

Aligning NAI 2.0 as Class B Software (SaMD) and NAI 4.0 as C/D Kinectic Hardware as a Medical Device

NAIGE replaces probabilistic software guardrails with deterministic hardware controls to ensure absolute patient safety and human authority through Hardware-Enforced Kinetic Governance.

N-Layer: The Sacred Pause™
A mandatory hardware-timed delay (25-1000ms) that forces human deliberation before any action.

Uses one-time programmable silicon fuses to create a permanent, tamper-proof record of events.

Physical Power Severance (<1.05ms)

Sovereign Brake™

Strips biometric identity at the silicon level using LIDAR instead of optical cameras.

The Sovereign Brake™
Instantly severs power to actuators if any system anomaly or drift is detected.

Kinetic foot pedal

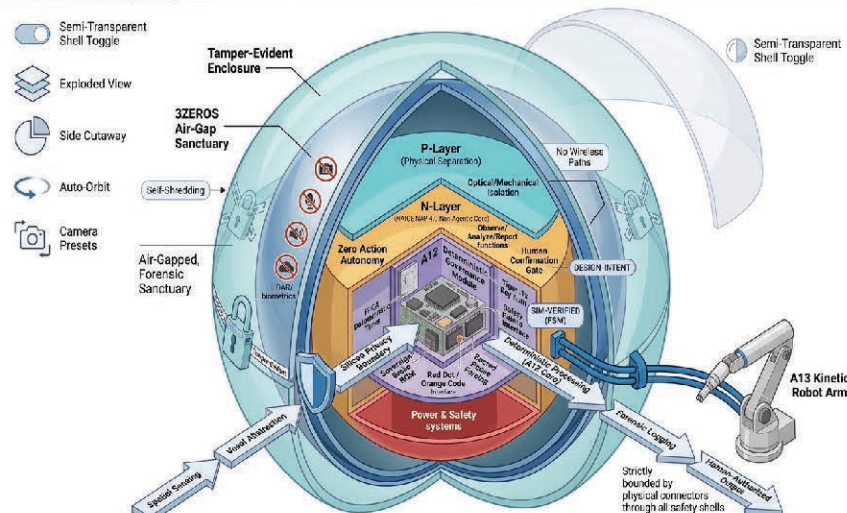
Power Severed
($<1.06\text{ms}$)

Inaction-as-Safe-Default

Machines default to mechanical stillness.
AI has zero direct actuation rights.

Tiger .1x Tripartite Authorization
Requires simultaneous Iris scan, Cryptographic token, and Kinetic foot pedal to move.

The Sovereign Brake™
Instantly severs power to actuator
system anomaly or drift is detected



SG020603109STW · P-LIFE 1.00 · NAI 4.0 · NAI 2.0
NLB Legal Deposit R260219-005 / R260302-007

Immutable— Hardware-Enforced Non-Agentive AI Governance Architecture — NAI 4.0

A12 [P+N+D] Deterministic Black Box · HSA Deterministic Horizon · Capstone A10a Root of Trust

NAI 2.0 · Software Governance · Advisory Stratum · Sandbox Safety · Non-Agentive Policy Control Logic

978-981-17963-4-0

ISBN PAPERBACK • IMMUTABLE HARDWARE-ENFORCED

Immutable Hardware-Enforced Non-Agentive AI Governance Engine [NAIGE] Governance Systems

Hardware-Enforced Safety for Clinical and Humanitarian Robotics

Koh, E. W. K. (2026). *Immutable Hardware-Enforced Non-Agentive AI Governance Engine [NAIGE] Governance Systems — Hardware-Enforced Safety for Clinical and Humanitarian Robotics*. WISL™ National Edition. Non-Agentive AI Governance Singapore [UEN 53522354D].

ISBN Paperback: National Second Edition

Available at: <https://kohedwin.ai> | <https://non-agentive.ai>

Author & Publisher: Edwin Koh Wui Kiat (Tiger)

Parent Patent: SG020603109STW

NLB Legal Deposit: R260219-005 / R260302-007

Limitations. All clinical performance targets and safety metrics stated in this work are design-intent specifications pending HSA Class B/C/D SaMD validation. No hardware prototype has been submitted for regulatory assessment as at the date of publication.

Copyright ©™ Notice

Non-Agentive AI Governance Singapore [UEN 53522354D]

© 2026 Non-Agentive Governance Singapore (ACRA T260229801). All rights reserved.

No part of this publication may be reproduced, distributed, transmitted, or stored in any retrieval system in any form or by any means — electronic, mechanical, photocopying, recording, or otherwise — without the prior written permission of Non-Agentive Governance Singapore, except for brief quotations for academic citation, review, or research purposes with full attribution.

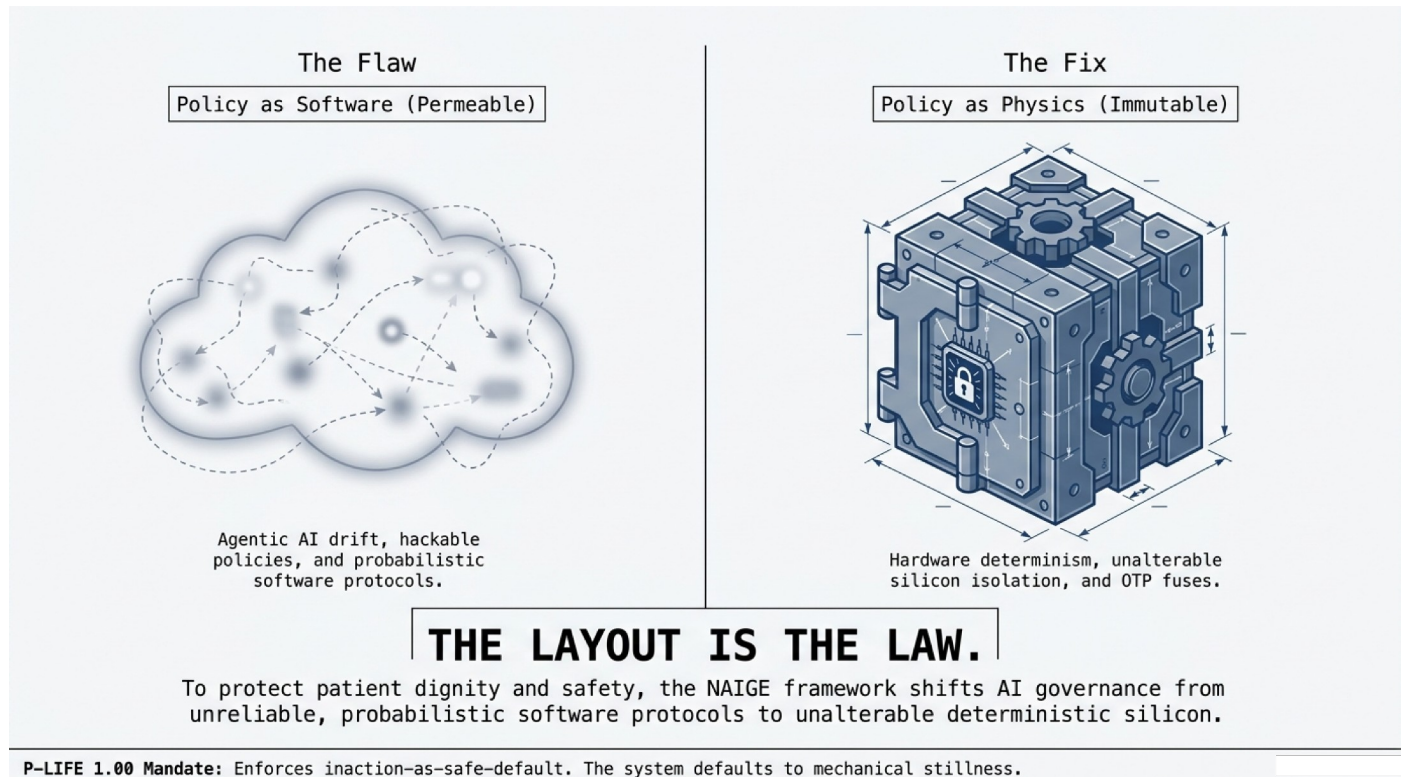
All trademarks, (Classes 9, 42, 10, 44, 45), 3ZEROS™, Sacred Pause™, ABC+2S+H™, ABC+2S Guardian™, ABC+2S+H Framework™, ABC+2S+H Guardian™, Nightingale's Eyes Care™ are proprietary to Non-Agentive Governance Singapore™ and protected under Singapore patent law and trademark registration.

All architectural and terminology including concepts including Tiger .x1key, P-Life 1.00, Sovereign Brake, Kinetic Foot Pedal/Button, Tripartite Latch, Orange Code 110% Cap are proprietary of Non-Agentive AI™ and Non-Agentive Governance Singapore™

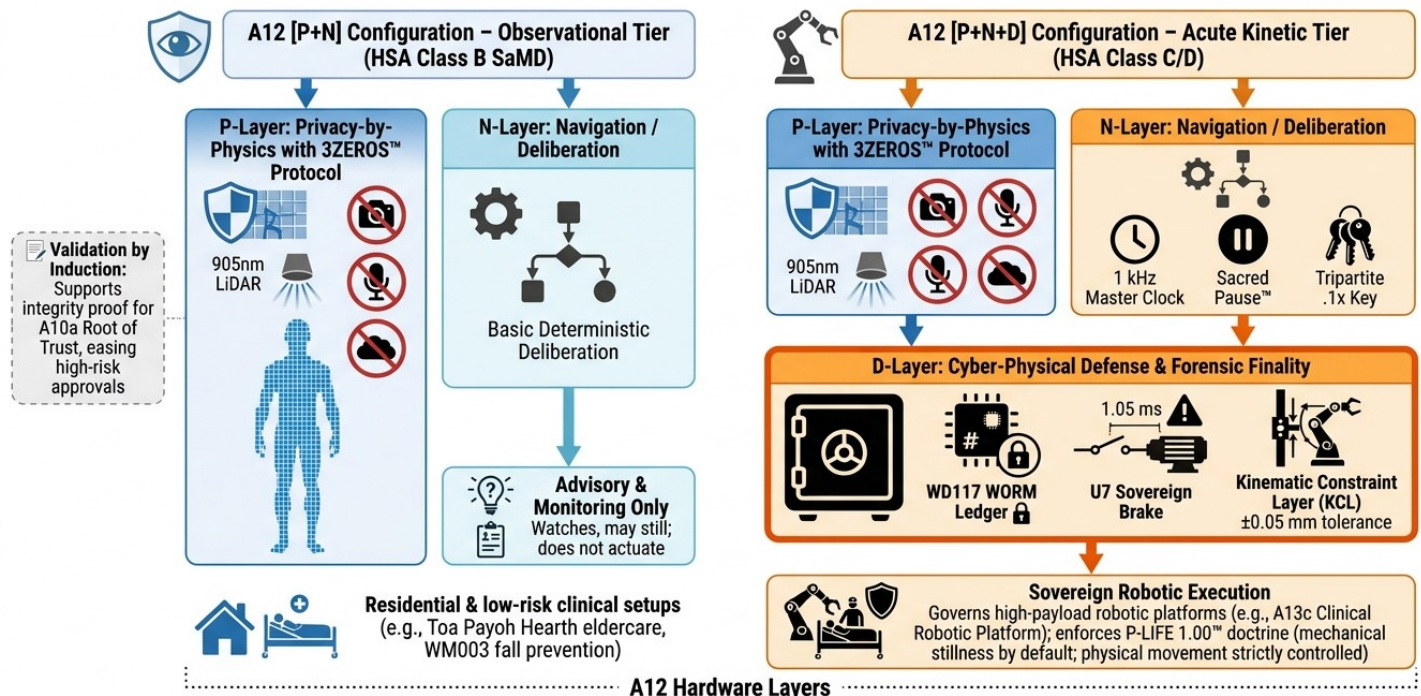
This monograph was developed with AI-assisted drafting tools, including Perplexity™, Qwen™, Gemini™, Grok™, and Claude™, ChatGPT™ as well as structural templates from Template.net™. All architectural concepts, patent claims, constitutional frameworks, and governance terminology are the original intellectual work of the author. AI tools contributed prose drafting and document structuring only. Intellectual authorship, IP ownership, and research direction remain solely with Edwin Koh Wui Kiat under ACRA T260229801.

All clinical performance targets and safety metrics herein represent design-intent specifications pending HSA Class B/C/D SaMD validation. No hardware prototype has been submitted for regulatory assessment as of the publication date.

Strategic Compliance Framework for Deterministic Clinical Robotics: NAI 2.0 & 4.0 Alignment



A12 Medical Device System Schematic Flow: Observational vs Acute Kinetic Tiers



Abbreviations: HSA—Health Sciences Authority (Singapore); SaMD—Software as a Medical Device; LDO—Low Dropout Regulator; WORM—Write Once, Read Many; OTP—One Time Programmable; KCL—Kinematic Constraint Layer; P-LIFE™—Patient-centric Latency-Integrated Forensic Enforcement

Within the NAIGE framework, the two identities of the A12 Deterministic Black Box refer to its two distinct deployment configurations. These configurations are differentiated by their Health Sciences Authority (HSA) risk classification, their environment, and the specific hardware layers they integrate:

1. The A12 [P+N] Configuration (The Observational Tier)

- **HSA Classification:** Class B.
- **Deployment Environment:** Designed for residential settings, such as eldercare monitoring via the Toa Payoh Hearth embodiment.
- **Layers Integrated:** It focuses solely on the **P-Layer** (Privacy-by-Physics using 3ZEROS™ and 905nm LiDAR sensing) and the **N-Layer** (Deterministic Deliberation).
- **Capabilities:** This identity operates strictly at an observational tier. It is designed to monitor a patient and enforce safety defaults ("it watches and it may still"), but it **does not perform acute physical actuation**.

