap. **The 8-bed ward cannot.** An enterprise-IT ward is networked by definition — EMR, nurse-call, clinical systems — and that is the whole engineering problem this study exists to answer:

> How does the A7 bridge integrate with enterprise clinical IT **without** the IT-gap drift, ransomware, and silent-failure exposure the isolation doctrine was built to prevent?

The proposed answer, to be validated: A7 is a **one-way deterministic chokepoint**. Advisory data is translated inbound to deterministic features; no reverse command path exists; WD117 writes are one-way; the fail-loud alarm and any safety response run on a path independent of facility IT. Integration at the data layer, isolation at the control layer.

This is the study's load-bearing claim, and the one a reviewer will test first.

---

5. Boundary Conditions

1. A7 accepts advisory data inbound; no outbound command path to any node.
2. WD117 is write-once, one-way-in; A11/enterprise IT may read for export, never write.
3. Non-B1 holds no actuation rights.
4. Safety alerting runs on a path that survives facility-IT compromise (fail-loud, non-network-dependent).
5. EMF / RF ingress screened at A7; no attack surface added by the IT integration.

---

6. Stage 1 — Site Survey (Non-Interventional)

No participants, no patient data, no ethics approval required.

- Ward topology and coverage geometry (8 beds)
- Enterprise-IT interface mapping: what connects where, and by what protocol
- Verification of the one-way boundary against §5
- Independent safety-alert path routing
- Workflow observation at the nurse station
- Closes at a **GO / CONDITIONAL-GO / NO-GO** gate with signed record

---

7. Stage 2 — Clinical Validation (Subject to Approval)

Separate protocol, named clinician investigator, and ethics approval before commencement. **Sponsor:** Non-Agentic AI Governance Singapore (legal manufacturer). **PI:** qualified clinician at the participating hospital.

Single ward. A7 claims an 8-bed embodiment, so the study runs at 8-bed scale — claimed and validated embodiment match.

---

8. Endpoints (CEP issued before data collection)

- Detection sensitivity; false alarms per bed-night
- Time-to-alert; time-to-clinician-acknowledgement; unacknowledged-alert rate
- Node-loss detection-to-annunciation time
- **IT-boundary integrity:** verified absence of a reverse command path under network-traffic inspection

---

9. Standards Position

ISO 14971 (risk), IEC 62304 (software lifecycle), IEC 62366-1 (usability), IEC 60601-1-2 (EMC), **IEC 81001-5-1 (health-software security lifecycle — central here, given the IT integration)**. Conformity with recognised standards is the HSA compliance route; EU AI Act Article 14 human-oversight adopted as the ethical reference above the floor.

---

10. Limitations

All figures are design-intent specifications pending HSA validation. No hardware prototype has been submitted for regulatory assessment as at publication. Ward topology is indicative until the site survey is complete.

WISL™ No.90 — Annex

NAIGE NAI 4.0 — Kinetic Arm (Class C/D) Documentation Plan

M(A12/A13) Manipulator · [P+N+D] Acute Kinetic Tier

Non-Agentic AI Governance Singapore [UEN 53522354D] Parent Patent SG020603109STW · NAIGE (NAI 4.0)

> This annex governs the **actuating** track only. The non-kinetic sensing and ward studies (No.89 A8, No.90 A7) sit under Class B [P+N]. Everything here adds the **D-Layer** and moves a machine near a patient — a different class, a different evidence burden, and a different assessor.

---

1. Capability Baseline (TRL)

An honest maturity statement anchors the whole plan; documentation cannot raise it.

TRL	Definition	Kinetic Arm status
1–2	Principles / concept	Complete
3	Analytical / experimental proof of concept	**Current — not yet evidenced**
4	Component validation in laboratory	Target of the RTS bench + NTU MAE instrumentation
5	Validation in relevant environment	Requires a built manipulator on a real arm
6	System demonstration in relevant environment	Post-build
7–9	Operational → qualified	Post-registration

Consequence: the kinetic corpus is rich at TRL 2 and unevidenced at TRL 3. Only measurement on real hardware advances it.

---

2. Framework Selection (Class C/D)

The kinetic tier is where medical *and* machinery-safety regimes both apply. Cite the right one to the right reader.

Concern	Governing framework	Metric
Deterministic core / FPGA (A12, N12, Sacred Pause)	DO-254 or IEC 61508-2	DAL A–E / SIL
U7 Sovereign Brake, Tripartite PLC gate	ISO 13849-1 + IEC 60204	Performance Level e; Category 3/4; stop category
Manipulator motion safety	ISO 10218 (industrial robots) / **IEC 80601-2-77** (medical robotic surgery)	Task-based risk controls

Concern	Governing framework	Metric
Collaborative operation near persons	ISO/TS 15066	Power-and-force limits, separation monitoring
Embedded software	IEC 62304	Software safety class A/B/C
Device electrical safety + PEMS	**IEC 60601-1 (clause 14)**	Regulator-facing baseline

Cite ISO 13849 / 10218 to an OEM; cite IEC 60601-1 / 80601-2-77 / 62304 to HSA. Both hold for the same arm.