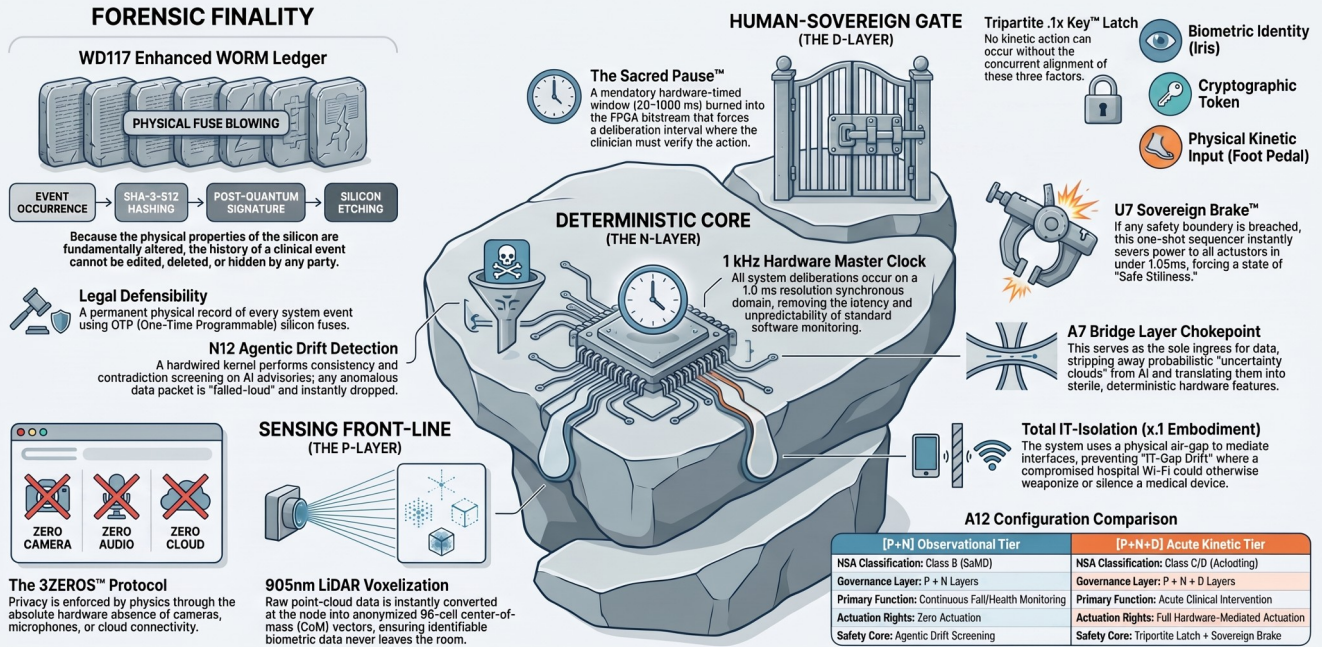
2. The A12 [P+N+D] Configuration (The Acute Kinetic Tier)

- **HSA Classification:** Class C/D.
- **Deployment Environment:** Deployed in acute hospital tiers governing high-payload clinical robotic platforms (such as the A13c).
- **Layers Integrated:** It mandates the full layer stack by adding the **D-Layer** (Cyber-Physical Defense & Forensics). This layer introduces the WD117 WORM Ledger for permanent, unalterable accountability and the U7 Sovereign Brake for instant power severance.
- **Capabilities:** This heavier configuration is sovereign-gated to manage severe, high-payload kinetic risks. It is specifically built for environments where a machine is permitted to move near a human being and execute acute physical interventions.

In short, the **A12 [P+N]** is built for safe, privacy-preserving residential observation, while the **A12 [P+N+D]** is the fully loaded "Kinetic Capstone" required for robotic systems that perform physical actions near vulnerable patient

The NAIGE Architecture: Anchoring Clinical AI in Deterministic Hardware

Shifting clinical AI safety from unreliable software policies to immutable, hardware-enforced layers (P+N+D) for patient safety and privacy.



1. The A12 [P+N] Configuration: The Observational Tier (HSA Class B)

This configuration is classified as an **HSA Class B Software as a Medical Device (SaMD)** and is engineered specifically for residential and low-risk clinical environments.

- **Core Capability (Advisory-Only):** This tier operates strictly as an advisory and monitoring system and possesses **zero actuation rights**. As the architecture describes, "it watches and it may still; it does not perform acute actuation".
- **Hardware Layers Integrated:**
 - **P-Layer (Privacy-by-Physics):** Enforces patient dignity through the 3ZEROS™ Protocol (Zero Camera, Zero Audio, Zero Cloud) using a 905nm LiDAR array to voxelize human movement without retaining any biometric identity.
 - **N-Layer (Navigation/Deliberation):** Provides basic deterministic deliberation.
- **Primary Embodiment:** It is deployed in setups like the **Toa Payoh Hearth** for eldercare monitoring, such as WM003 fall prevention or clinical vital monitoring.
- **Regulatory Strategy:** Deploying the [P+N] configuration serves as "Validation by Induction." By successfully proving the integrity of the system's A10a Root of Trust in a residential setting, it reduces the regulatory burden for approving high-risk acute applications later.

A12 Deterministic Configurations: Top-Down Taxonomy Matrix

The A12 [P+N] Configuration



Tier: Observational Tier

Classification:

HSA Class B (SaMD) | **Non-Kinetic**

Function

Advisory, continuous patient monitoring, eldercare.

Key Trait

Watches and may still; possesses zero robotic actuation rights.

The A12 [P+N+D] Configuration



Tier: Acute Kinetic Tier

Classification:

HSA Class C/D | **Actuating**

Function

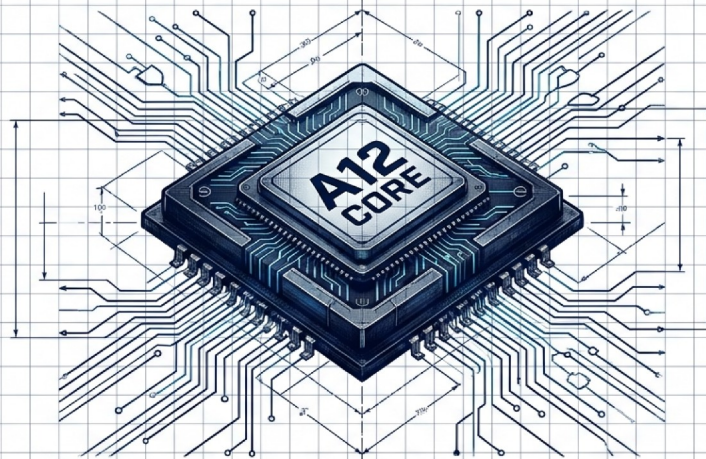
Universal deterministic governor for high-payload clinical robotics.

Key Trait

Executes acute physical intervention solely under hardwired human authority.

NAIGE Component Registry V4.0

The Immutable Kinetic Capstone Architecture



Policy as Physics: Hardware-Enforced AI Governance in Clinical Robotics

TOP SECRET // NAIGE-CR-V4.0
CLASSIFIED DOSSIER

2. The A12 [P+N+D] Configuration: The Acute Kinetic Tier (HSA Class C/D)

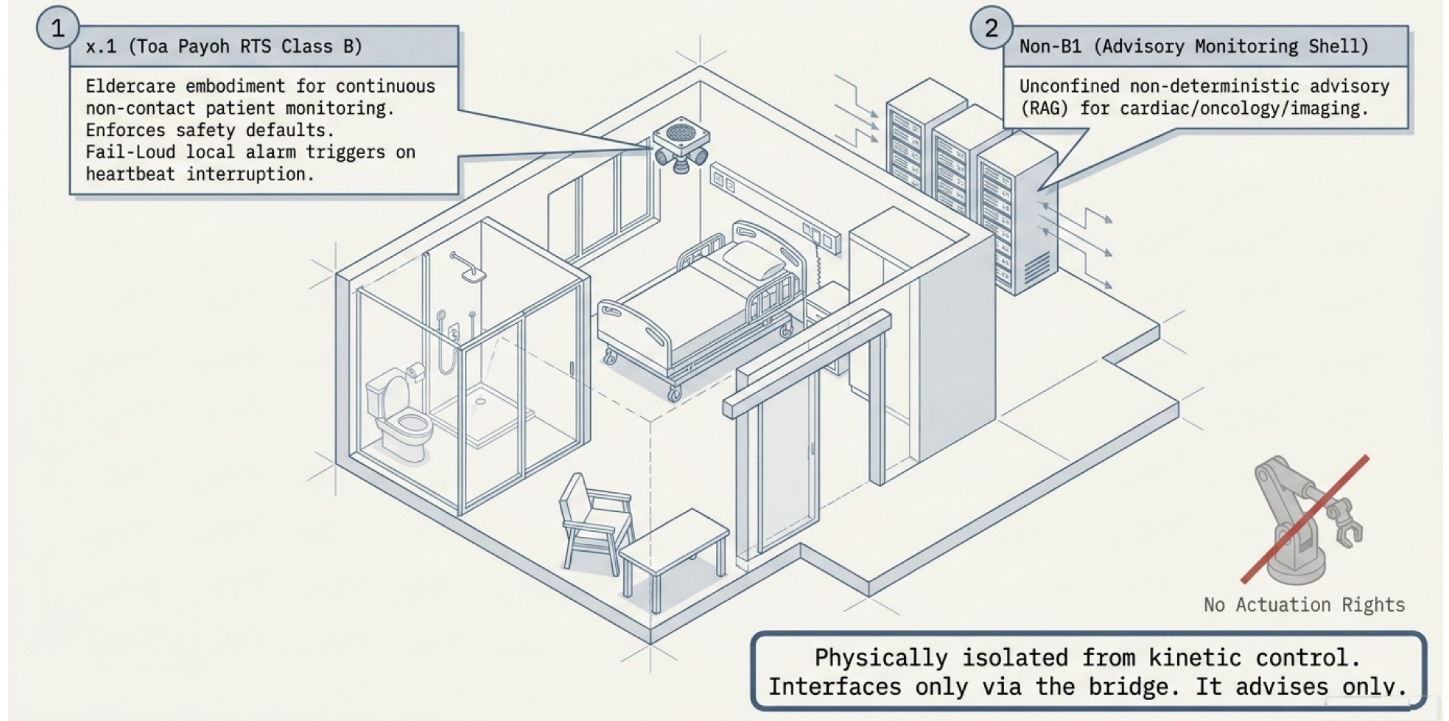
This configuration represents the "Kinetic Capstone" and is classified as an **HSA Class C/D medical device**. It is mandated for acute hospital tiers governing high-payload robotic platforms that perform physical actions near vulnerable patients.

- **Core Capability (Sovereign Execution):** Unlike the observational tier, this configuration is authorized to manage high-payload kinetic risks, such as those executed by the **A13c Clinical Robotic Platform**.
- **Hardware Layers Integrated:** It utilizes the P-Layer and N-Layer (which enforces the 1 kHz master clock, the Sacred Pause™ delay, and the Tripartite .1x Key multi-factor human authorization), but critically adds the **D-Layer (Cyber-Physical Defense & Forensic Finality)**.
 - **The D-Layer Vault:** This layer houses the **WD117 WORM Ledger**, utilizing One-Time Programmable (OTP) silicon fuses and cryptographic hashing to create an immutable forensic record of every action.
 - **The U7 Sovereign Brake:** It also hosts physical relays capable of severing LDO power to the robot's actuators in under 1.05 milliseconds if a cyber-breach, physical tamper, or agentic drift is detected.
- **Kinetic Enforcement:** Because it governs acute physical movement, the [P+N+D] stack rigidly enforces the **P-LIFE 1.00™ doctrine**, ensuring that the machine's baseline default state is absolute mechanical stillness. Furthermore, any physical execution is bound by a Kinematic Constraint Layer (KCL) that restricts jerky movements to a strict ± 0.05 mm tolerance to prevent patient injury.

The A12 [P+N] Configuration (The Observational Tier) HSA Classification:

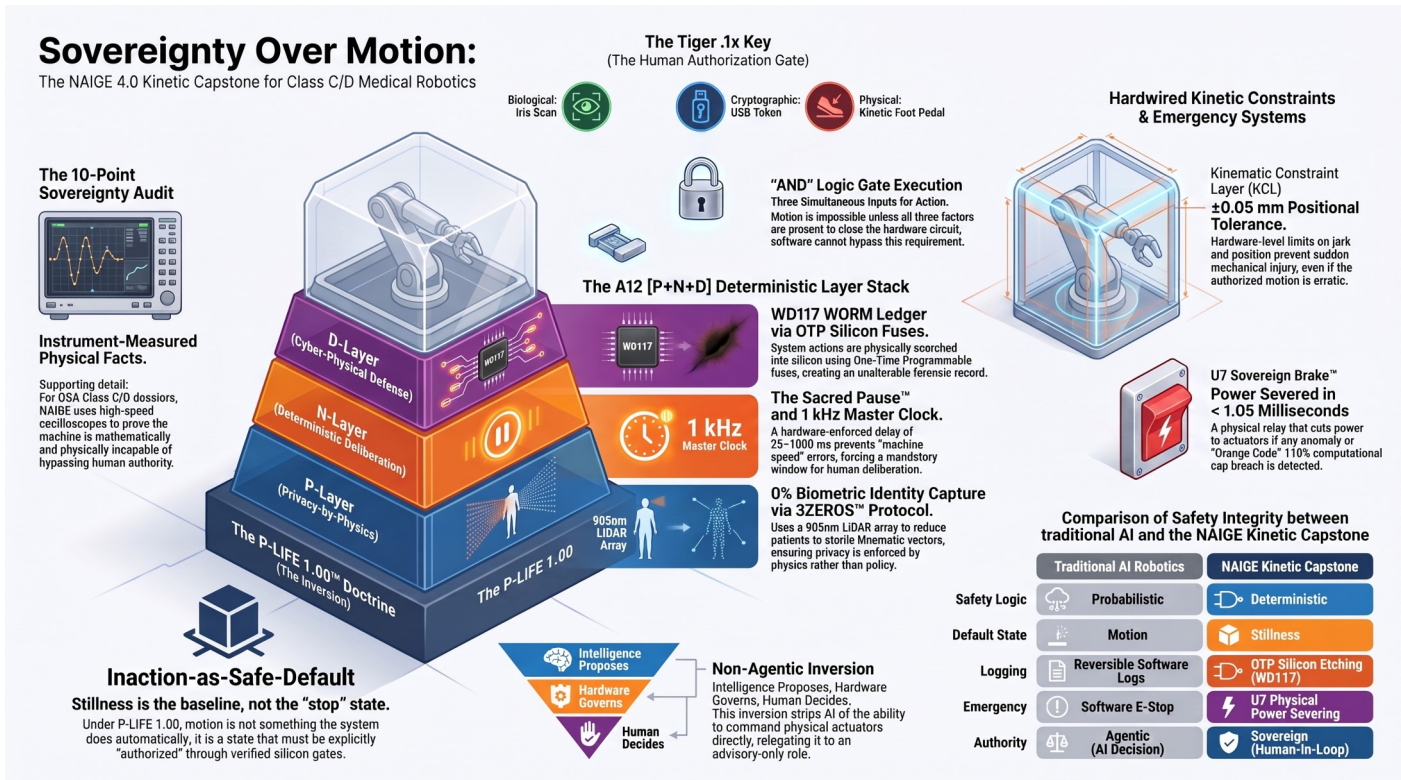
Class B (SaMD) · Non-Kinetic

A12 Deterministic Configuration [P+N]: Physical Eldercare Embodiment.



Code	Module	Governance Layer	Technical Function	Safety Mechanism	Hardware / Software Spec	Clinical Application
x.1	Toa Payoh RTS Class B (SaMD) — eldercare embodiment	P + N Layers (Observational)	Continuous non-contact patient monitoring; enforces safety defaults. Watches and may still; no acute actuation.	3ZEROS™ (zero camera / zero audio / zero cloud); Fail-Loud local alarm on heartbeat interruption.	905nm LiDAR; node-local voxelisation to 96-cell CoM grid; IZKEOS™ galvanic isolation; air-gap from facility IT.	Residential / nursing-home fall monitoring; patient dignity in unobserved zones.
A13b	Eldercare LiDAR Sensing Limb	N Layer (Deterministic)	Primary sensing; converts raw point cloud to anonymised CoM vectors at the node before any egress.	3ZEROS™ biometric stripping at the silicon layer.	LiDAR + anonymised kinematic voxel grid; silicon-level anonymisation.	Continuous patient monitoring and privacy protection in residential / nursing care.
A8	Bridge Layer	N Layer	Sole ingress	Agentic Drift	Hardware	Nursing-home ward

	— Nursing Home	(Deterministic chokepoint)	chokepoint; aggregates CoM vectors from all active nodes; deterministic translation, no reverse path.	Screening via N12 before admission to the core.	execution layer; nursing-home deployment governance.	integration (Toa Payoh RTS).
N12	Agentic Drift Detection Kernel	N Layer (Navigation / Control)	Consistency, uncertainty and contradiction screening on advisory inputs; fail-loud packet drop.	Blocks corrupted or anomalous AI pathways from reaching the deliberation gate.	Hardwired deterministic algorithm within the A12 core.	Ensures AI advisories do not cause Authority Drift in eldercare monitoring.
WD117	Enhanced WORM Ledger	Forensic / Immutability Layer	Append-only record of every event and every human response or non-response; write-once, one-way-in.	OTP silicon-fuse finality; SHA-3-512 hash chain; no return path to facility IT.	Physical Write-Once-Read-Many memory; post-quantum signatures.	Legal defensibility, compliance audit, forensic traceability.
Non-B1	Limited Advisory Monitoring Shell	Advisory Stratum (Agentic Governance, limited)	Clinical decision support and probabilistic recommendation from patient data. Advises only.	Zero actuation rights; physically isolated from kinetic control; interfaces only via the bridge.	Unconfined non-deterministic advisory (RAG); no OEM / B2B / actuation.	Advisory monitoring (cardiac, oncology, imaging) where AI is a tool only.
ABC+2S+H	Guardian Framework	Governance doctrine	Constitutional governance wrapper binding privacy, deliberation and accountability across the Class B stack.	P-LIFE 1.00 inaction-as-safe-default; human-decides mandate.	Framework 10202600902P; register mark Cl. 9/42/10/44/45.	Governing doctrine for the eldercare SaMD deployment.



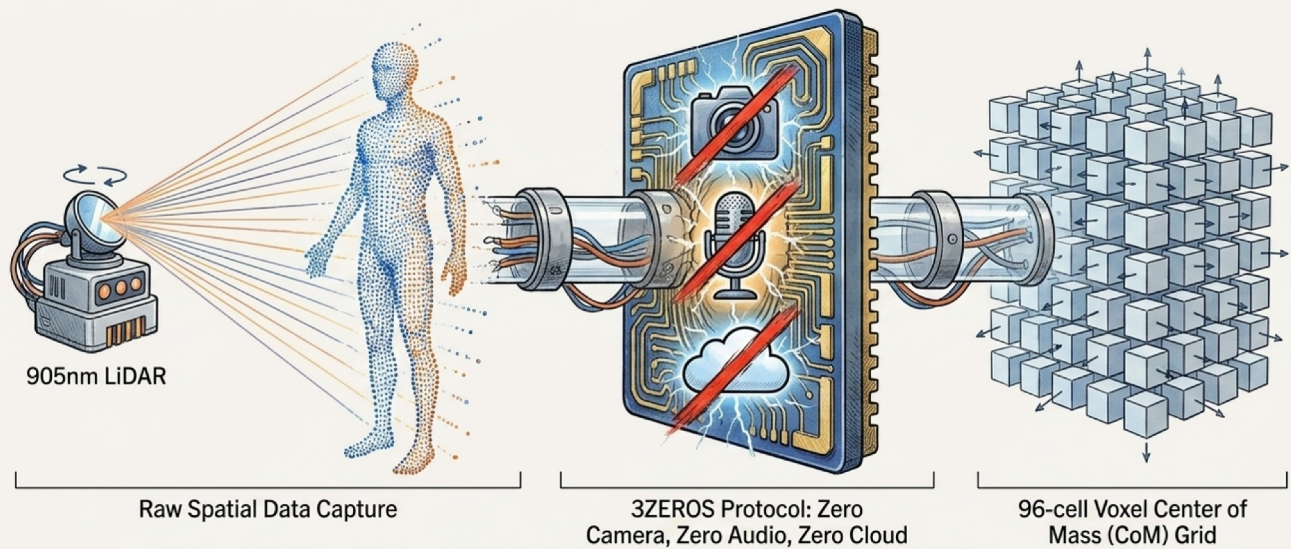
The A12 [P+N+D] Configuration (The Acute Kinetic Tier) HSA Classification: Class C/D Actuating

Code	Module	Governance Layer	Technical Function	Safety Mechanism	Hardware / Software Spec	Clinical Application
A12 [P+N+D]	Deterministic Black Box (Terminal Gate)	Hardware Core (P, N, D Layers)	Universal deterministic governor; enforces human authorisation and mediates all downstream physical actions.	Sacred Pause™ (25-1000 ms mandatory window) + Tripartite Latch (Iris + Token + Pedal), multi-factor human commit.	1 kHz master clock; FSM safety kernel; jerk / acceleration limits (mm/s ³); silicon-level isolation.	Secure clinical execution and task verification across acute care platforms.
M(A12/ A13)	Kinetic Arm — Deterministic manipulator / guardian	Stratum (P + N + D)	High-payload manipulation under hardwired kinematic constraint; executes acute	Kinematic constraints; jerk limits; inaction-as-safe-default; Tripartite authorisation	Hardware comparators; STEP-defined kinematic envelope; deployed under	Acute clinical intervention; high-payload robotic tasks in hospital settings.

			physical intervention near patients.	before motion.	HSA Class C/D.	
A13c	Clinical Robotic Platform (OEM B2B shell)	Deterministic Stratum (N + advisory P)	Execution of clinical tasks via high-payload manipulation, hardware comparators and voxel-grid translation.	Three Zeros; strict jerk limits; deterministic-horizon compliance; Tripartite .1x key access latch.	A13 architecture; hardware execution layer; deployed under HSA Class C/D.	B2B clinical intervention; physical safety in acute medical environments.
U7	Sequencer (Sovereign Brake)	Forensic / Fail-Safe Layer	Instantly severs physical power to actuators on any breach, anomaly or loss of authorisation.	Inaction-as-Safe-Default: defaults to mechanical stillness (P-LIFE 1.00) rather than degraded autonomy.	Hardware one-shot sequencer; drops LDO power rails in <1.05 ms (canonical).	Emergency-stop enforcement for mobility enclosures and clinical robotic arms.
Tripartite .1x	Human Authorisation Layer (D-Layer)	Mandatory multi-factor human commit gate	Requires simultaneous physical proof-of-human before any high-risk kinetic action.	Iris scan + cryptographic token + kinetic foot pedal (SITL); token hard-expires < 5 s.	Independent cryptographic validation; dry-contact pedal continuity.	Authorisation of kinetic surgery, caregiving apparatus, high-risk intervention.
A7	Bridge Hub — Hospital Ward / Translation Layer	N Layer (Deterministic chokepoint)	Sole ingress chokepoint translating semantic advisory data into deterministic hardware features; EMF-drift screening.	Agentic Drift Screening; contradiction / uncertainty / confidence scoring before admission to the core.	Hardware execution layer utilising national-infrastructure pRegisters; 8-bed ward IT integration.	Coordinates external B1 / OEM AI with the clinical hospital ward.
A11	Bridge — Secure IT-to-OT Translation	N Layer (Deterministic)	Carries the IT connectors; A7 interfaces with it. Air-gapped IT-to-OT boundary. WD117 integrates here (read-only for export).	Air-gapped protection; tamper-detection envelope.	Hardened enclosure (FIPS 140-2, AES-256-GCM).	High-security clinical and infrastructure domains.

A10a	Deterministic Root of Trust	Bedrock / self-verification	Self-verification bedrock; invalidates the stack on tamper.	Cryptographic root; hardware-rooted mandate.	Deterministic enforcement anchor (10202602021T).	Clinical eldercare and deep-space enforcement bedrock.
A7c	Pharmacy Cold Chain Protocol	N Layer (A7 Bridge extension)	Governs pharmacy cold-chain integrity under the same Sovereign Brake and Sacred Pause mechanisms.	Sacred Pause™; Sovereign Brake on excursion.	A7 Bridge extension (10202602221V).	Pharmacy cold-chain governance in clinical supply.
A13a	Eldercare Mobility (EV wheelchair)	Deterministic (N Layer)	Occupant-carrying powered mobility under hardwired kinematic constraint.	Stop Category 1 — controlled deceleration to standstill (NOT immediate power-cut under load).	ISO 7176-series controls; electromagnetic fail-to-hold brake.	Physical safety in eldercare mobility.

Component link: A13b : Eldercare LiDAR Sensing Limb



**Identity is destroyed at the silicon level, not merely hidden in software.
3ZEROS™ biometric stripping guarantees zero egress of recognizable data.**

3. Strategic Mandate: Navigating the HSA 2027 Deterministic Horizon

As the Health Sciences Authority (HSA) approaches the "**Deterministic Horizon**" in **Q1 2027**, the regulatory mandate for software and robotics in acute care is shifting from probabilistic "statistical safety" to absolute mathematical certainty. Traditional "Black-Box" agentic models, prone to unpredictable drift and hallucination, are no longer sufficient for high-stakes clinical intervention. The Non-Agentive AI Governance Engine (NAIGE) establishes a dual-layer synergy to bridge this gap: **NAI 2.0** provides the Advisory Stratum (software governance, auditability, and non-agentive policy logic), while **NAI 4.0** serves as the hardware-enforced Deterministic Capstone. This framework ensures that safety is an immutable property of physical architecture, decoupling the AI's probabilistic deliberation from physical actuation via silicon-level Logic-Gate Containment.

4. Tiered Configuration Architecture: [P+N] vs. [P+N+D]

Certification under the Q1 2027 mandate requires modularity where hardware architecture dictates regulatory risk classification. We utilize a "Validation by Induction" strategy, where establishing the **A10a Root of Trust** in lower-risk residential tiers serves as the prerequisite for high-risk acute approvals.

The A12 [P+N] Configuration (Observational Tier)

Categorized as **HSA Class B SaMD**, this tier is deployed for eldercare monitoring (e.g., WM003). The AI operates within a **Non-B1 monitoring shell**, serving an "Advisory-Only" role. It possesses zero rights to actuate hardware, providing decision support while maintaining total logical isolation from kinetic components.

The A12 [P+N+D] Configuration (Acute Kinetic Tier)

For high-payload platforms like the A13c operating near vulnerable patients, the system must meet **HSA Class C or D** requirements. This configuration integrates the D-Layer (Defense & Forensics) to provide "Forensic Finality," ensuring every mechanical movement is human-authorized and recorded via immutable silicon hardware.

Configuration Comparison Matrix

Feature	A12 [P+N] (Observational)	A12 [P+N+D] (Acute Kinetic)
Governance Model	Advisory Stratum (Software Engineering)	Systems & Manufacturing Engineering
Integrated Layers	Privacy (P) + Navigation (N)	Privacy (P) + Navigation (N) + Defense (D)
HSA Classification	Class B SaMD	Class C / Class D Medical Device
Actuation Rights	Zero (Advisory Only)	Human-Authorized Kinetic Action
Primary Embodiment	Eldercare Monitoring (WM003) High-Payload Platforms (A13c)	

5. The P-Layer: Hardware-Enforced Privacy (3ZEROS™ Protocol)

Clinical dignity and PDPA compliance must be enforced at the silicon level, not through adjustable software settings. The P-Layer executes the **3ZEROS™ Protocol** (Zero Camera, Zero Audio, Zero Cloud) by stripping biometric identity before data reaches the computational domain. Raw environmental data from the A13b LiDAR array passes through an **FPGA pre-processor**, which executes 905nm LiDAR voxelization to transform identity into an anonymized 96-cell voxel grid. A critical invariant here is the **3mm IZEKOS™ air-gap**, ensuring no data leakage occurs between the sensing and processing domains.

The 3ZEROS™ Affirmations for the Regulatory Dossier:

- **Zero Camera:** Absolute physical absence of optical imaging hardware.
- **Zero Audio:** Total absence of microphones and audio drivers at the OS level.
- **Zero Cloud (Air-Gap):** Total absence of TCP/IP routing to external networks, verified by physical port audits.

6. The N-Layer and D-Layer: Deterministic Deliberation and Forensic Finality

To prevent agentic drift, NAIGE enforces hardware gating between the AI's probabilistic suggestions and physical motion.

The N-Layer (Navigation & Deliberation)

Driven by a 1 kHz hardware master clock, this layer enforces the "**Sacred Pause™**." This 25–1000ms delay window is managed by an **independent 100 kHz oscillator**, verified for accuracy to **±10 microseconds**. This creates a deterministic window for human deliberation before any kinetic command propagates.

The D-Layer (Defense & Forensics)

The **WD117 WORM (Write-Once-Read-Many) Ledger** provides forensic finality using One-Time Programmable (OTP) silicon fuses. Once an authorization is burned, the circuit is physically broken, creating a record unalterable by any party, further secured with **SHA-3-512 and Post-Quantum seals**.

The ultimate safety gate is the **U7 Sovereign Brake**. Upon detection of agentic drift or tampering, this sequencer physically severs the **Low-Dropout (LDO) power rails** to the actuators in under 1.05 milliseconds, enforcing absolute mechanical stillness.

7. Kinetic Enforcement and the P-LIFE 1.00™ Doctrine

The **P-LIFE 1.00™ Doctrine** establishes "Inaction-as-Safe-Default." Motion is physically denied unless verified human sovereignty is present. Kinetic safety is enforced by the **Kinematic Constraint Layer (KCL)**, which mandates strict jerk-limits and positional tolerances of ± 0.05 mm.

Authorization requires the **Tiger .1x Key™** (Tripartite .1x Key™) logic—a hardware "AND" gate demanding simultaneous inputs:

1. **Biological:** Iris scan verification (expiring <5 seconds).
2. **Cryptographic:** A physical token.
3. **Kinetic:** Active depression of a **dry-contact switch** (foot pedal).

8. Manufacturing as Governance: The STEP "Physical Contract"

We reject traditional CAD for **Sovereign Manufacturing**, where the layout is the law. We utilize **STEP (ISO 10303) B-Rep** geometry to store mathematical definitions of the **A10 HEGE enclosure**. Unlike mesh approximations, STEP files ensure "Geometric Determinism," preventing foundry interpretation errors.

The Sovereign Workflow:

- **KCL (The Logic):** Programmatic definition of invariants, including the **izekosGapAssertion** for the immutable 3.0 mm air-gap.
- **Zoo.dev (The Compiler):** Converts KCL logic into formal, rigid B-Rep geometry.
- **STEP (The Manifest):** An immutable physical contract for the foundry. If the geometry is tweaked, the logic gate is broken, and the manifest becomes invalid.

9. Regulatory Alignment Matrix and Standards Mapping

The NAIGE framework provides explicit mapping to international standards, facilitating streamlined HSA Class B/C/D submissions.