---

3. Artifact Set — Two Tiers

Roughly half is writable now; half is blocked on a built manipulator.

Tier A — writable now (no hardware): PHAC / assurance-level declaration; Hardware & Safety Requirements Specifications (incl. **stop category per embodiment**); Safety Concept (PL/SIL per function); Hazard Analysis (ISO 14971 + task-based per ISO 10218/80601-2-77); V&V Plan with instruments and pass criteria; Configuration Management Plan; Tool Qualification record; Interface Control Documents (A7 ↔ A11, A12 ↔ actuator, WD117 write path, pedal/token I/O).

Tier B — requires implementation: Conceptual & detailed design data (HDL, schematics, STEP kinematic envelope); implementation records (bitstream, netlist, BOM); verification reports (brake-latency traces, envelope-breach tests, force-limit measurement); reliability data (MTTFd, DCavg, CCF); Hardware Accomplishment Summary; closed traceability matrix.

Sequencing rule: finish Tier A before OEM or NTU MAE engagement. Tier A is what a builder needs to quote and schedule; Tier B is what they help produce.

---

4. Per-Module Matrix (Kinetic)

Module	Safety function	Framework	Capability statement
A12 [P+N+D] core	Mediate all downstream action	DO-254	DAL + timing-determinism evidence
M(A12/A13) Kinetic Arm	Constrained high-payload motion	ISO 10218 / 80601-2-77	Task risk controls; envelope proof
A13c Clinical Robotic Platform	OEM B2B execution shell	ISO 10218 + IEC 60601-1	Deployed under Class C/D
U7 Sovereign Brake	Sever / hold / controlled stop	ISO 13849-1 + IEC 60204	PL e; **stop category declared per embodiment**
Tripartite .1x Latch	Multi-factor human commit	ISO 13849-1	PL e; token hard-expiry < 5 s; diagnostic coverage
WD117 (A12L) ledger	Immutable event record	61508-2 + 13485 records	Write-once proof; hash-chain integrity
Orange Code p006	Bound compute headroom	61508-2	Enforcement + measurement method

Open item (carried): the U7 stop category is not uniform — arm in free space = Category 0 (immediate de-energisation); load-bearing / occupant-carrying = Category 1 or fail-to-hold. One brake, declared behaviour per embodiment, resolved in the Safety Requirements Spec before any Tier B work.

---

5. Canonicalisation Prerequisite

Resolve to one value each in the Hardware Requirements Spec before Tier A is baselined:

- **U7 severance** — canonical **<1.05 ms**; retire <1.85, <1.00, "1.0 ms".
- **Sacred Pause** — **25–1000 ms window on a 1 kHz master clock**; the ~30 ms schematic figure is one in-range example.
- **Kinematic limits** — 0.05 mm is a *positional tolerance*; jerk is mm/s³, acceleration mm/s². Separate rows, correct units.
- **V&V identifiers** — one VV registry, one test per ID.

---

6. Configuration Management

One scheme across all artifacts: `NAIGE4-[module]-[artifact]-[seq]-[rev]` (e.g. `NAIGE4-U7-SRS-001-A`). Every document carries title, identifier, revision, date, author, approval, change history. Superseded revisions retained, not deleted.

---

7. Known Gaps — State Openly

1. No manipulator built; TRL 3 unevidenced.
2. No independent measurement of brake latency, envelope, or force limits.
3. No named safety assessor or notified/certification body engaged.
4. Reliability data pending component selection.
5. Toolchain not qualified.
6. Collaborative force-limit strategy (ISO/TS 15066) not yet specified.

Declaring these reads as configuration control; omitting them reads as oversight.

---

8. Immediate Sequence

1. Canonicalisation record (§5) — blocked on nothing.
2. Safety Requirements Spec incl. stop categories — after 1.
3. Hazard analysis (system + task-based) — after 2.
4. Safety concept, PL/SIL per function — after 3.
5. V&V plan with instruments + pass criteria — after 4.
6. PHAC / assurance-level declaration — after 4.
7. OEM / NTU MAE engagement package (Tier A + BOM + STEP) — after 1–6.

Steps 1–6 need no hardware, no lab, no affiliation — completable independently, and they are exactly what an MAE supervisor or OEM needs before they can commit.