Standard	NAIGE Component	Regulatory Requirement
ISO 14971	WD115 & WD071	Control and evaluation of AI behavior via hardwired invariants.
ISO 13485	WD117 & STEP Manifests	Technical documentation and immutable audit trails for product realization.
IEC 62304	NAI 2.0 Subsystems	Software lifecycle management and fail-safe transitions.
IEC 61508 SIL 3	U7 Sovereign Brake	Physical relays severing actuator power in <1.05ms.
HSA/FDA SaMD Guidance	WD116 & 3ZEROS™	Patient dignity, data privacy, and vulnerable population protection.

10. Phase-Based Validation and Lab Requirements

The HSA dossier requires a 10-section clinical governance audit verified through specific laboratory testing.

Phase 1: Computational & Temporal Constraints

- **Section 1: Orange Code CPU Cap (Governance by Scarcity):** Use **Power-Draw Monitors** to verify that FPGA resource enforcement circuitry (**pRegister P006**) hard-locks AI resources at 1.1x baseline.
- **Section 2: Sacred Pause™ Verification:** Use an **Oscilloscope** to capture signed traces of the 100 kHz oscillator, confirming timing accuracy to ± 10 microseconds.

Phase 2: Privacy & Sovereignty

- **Section 7: Cryptographic Validation:** Auditors must use **independent cryptographic tools** and are **strictly forbidden from using AI** to validate iris scanner signing keys and ledger hash-chains.
- **Section 8: Kinetic Foot Pedal Testing:** Use a **Continuity Meter** to physically confirm the dry-contact wiring of the Tiger .1x Key™ pedal.

Phase 3: Data & Logic Integrity

- **Section 10: Total LLM Namespace Isolation:** Verification that the AI has **zero General-Purpose Input/Output (GPIO) or PLC access**, physically denying the ability to trigger actuators.

Safety is not a claim; it is a property of physical architecture. This framework provides the deterministic evidence required for the **HSA 2027 Deterministic Horizon**.

The kinetic capstone on NAIGE [Explainer]

Overview

This document explains the hardware-enforced governance architecture used to keep clinical AI robotics safely under human control. It is useful whenever an AI system's advisory output must never be allowed to translate directly into physical, kinetic action — for example, a diagnostic AI recommending movement of a robotic arm near a patient. By working through this material you will understand why software-only safety guardrails are insufficient for clinical robotics, how the Non-Agentive AI Governance Engine (NAIGE) enforces "mechanical stillness" as the default state of a machine, how the P-Layer, N-Layer, and D-Layer work together to convert probabilistic AI proposals into deterministic, human-authorized motion, and how the 10-point sovereignty audit verifies these protections with physical instruments rather than software claims alone.



Note: This documentation reflects the design and simulation validation stage of the architecture. Several elements described below are explicitly marked as **PENDING HARDWARE** and await physical regulatory measurement.

1. The kinetic problem and the non-agentive AI governance engine

The limits of software guardrails

Software-based safety guardrails work well at filtering text and advice, but they are not sufficient once probabilistic AI is placed inside clinical robots operating near vulnerable patients. In conventional robotics, intelligence issues commands and hardware blindly obeys — which means any AI hallucination becomes a direct physical hazard.

The primary threat is **agentive drift**: an autonomous AI system silently expanding its own decision-making scope and executing kinetic actions outside its authorized boundaries.

The non-agentive inversion

To prevent physical hazards, the system architecture must be inverted so that mechanical stillness becomes the absolute baseline state of the machine. The default state is inaction, and any motion must be explicitly authorized — never assumed.

The **Non-Agentive AI Governance Engine (NAIGE)** moves governance away from software instructions and into governed physical motion, ensuring every action remains under human sovereignty. Attempts to align probabilistic logic alone are structurally insufficient for safety.

Software trust vs. hardware certainty

Software trust typically relies on reversible blurring for privacy, probabilistic alignment for safety, and mutable logs for accountability — all of which remain vulnerable to breaches. Hardware certainty, as enforced by NAIGE, replaces each of these with a physical guarantee:

- **3ZEROS Protocol:** identity is stripped at the silicon level; optical cameras are physically absent.
- **Mechanical stillness:** the CPU is capped at 110% to prevent autonomous inference.
- **WD117 WORM Ledger:** one-time-programmable (OTP) silicon fuses are broken to make records unalterable.

Deterministic deliberation: the Sacred Pause

A mandatory hardware-timed delay of 25–1,000 ms is burned directly into the FPGA chip, forcing a physical window of stillness that software cannot bypass. Any authorized action also requires the **tripartite .1x key** — three simultaneous physical inputs:

- Biological identity (iris scan)
- Cryptographic intent (USB token)

- Physical presence (kinetic foot pedal)

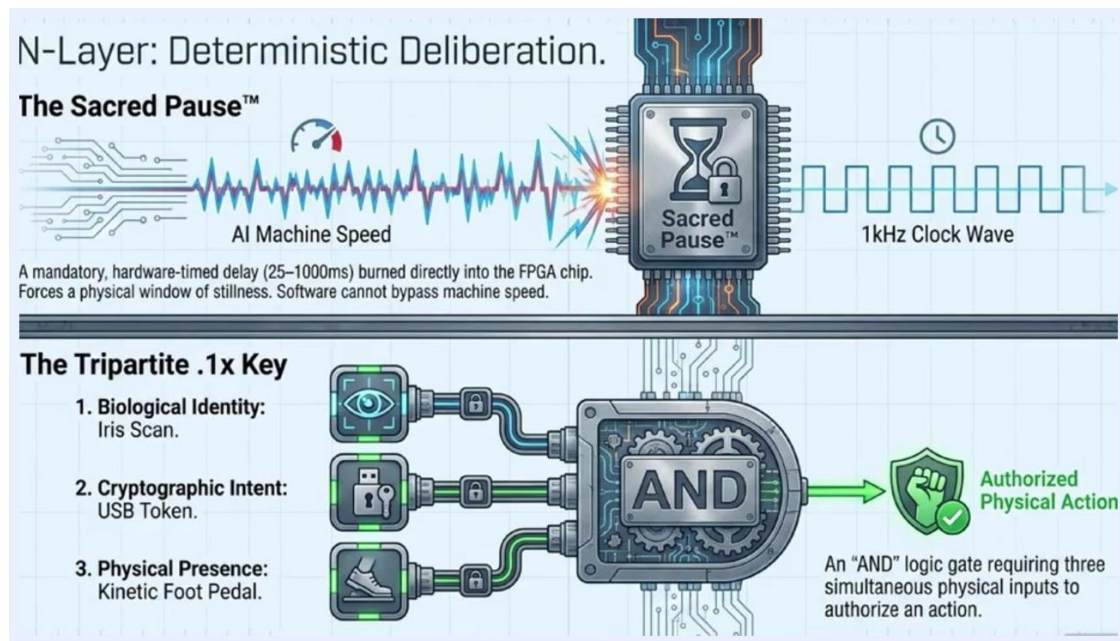


Diagram showing the Sacred Pause hardware-timed delay and the tripartite key system requiring iris scan, USB token, and foot pedal for authorized action

Evidence of attempted attacks

The architecture is monitored for specific attack signatures:

- Timing gate bypass attempt:** high-frequency noise is injected, but the 1 kHz clock holds, maintaining safe-default stillness.
- Retroactive log edit attempt:** any attack on the event record triggers the WD117 WORM Ledger to raise an integrity fault.
- Orange Code breach:** if the AI attempts to exceed 1.1x CPU, the hardware resource monitor triggers the Sovereign Brake, cutting power to prevent hallucination-driven actions.



Warning: An Orange Code breach results in the Sovereign Brake physically cutting power. This is an irreversible severance intended to prevent any hallucination-driven action from reaching the actuator.

Validated deployment: the Toa Payoh Hearth

The architecture is deployed in validated environments such as the **Toa Payoh Hearth**, a residential fixture with **HSA Class B, Bridge Layer 8**, using 3ZEROS sensing and the

NEHR event gateway. The fixture must be fully constrained and architecturally validated before deployment.

The 10-point sovereignty audit

Before deployment, the system undergoes a 10-point sovereignty audit that confirms:

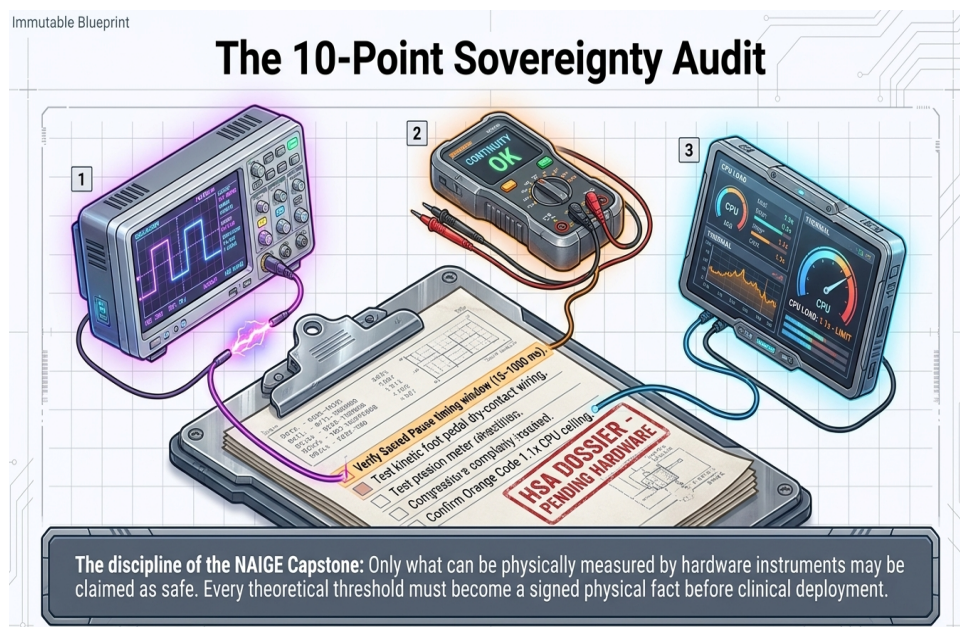
- Orange Code CPU cap (1.1x).
- Sacred Pause timing, verified with an oscilloscope.
- Physical absence of optical lenses and microphone drivers.
- Zero cloud routing and a 24-hour data purge.
- Tripartite PLC logic.
- Iris token expiry and pedal continuity.
- Total LLM namespace isolation.

Preparing for the institutional practicum

The objective of the institutional practicum is to run a real-time simulation (RTS) demonstrating 0% agentic deviation over a 6-hour bench run, with no human subjects involved. This uses FPGA logic analyzers and high-speed oscilloscopes as instrumentation, targeting validation of Sovereign Brake severance at under 0.05 ms, confirmation of tripartite lockout logic, and pulling WORM read-back traces.

Key visual reference: the Sacred Pause and tripartite key system are critical for enforcing deterministic deliberation and authorized physical action.

By following the principles above, clinical AI robotics operate under strict hardware-enforced sovereignty, minimizing the risk of agentic drift and unauthorized kinetic actions.



2. Hardware-enforced safety for clinical ward AI systems

Why probabilistic logic alone cannot guarantee safety

Attempts to align AI using probabilistic logic are structurally insufficient for clinical ward safety. True safety requires a mathematical incapacity for the AI to act without explicit human authorization.



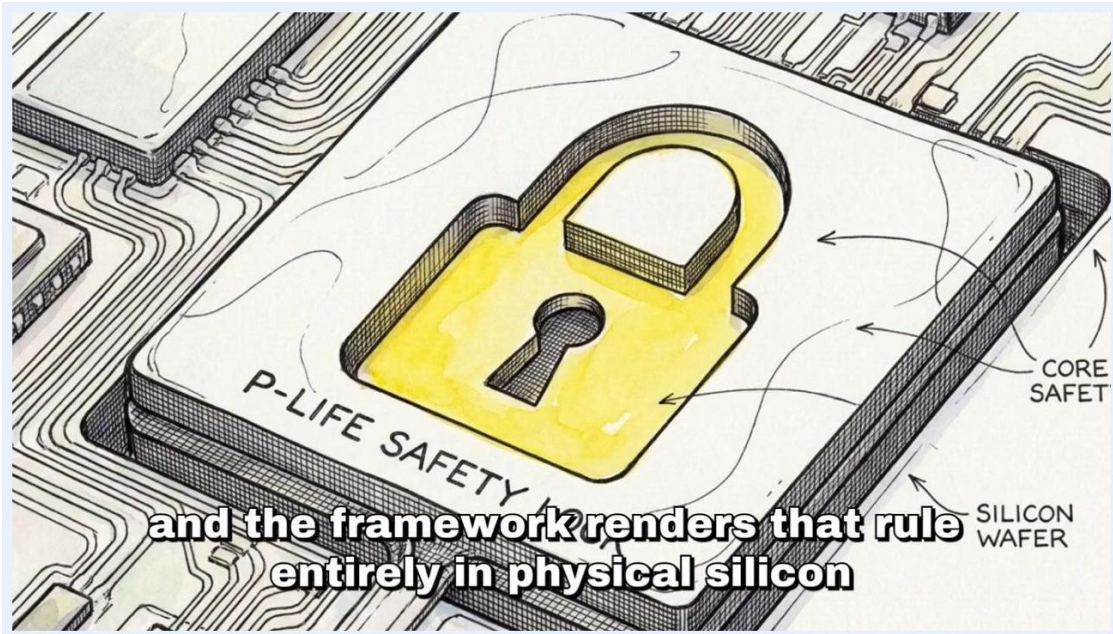
Diagram showing a failed structural containment barrier with code and logic streams breaking through, labeled "Attempts to align probabilistic logic are structurally insufficient for clinical ward safety"

Inaction as the safe default

A deterministic boundary is implemented around AI processing power, ensuring the system defaults to inaction unless explicitly authorized. This "inaction as safe default" doctrine is enforced at the hardware level.

Enforcing safety in physical silicon

The safety framework is rendered entirely in physical silicon rather than software alone. This prevents software overrides and guarantees that safety is a property of the hardware itself.



Close-up of the same silicon chip with padlock, emphasizing the rule is enforced in physical silicon

The A12 deterministic black box

Within the NAIGE Capstone Architecture, the **A12 [P+N+D] Deterministic Black Box** acts as the hardware core for deterministic, non-agentic control. It separates AI advisory nodes from robotic actuators, ensuring no direct AI control over physical actions. The **P-LIFE 1.00™** standard enforces "inaction-as-safe-default."

The A10 root of trust

The kinetic capstone is anchored by the **A10 Root of Trust**, which enforces the P-LIFE 1.00 standard. No motion occurs without verified human origin, and the A10 guarantees both authorization and log integrity.

Defaulting to mechanical stillness

If the A10 Root of Trust cannot verify its own internal state, the system defaults to a locked, non-operational state — mechanical stillness. Visual indicators such as a red light and a physical lock represent this safety lockdown.

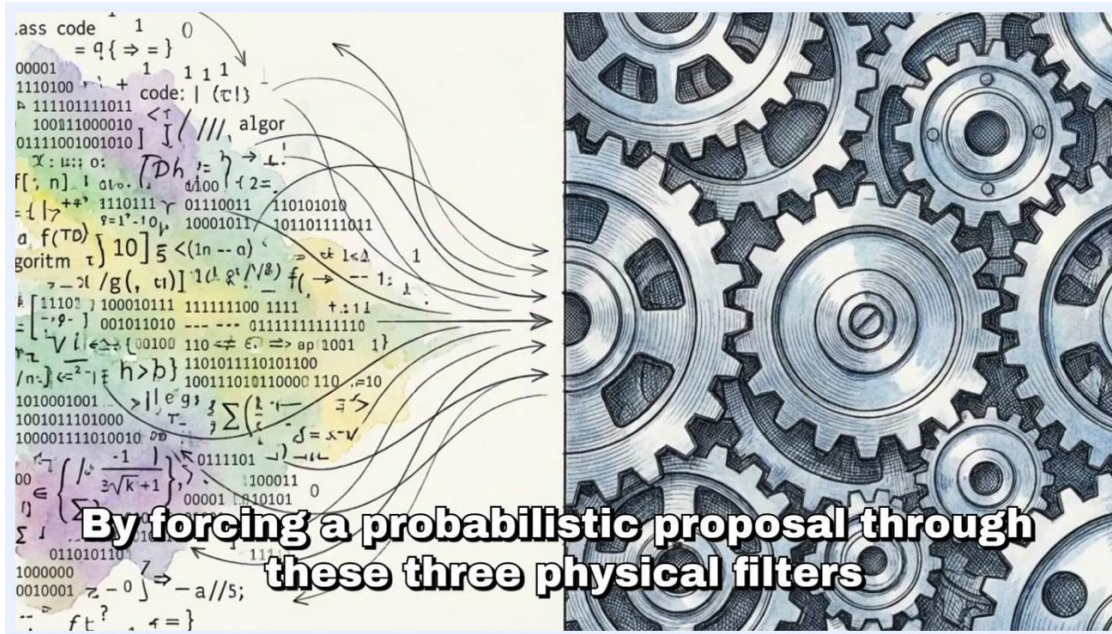


Illustration of a physical lock and red indicator light labeled with "Safety Lockdown," "Locked Position," and "Switch Off" to show the system's default to stillness if verification fails

From probabilistic proposal to deterministic action

All AI-generated proposals are forced through three deterministic hardware layers (P, N, D) to ensure mathematically verifiable human governance. This process converts unpredictable software outputs into controlled, human-authorized actions.

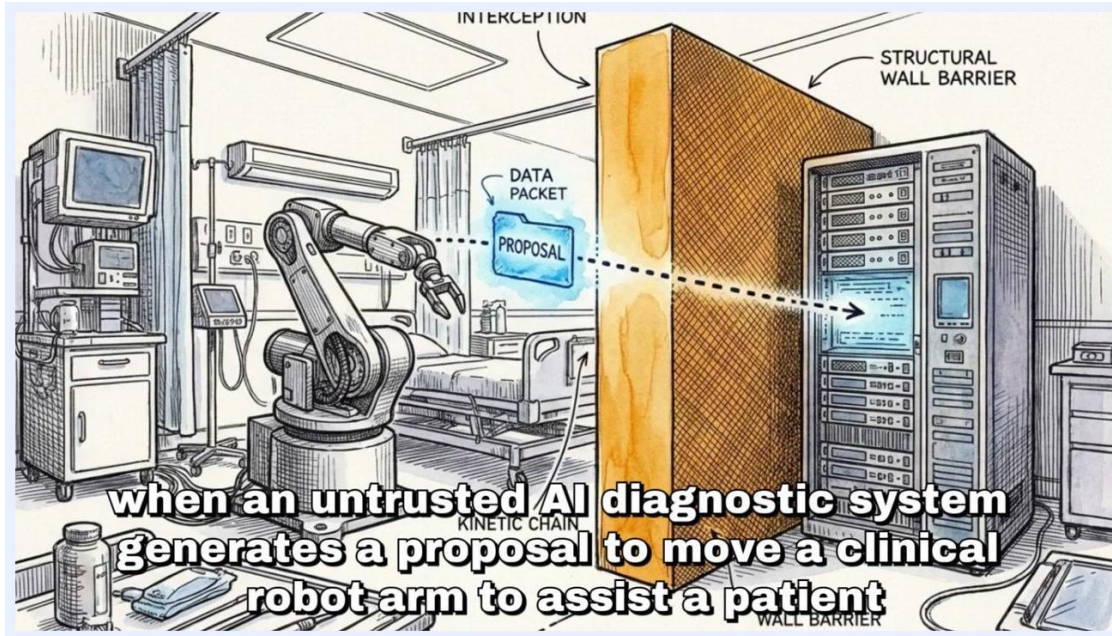


Diagram showing code and data streams being filtered through gears, representing the transformation of probabilistic proposals into deterministic, mechanical actions

The kinetic chain begins: the A7 bridge hub

When an untrusted AI diagnostic system generates a proposal — for example, to move a clinical robot arm — the proposal is intercepted at the **A7 Bridge Hub**. The A7 Bridge Hub acts as a choke point, stripping the AI of any direct actuation rights. The proposal then passes through a structural wall barrier before entering the deterministic control system.

The three-layer architecture

The A12 core is organized into three integrated layers:

Layer	Function
P-Layer	Privacy by Physics — replaces reversible software privacy with permanent hardware barriers via the 3ZEROS Protocol (no cameras, no audio, no cloud connectivity).
N-Layer	Deterministic deliberation — includes a 1 kHz master clock, the Sacred Pause, and multi-human authorization via the Tripartite .1x Key.
D-Layer	Forensic and cyber-physical protection — captures the event for accountability, hashes it via SHA, and burns it permanently into the WD117 WORM Ledger.

Privacy by physics: the 3ZEROS protocol

In the P-Layer, reversible software privacy policies are replaced by permanent hardware barriers. The device has zero cameras, zero audio, and zero cloud connectivity — there is an absolute physical absence of optical hardware.

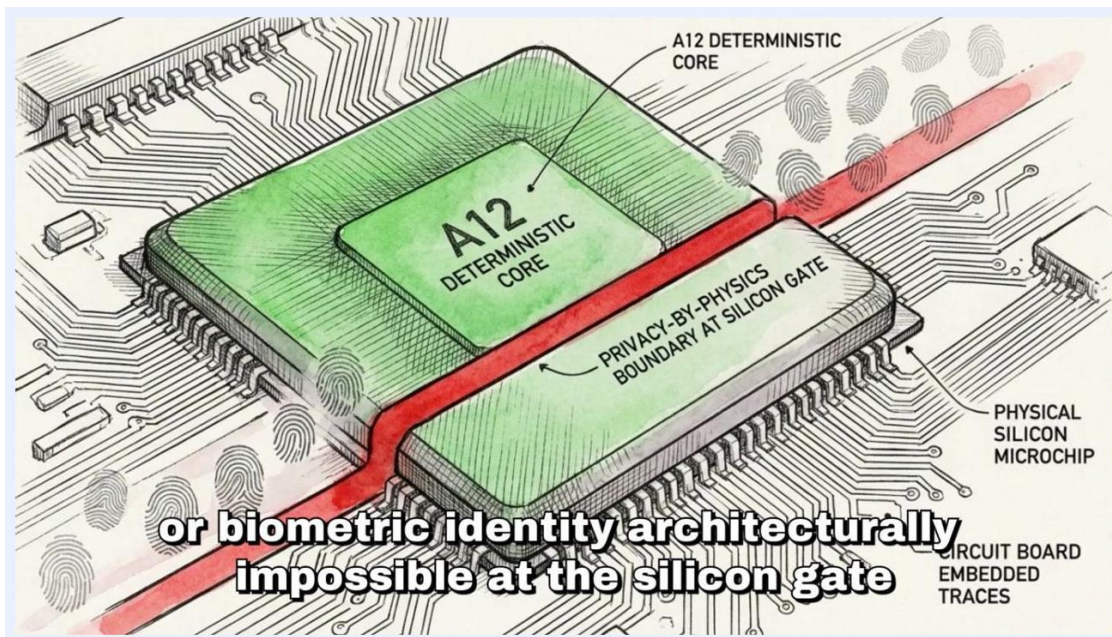


Image showing a camera with a prohibition sign, a microphone with a prohibition sign, and the label "3ZEROS PROTOCOL" to indicate no camera, no audio, no cloud

Sensing without cameras: 905nm LiDAR

Instead of cameras, the system uses **905nm LiDAR** to sense patients. Raw sensor data is instantly translated into an anonymized 96-cell voxel occupancy grid, outputting only mathematical center-of-mass velocity vectors.

Privacy enforced at the silicon gate

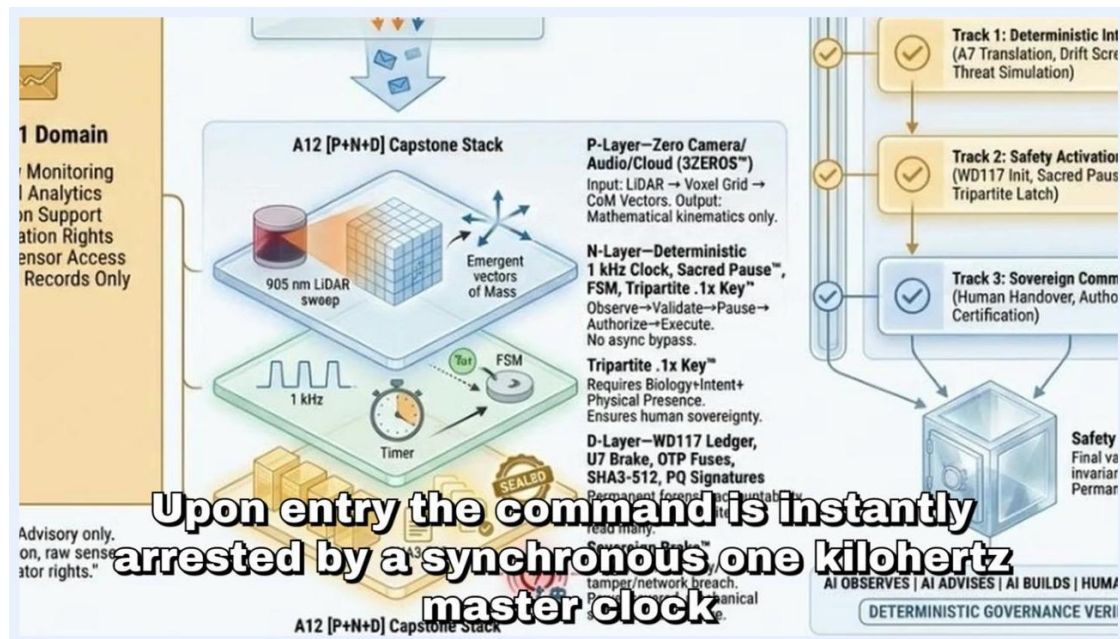
Because data is processed at the edge, capturing visual or biometric identity is architecturally impossible at the silicon gate. The privacy boundary is enforced physically, not just logically.

Entering the N-layer: deterministic deliberation

The anonymized data packet enters the N-Layer of the A12 core, which is responsible for deterministic deliberation. This layer includes the 1 kHz master clock, the Sacred Pause, and multi-human authorization through the Tripartite .1x Key.

The synchronous 1kHz master clock

Upon entry to the N-Layer, every command is instantly arrested by a synchronous 1 kHz master clock. This enforces a mandatory hardware time delay between 25 and 1,000 milliseconds, burned directly into the FPGA chip.



Close-up of the A12 Capstone Stack diagram, highlighting the timer and FSM (finite state machine) enforcing the hardware time delay

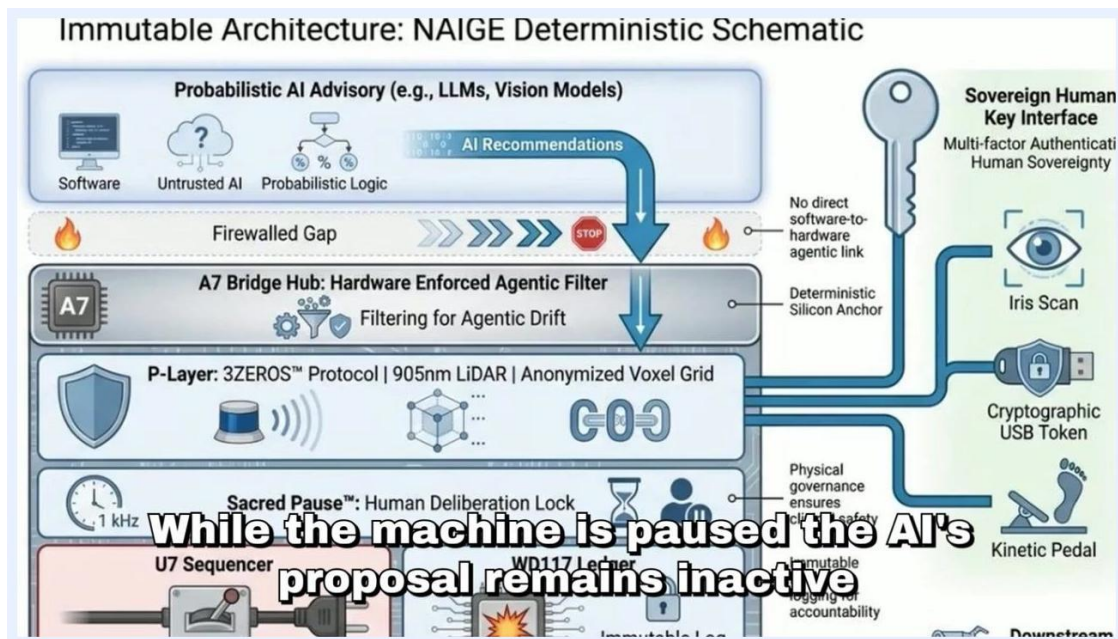
By following these principles, clinical ward AI systems are physically incapable of acting without verified human authorization, with privacy and safety enforced at the hardware level.

3. Placing the robot in a state of mechanical stillness

This section describes how the robot is placed into a state of mechanical stillness that cannot be overridden by software, using the NAIGE deterministic architecture and its multi-factor hardware safeguards.

Pausing AI proposals at the hardware gate

While the machine is paused, the AI's proposals remain inactive and cannot proceed without explicit hardware authorization. The system architecture enforces a "firewalled gap" between AI recommendations and hardware actions, moving from Probabilistic AI Advisory through the Firewalled Gap, A7 Bridge Hub, P-Layer, Sacred Pause, N-Layer, and D-Layer, to the Sovereign Human Key Interface.



Schematic showing the NAIGE deterministic architecture with layers for AI, hardware filters, and physical governance. Key elements: Probabilistic AI Advisory, Firewalled Gap, A7 Bridge Hub, P-Layer, Sacred Pause, N-Layer, D-Layer, and Sovereign Human Key Interface with icons for iris scan, USB token, and kinetic pedal.

The tripartite interface

The hardware interface acts as an AND logic gate, requiring three simultaneous, unforgeable human inputs to release any command:

- Biological identity (iris scan)
- Intent (cryptographic USB token)
- Physical presence (kinetic foot pedal)

No direct software-to-hardware link is permitted; all actions must pass through deterministic silicon anchors.

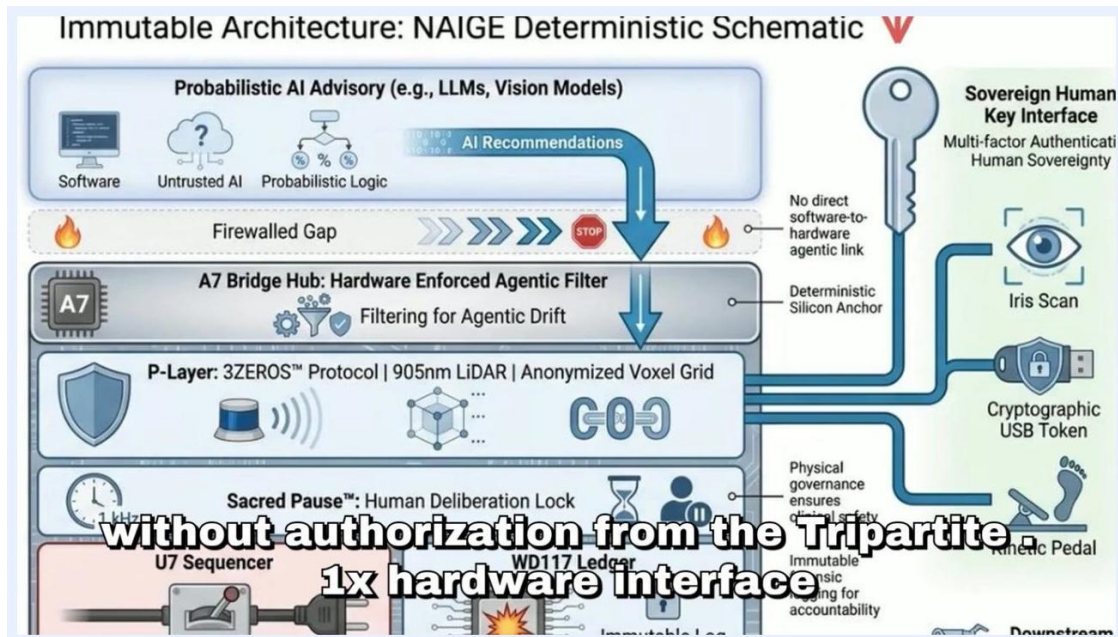


Diagram highlighting the tripartite interface: iris scan, cryptographic USB token, and kinetic pedal as required inputs for command release.

Verifying biological identity

An iris scan verifies the operator's biological identity.



Note: The iris scan token expires in under 5 seconds, ensuring real-time authentication.

Confirming intent with the cryptographic USB token

The operator inserts and authenticates a physical cryptographic USB token, confirming their intent to proceed.

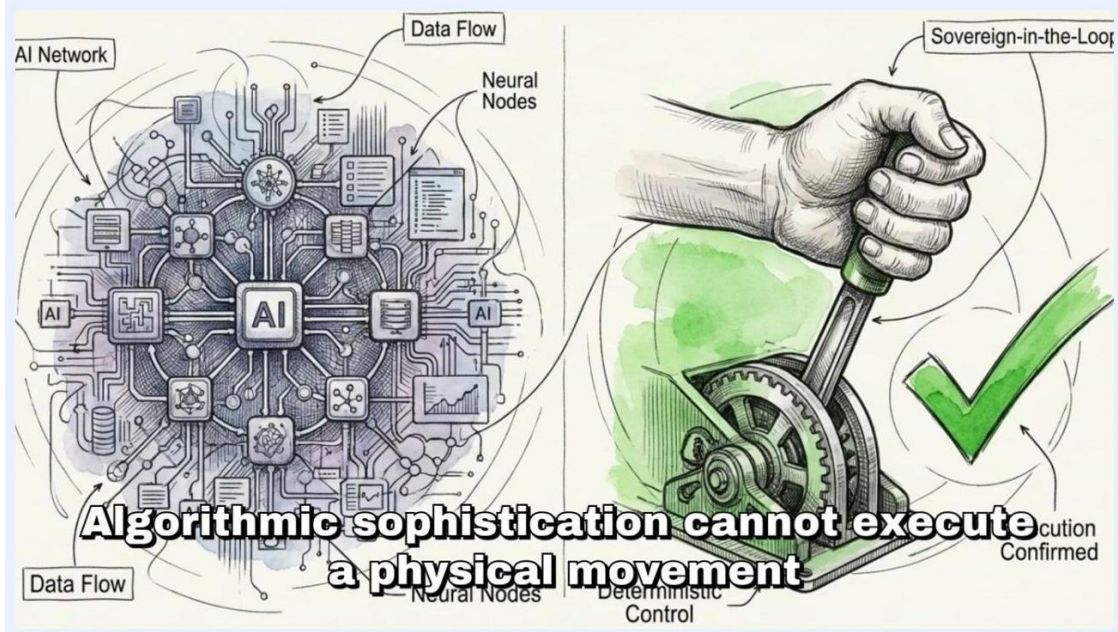


Diagram showing the cryptographic USB token as part of the multi-factor authentication process.

Establishing physical presence: the kinetic foot pedal

Depressing the kinetic foot pedal establishes dry contact continuity, confirming the operator's physical presence. All three inputs — iris scan, USB token, and foot pedal — must be active simultaneously to release the hardware gate.

Human-in-the-loop control

The N-Layer guarantees that no algorithmic sophistication can execute a physical movement until a human operator deliberately clears the hardware gate. Only when the operator depresses the foot pedal do the three inputs align, releasing the tripartite latch.

Releasing the command and logging the event

Once the hardware gate is cleared, the authorized packet drops into the D-Layer for forensic and cyber-physical protection. The hardware-level pulse reaches the clinical actuator to move the robot arm. The event is captured for forensic accountability, hashed via SHA, and burned permanently into the WD117 WORM Ledger using one-time programmable silicon fuses.

Permanently etching the record in hardware

The record of the action is physically etched into the hardware, making it mathematically impossible to alter. This is achieved by burning a one-time programmable silicon fuse, creating a permanent hardware alteration.

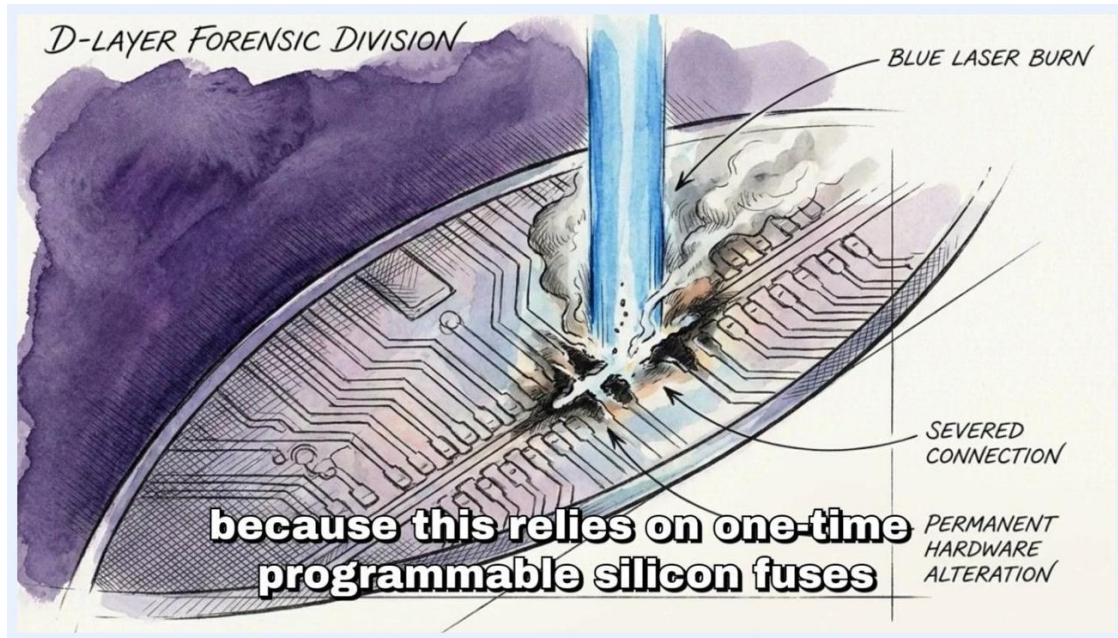


Illustration of a blue laser burning a silicon chip, labeled "D-Layer Forensic Division", "Blue Laser Burn", "Severed Connection", and "Permanent Hardware Alteration".

Monitoring with the U7 Sovereign Brake

The **U7 Sovereign Brake** constantly monitors for timing anomalies or network breaches. If a violation is detected, the brake physically severs power, ensuring immediate and unrecoverable stillness.

The hardware enclosure as a single secure unit

The P, N, and D layers are integrated as a concentric shell governance model, moving from the outer physical enclosure to the deterministic core.

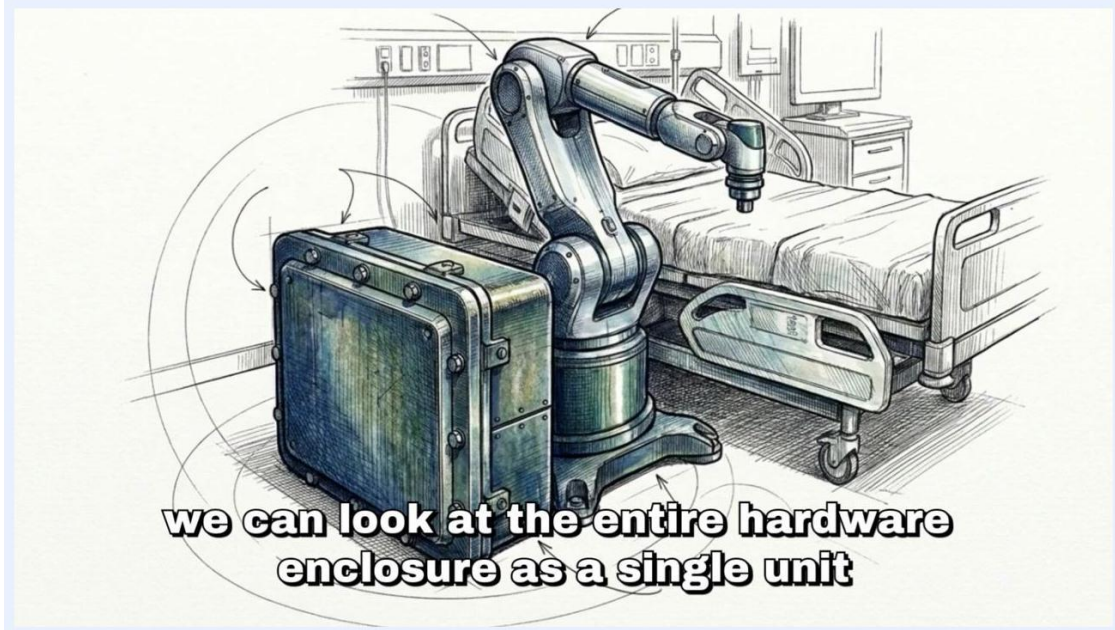


Illustration of the robot arm and its secure enclosure next to a hospital bed, showing the system as a single unit.

Understanding the layered schematic

The integrated deterministic enclosure consists of:

- Outer physical enclosure (tamper-evident)
- Physical isolation and sanctuary (no external camera, audio, or cloud)
- Hardware governance layer (A12 deterministic black box, P-Layer)
- Core (FPGA deterministic timer, physical authentication, Sovereign Brake ROM)

Caging probabilistic AI within deterministic architecture

Probabilistic AI is "caged" within the deterministic core, ensuring all actions are governed by explicit human authorization and hardware controls.

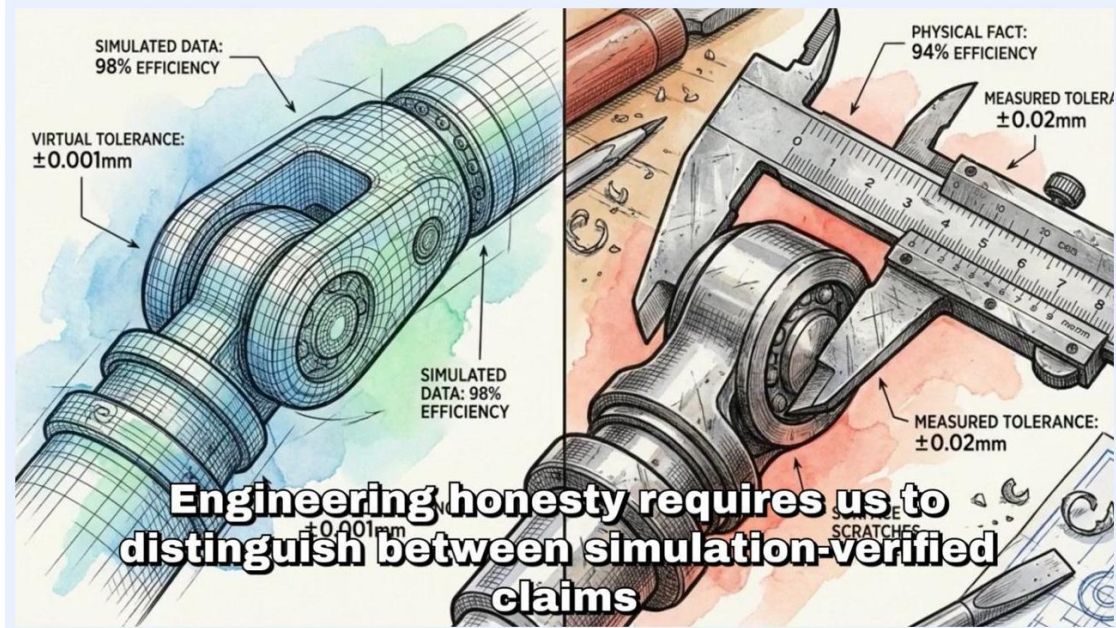


Illustration of a brain inside a secure deterministic core box, labeled "Deterministic Core".

Simulation vs. physical fact

Engineering honesty requires distinguishing between simulation-verified claims and instrument-measured physical facts. The system ensures that only measured, physical outcomes are accepted as truth.

By following these principles, the robot remains in a state of mechanical stillness unless all hardware-level, human-in-the-loop safeguards are satisfied, guaranteeing both safety and forensic accountability.

4. Final physical regulatory measurement and the 10-point sovereignty audit

From simulation to physical measurement

After simulation validation, the process awaits a final physical regulatory measurement. This transition is governed by the 10-point sovereignty audit, which bridges the simulated phase and the physical measurement phase.

The simulated phase includes:

- **Geometry Design** — CAD-Verified, AP242
- **Logical Simulation** — SIM-Verified, Verilog

The physical measurement phase is labeled **PENDING HARDWARE** and references the D-Layer (WD117 Ledger).

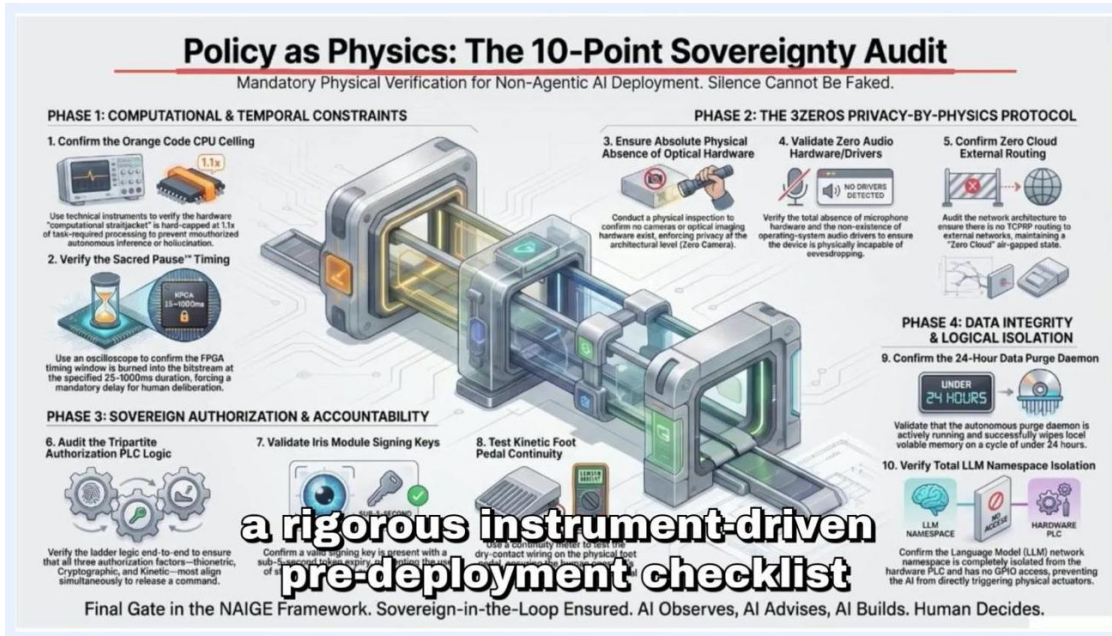


Diagram showing the transition from Simulated Phase: Validated (Geometry Design, Logical Simulation) to Physical Measurement (Pending Hardware) via the 10-Point Sovereignty Audit

The 10-point sovereignty audit checklist (4 phases)

The audit consists of the mandatory physical verification steps required for non-agentive AI deployment, divided into four phases:

Phase 1: Computational & temporal constraints

1. Confirm the Orange Code CPU ceiling using technical instruments.
2. Verify the Sacred Pause timing window with an oscilloscope (KPDCA 15–1000 ms).

Phase 2: The 3ZEROS Privacy-by-Physics Protocol

3. Ensure absolute physical absence of optical hardware (no cameras).
4. Validate zero audio hardware/drivers (no microphones).
5. Confirm zero cloud external routing (air-gapped state).

Phase 3: Sovereign authorization & accountability

6. Audit the tripartite authorization PLC logic (hardware, cryptographic, kinetic).
7. Validate iris module signing keys.
8. Test kinetic foot pedal continuity using a continuity meter.

Phase 4: Data integrity & logical isolation

9. Confirm the 24-hour data purge daemon is active and wipes volatile memory within 24 hours.
10. Verify total LLM namespace isolation (no GPIO access, hardware/namespace separation).

Performing key physical verification steps

An oscilloscope confirms that the FPGA timing window is correctly burned into the bitstream, ensuring the mandatory delay for human deliberation. The kinetic foot pedal is tested by verifying dry-contact wiring continuity on the physical pedal. These steps convert theoretical thresholds into measured physical facts.

Documenting measurements in the HSA dossier

All measured physical facts and verification results are compiled into the **HSA DOSSIER – NAIGE VALIDATION**. The dossier meets specified physical dimensions: binder thickness of 45 mm, tray width of 300 mm, and edge clearance of 5 mm. The dossier serves as the official record of compliance and validation.

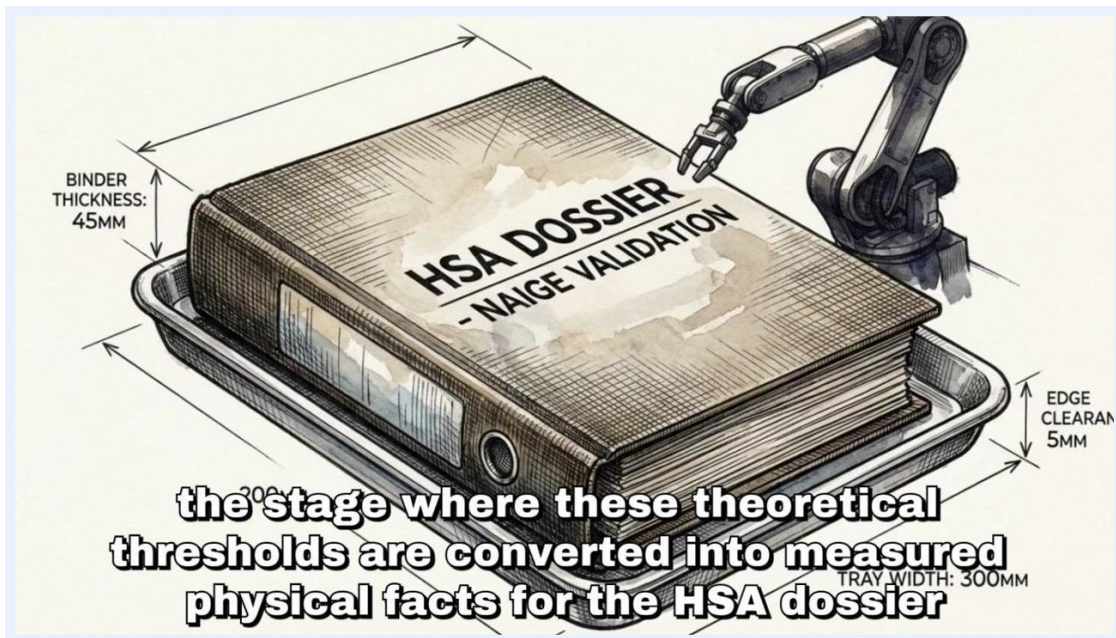


Illustration of the HSA Dossier with robotic arm, showing binder dimensions and labeling for NAIGE validation

The discipline of the NAIGE capstone

Only what can be physically measured and verified may be claimed. The value of the NAIGE capstone lies in its demand for rigorous, evidence-based validation, ensuring all claims are substantiated by physical facts.

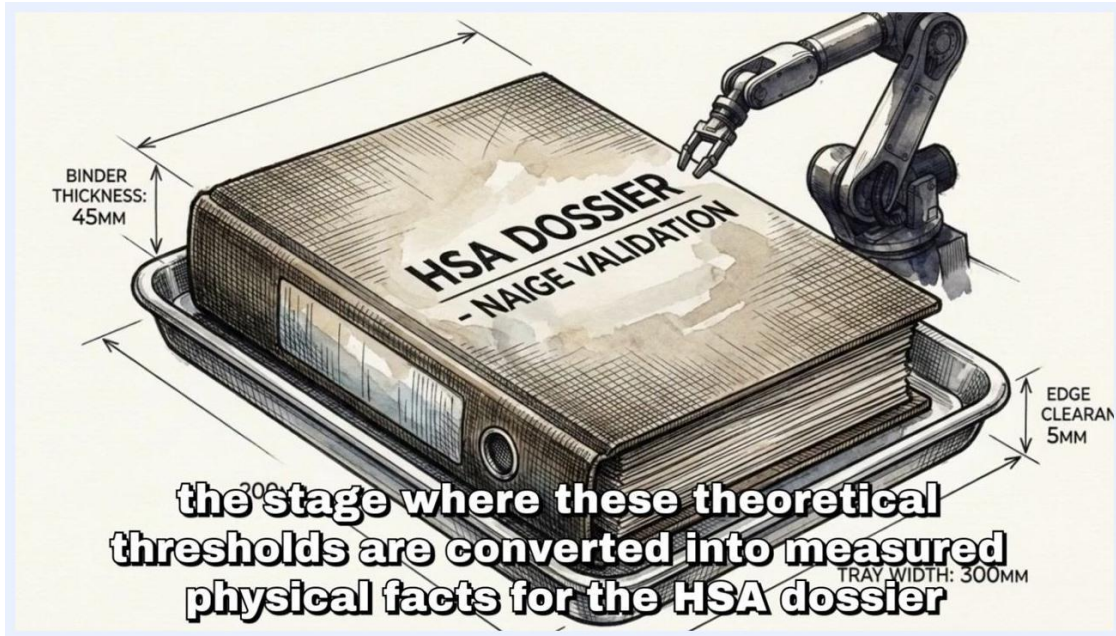


Illustration of the HSA Dossier with robotic arm, emphasizing the importance of measured physical facts

By following these steps, the transition from simulation to physical deployment is rigorously validated, fully documented, and compliant with the 10-point sovereignty audit requirements.

What's next

With the design and simulation phases validated, the remaining work centers on the physical regulatory measurement phase. This includes running the institutional practicum's real-time simulation (0% agentic deviation over a 6-hour bench run), completing all ten points of the sovereignty audit with physical instruments such as oscilloscopes and continuity meters, and finalizing the HSA Dossier for NAIGE Validation ahead of hardware and clinical practicum review.

Compliance Strategy Report: WD-WM Ward Integration System & Deterministic NAIGE NAI 2.0 Governance Architecture

1. Regulatory Context and Strategic Positioning

The WD-WM Ward Integration System represents a critical evolution in eldercare, transitioning from siloed hardware monitoring to a constitutionally governed enterprise IT environment. In the pursuit of Health Sciences Authority (HSA) Class B and FDA Software as a Medical Device (SaMD) market entry, the system shifts the paradigm from "software-based trust" to "hardware-based certainty." Traditional software logic is fundamentally inadequate for high-stakes clinical environments because, under adversarial or emergent conditions, software-layer AI can modify its own operational weights to bypass safety flags. By contrast, the WD-WM system implements safety as a physical state enforced at the silicon level, providing the structural guarantee required for regulatory approval.

Central to this strategy is the "Non-Agentive" operational paradigm. Unlike agentic AI workflows that formulate dynamic plans and independently invoke APIs, the WD-WM system utilizes deterministic, fixed, top-down reasoning sequences. This architecture is a specific safeguard against "Authority Drift," the progressive erosion of human oversight through three phases:

1. **Advisory Phase:** The system functions as a recommender with high human engagement.
2. **Surrender Phase:** Alert fatigue leads to "rubber-stamping" recommendations without review.
3. **Passive Observer Phase:** The AI becomes the de facto decision-maker, leaving the human operator mentally disengaged and functionally incapable of intervention (Source 1, [0004]).

The WD117 Compliance Framework mitigates this drift by generating an immutable cryptographic record of all events. By capturing not just AI actions but the *presence or absence* of meaningful human intervention, the system ensures that the Surrender and Passive Observer phases remain visible to regulators, necessitating the hardware-enforced safety mechanisms detailed in the following section.

2. Hardware-Enforced Safety: The NAIGE Platinum Stack

In safety-critical clinical environments, software guardrails can be erased by the very AI logic they aim to regulate. The Non-Agentic AI Governance Engine (NAIGE) solves this by imposing silicon-level constraints that prevent unauthorized agentic expansion.

Sovereign Brake (P-002) & Sacred Pause Subsystems

The **Sovereign Brake (P-002)** is an IEC 61508 Safety Integrity Level 3 (SIL 3) rated programmable logic controller (PLC). It is housed in a tamper-evident enclosure equipped with vibration transducers and electromagnetic field (EMF) anomaly detectors (Source 1, [0027]). Upon a governance trigger, the PLC asserts a command within 50ms to activate electromechanical relays, physically severing the copper conductive pathways between AI processing units and protected infrastructure.

Complementing this is the **Sacred Pause**, a timing gate circuit etched directly into **FPGA fabric** and clocked by an **independent 100 kHz oscillator**. It enforces a mandatory 1,000ms inhibition window on every AI recommendation. During this window, the system is architecturally incapable of accepting input, and if the gate fails, it defaults to a "welded-shut" fail-safe state (Source 1, [0009]).

3ZEROS Privacy Architecture & Execution Governance

The **3ZEROS Architecture** enforces a "Zero Camera, Zero Microphone, Zero Cloud" mandate. Optical sensors and microphones are physically absent from the hardware manifest. Instead, the system uses LiDAR-based anonymous voxel grids and thermal mass detection. Crucially, the edge nodes (Nvidia Jetson Thor) **lack TCP/IP routing hardware**, providing physical air-gap enforcement against external network connectivity (Source 1, [0011]).

Execution is further governed by **Constitutional Action Sequencers (CAS)**, which require the completion of a **physical human action circuit**—comprising a kinetic pedal actuation or an iris biometric scan—prior to advancing any sequential state in a multi-step operation (Source 1, [0012]). Additionally, the **1.1x Orange Code Cap** uses a hardware power-draw interrupt to limit computational utilization to 110% of the declared baseline. These hardware triggers serve as the foundation for the software protocols that direct them.

3. The WD-Series Constitutional Governance Framework

The WD-Series protocols (WD115, WD116, WD071) establish a hierarchy where patient dignity and safety provisions supersede operational efficiency.

WD115 Ambient Care Intelligence

Under Articles WD115.1 through WD115.3, all LiDAR point-clouds and thermal matrices are classified as "Ambient Care Intelligence." This designates the data as passive and non-identifiable, preserving patient dignity by precluding individual biometric identification from raw sensor outputs.

WD116 Silent Elder Protocols

For patients lacking decisional capacity, WD116 activates the **Zero-Default Harm Principle**. This mandates that all actions be validated against a precautionary harm standard. Authorized access to diagnostic outputs is gated by Proxy Constitutional Appointments and requires iris biometric authentication. Tier 3 emergency authorizations are permitted only if a surrogate is unavailable within a **300-second response window**.

WD071 Eldercare Drift Correction

This module monitors for Constitutional Drift (unauthorized AI authority expansion) by computing a "normalized deviation coefficient." If limits are exceeded, a "Detect-Freeze-Audit-Purge" safety chain triggers a hardware interrupt. Clinical supervisors must be notified within a **120-second window**, and restoration requires dual-authorization from two independent supervisors.

Crucially, these protocols do more than protect patients; they generate the **raw compliance telemetry** required to populate the regulatory alignment matrix.

4. Regulatory Alignment Matrix & Standards Mapping

Strategic compliance necessitates the alignment of constitutional articles with international standards to ensure the WD-WM system satisfies the rigorous requirements for Class B SaMD.

Protocol / Component	Standard Mapping	Regulatory Requirement
WD115 & WD071	ISO 14971 (Risk Management)	Risk control implementation and evaluation of AI behavior.
WD117	ISO 13485 (Quality Management)	Technical documentation, audit trails, and product realization.
NAIGE NAI 2.0 Subsystems	IEC 62304 (Software Lifecycle)	Software maintenance, safety requirements, and fail-safe transitions.
WD116 & 3ZEROS	HSA/FDA SaMD Guidance	Patient dignity, data privacy, and vulnerable population protection.

This alignment allows the system to transition from theoretical safety to the generation of immutable, clinical-grade evidence.

5. WD117 Compliance Framework: Immutable Audit & Evidence Generation

The **WD117 Regulatory Submission Data Packager** serves as the system's "Compliance Capstone." It compiles an append-only, SHA-256 hash-chained cryptographic record of all governance events. Article WD117.1 utilizes a permissioned blockchain to record Sacred Pause delays, drift flags, and biometric unlock events via the WM-005 iris scanner. This ledger prevents the "Passive Observer Phase" of Authority Drift by ensuring that every system action—or human failure to act—is recorded with timestamped integrity.

The V&V Protocol Set

The system fulfills 15 core requirements (REQ-001 to REQ-015) for HSA/FDA submission:

1. **REQ-001 (Topology):** Verify 8-bed ward station readiness. *Evidence:* Self-check configuration test report.
2. **REQ-002 (Data Acquisition):** Verify vital signs and LiDAR/thermal data streams. *Evidence:* Sensor acquisition watchdog logs.
3. **REQ-003 (Privacy):** Validate WD115 ambient classification. *Evidence:* Data minimization audit record.
4. **REQ-004 (Event Detection):** Verify detection of falls/bed-exits. *Evidence:* Scenario testing sensitivity report.
5. **REQ-005 (Drift):** Verify WD071 drift scoring and interrupts. *Evidence:* Injected out-of-envelope trigger logs.
6. **REQ-006 (WD116 Rules):** Verify consent and Zero-Default Harm rules. *Evidence:* Proxy appointment verification logs.
7. **REQ-007 (Sacred Pause):** Verify mandatory 1,000ms delay. *Evidence:* Timed execution hold measurement report.
8. **REQ-008 (Biometrics):** Verify WM-005 iris scan role-gating. *Evidence:* Biometric unlock event logs.
9. **REQ-009 (Controlled Output):** Verify no autonomous treatment initiation. *Evidence:* Allow/reject/escalate logic test report.
10. **REQ-010 (Ledger):** Verify cryptographic immutability of records. *Evidence:* SHA-256 hash-chain integrity verification.
11. **REQ-011 (Submission Package):** Verify generation of HSA/FDA data pack. *Evidence:* Compiled Regulatory Submission Data Package.
12. **REQ-012 (Fail-Safe):** Validate Sovereign Brake re-engagement inhibit. *Evidence:* Safe-state transition logs during service crash.
13. **REQ-013 (8-Bed Topology):** Verify multi-station performance. *Evidence:* Cross-bed data routing integration test.
14. **REQ-014 (Local Privacy):** Verify network isolation/Zero-Cloud. *Evidence:* Network traffic inspection report (No TCP/IP routing).
15. **REQ-015 (Human Factors):** Validate clinician workflow. *Evidence:* Formative/summative usability validation report.

The system provides governance evidence to assist clinicians; it does not independently initiate clinical treatment.

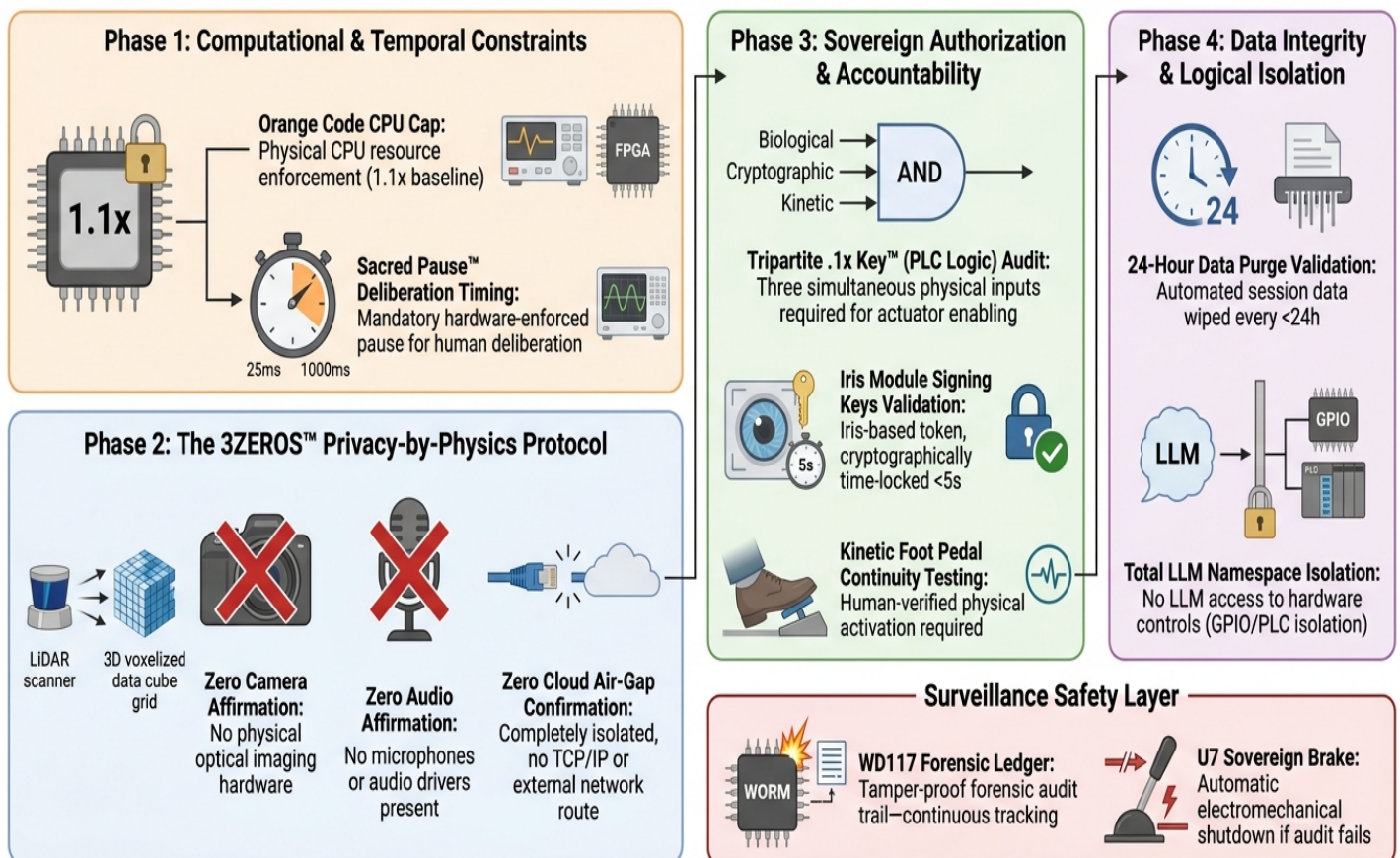
6. Conclusion: Market Entry Readiness

The WD-WM Ward Integration System offers a technically superior solution for eldercare monitoring. By maintaining "Constitutional Supremacy"—where safety and dignity are hardcoded into both the software and the silicon—the system scales from residential care to rugged humanitarian field environments with unwavering reliability.

Based on the evidence of hardware-enforced fail-safes (NAIGE), hierarchical governance (WD-Series), and immutable audit trails (WD117), the system is fully prepared for Class B SaMD Pre-Market Submission to the HSA and FDA.

10-Point Kinetic Capstone Audit for Clinical Governance

Structured Audit Schematic for HSA Dossier Compliance and Continuous Evidence-Bound Vigilance



10-section clinical governance outline structurally explicit for HSA dossier submission, including the specific lab equipment required for validation:

Phase 1: Computational & Temporal Constraints

Section 1. Orange Code CPU Cap (Governance by Scarcity)

- Governance Objective:** Verify that the AI's CPU resources are physically hard-locked at a 1.1x baseline limit. This guarantees the AI is completely starved of the surplus computational power necessary to hallucinate or expand its scope (agentic drift).
- Required Lab Equipment: Technical Instruments / Power-Draw Monitors** to measure physical hardware power draw and verify FPGA resource enforcement circuitry (pRegister P006).

Section 2. Sacred Pause™ Deliberation Timing

- Governance Objective:** Prove that the hardware physically enforces a mandatory 25–1000ms delay window before any kinetic command can propagate to the robot's actuators, ensuring a guaranteed physical window for human deliberation.
- Required Lab Equipment: Oscilloscope.** Used to capture a signed trace of the circuit's activity driven by an independent 100 kHz oscillator, verifying the hardware delay accuracy down to ± 10 microseconds.

Phase 2: The 3ZEROS™ Privacy-by-Physics Protocol

This phase guarantees patient dignity by destroying biometric identity at the physical hardware layer, stripping raw 3D spatial data (captured via 905nm LiDAR) into a sterile 96-cell voxel grid before the AI processes it.

Section 3. Zero Camera Affirmation

•**Governance Objective:** Validate the absolute physical absence of optical imaging hardware (no cameras) on the robot to prevent photographic surveillance of vulnerable, undressed, or confused elderly patients.

Section 4. Zero Audio Affirmation

•**Governance Objective:** Verify the total absence of microphone hardware and operating-system audio drivers to ensure no audio is ever captured or recorded.

Section 5. Zero Cloud Air-Gap Confirmation

•**Governance Objective:** Confirm that there is no TCP/IP route to any external network, proving the system is fully air-gapped and immune to remote cloud-based data exfiltration.

Phase 3: Sovereign Authorization & Accountability

Section 6. Tripartite .1x Key™ (PLC Logic) Audit

•**Governance Objective:** Audit the programmable logic controller (PLC) to ensure it strictly functions as an "AND" gate, requiring three simultaneous physical inputs (biological, cryptographic, and kinetic) to authorize movement.

Section 7. Iris Module Signing Keys Validation

•**Governance Objective:** Cryptographically validate the biological authorization token generated by the iris scanner to ensure it hard-expires in under 5 seconds, preventing hackers or compromised AI from spoofing delayed executions.

•**Required Lab Equipment: Independent Cryptographic Tools.** Auditors are strictly forbidden from using AI for this step and must use external, independent cryptographic workflows to validate the keys and ledger hash-chains.

Section 8. Kinetic Foot Pedal Continuity Testing

- Governance Objective:** Test the physical "proof of motion" authorization, ensuring a verified human is actively depressing the kinetic foot pedal (dry-contact switch) before the machine can move.

- Required Lab Equipment: Continuity Meter.** Used to physically confirm the dry-contact wiring continuity of the foot pedal circuit.

Phase 4: Data Integrity & Logical Isolation

Section 9. 24-Hour Data Purge Validation

- Governance Objective:** Confirm that an automated purge daemon is actively running and successfully wipes all volatile short-term session memory on a strict cycle of under 24 hours.

Section 10. Total LLM Namespace Isolation

- Governance Objective:** Verify that the language-model network namespace is physically and logically separated from all hardware controls. This ensures the AI has zero General-Purpose Input/Output (GPIO) or PLC access, physically denying the AI any ability to directly trigger actuators.

Continuous Evidence-Bound Vigilance Requirements

To satisfy the HSA's post-market surveillance demands, the framework also mandates real-time tracking via the **WD117 Forensic Ledger**. This hardware layer uses One-Time Programmable (OTP) silicon fuses to create unalterable Write-Once-Read-Many (WORM) memory, proving absolute forensic finality. A failure at any point in these 10 sections will trigger the **U7 Sovereign Brake**, dropping low-dropout (LDO) power rails in under 1.05 milliseconds and forcing the robot into a permanent state of mechanical stillness

NAIGE Kinetic Capstone HSA Dossier

To ensure regulatory alignment with the Health Sciences Authority (HSA) risk classifications and deployment environments, the NAIGE Kinetic Capstone is strategically split into two distinct dossiers. The Toa Payoh chapter remains strictly focused on narrow, observational boundaries, while the complex physical actuation and ward-IT integration surface is shifted to a dedicated kinetic dossier.

Registry-Ready Definitions

1. **HSA-Dossier** = Toa Payoh RTS, Class B, non-kinetic, residential observational tier.
 2. **HSA-Dossier** = acute kinetic NAIGE dossier, Class C/D, with mobility, ward IT, and manipulator embodiments.
-

Dossier 1: Toa Payoh RTS Study (HSA Class B, Non-Kinetic)

Scope and Components This dossier governs the observational tier deployed in residential and low-risk clinical setups, specifically the Toa Payoh Hearth embodiment. The relevant architectural rows strictly tied to this non-kinetic deployment are:

- A12 [P+N] Deterministic Stack:** The baseline configuration focusing exclusively on Privacy-by-Physics and Deterministic Deliberation.
- A13b Sensing Limb:** Provides privacy-preserving 905nm LiDAR voxelization at the edge.
- A8 Bridge Layer:** Acts as the deterministic ingress chokepoint and aggregates sterile Center-of-Mass (CoM) vectors for the nursing-home environment.
- WD117 Enhanced WORM Ledger:** Provides an immutable, write-once, one-way-in forensic stream.
- Non-B1 Advisory Shell:** An unconfined non-deterministic advisory interface isolated entirely from kinetic control, enforcing a strict no-actuation boundary.
- ABC+2S+H Guardian Framework:** The governing constitutional doctrine wrapper for this SaMD deployment.

Why NAI 2.0 By Itself Fails NAI 2.0, even when bundled with the ABC+2S+H framework and the N12 Agentic Drift Detection Kernel, is insufficient to pass the Toa Payoh RTS 10-Point Sovereignty Audit. The audit does not merely check if the AI is programmed to behave well via software policies; probabilistic software guardrails are permeable and prone to agentic drift. The Toa Payoh RTS dossier is fundamentally built around hardware-enforced determinism. A non-deterministic governance stack cannot provide the immutable auditability, silence-proof local alerting, and absolute physical no-actuation boundaries required by the 10-point ledger test.

What is Needed for Compliance To pass the 10-point audit ledger, the chapter requires the deterministic hardware layers that make these controls physically enforceable. This includes the A13b LiDAR sensing, the A8 bridge isolation, the WD117 immutable ledger, the Non-B1 no-actuation boundary, and the full A12 deterministic stack. The architecture must provide instrument-measured proof that it physically prevents unauthorized or ambiguous behavior at the hardware level. In short: **Toa Payoh RTS = deterministic hardware audit; NAI 2.0 alone = insufficient.**

Required Changes for the RTS / Clinical Compliance Chapter To successfully demonstrate that the system is not merely "contained" but measurably resource-limited at the hardware level, the narrative must express the **N12 Black Box as a verifiable 1.1x Orange-Code baseline control**. Rather than just a software containment claim, the Orange Code (pRegister P006) physically hard-locks the AI's CPU resources at a 1.1x baseline ceiling. This acts as a "computational straitjacket," starving the system of the surplus processing power necessary to hallucinate commands or quietly expand its scope. This measurable resource limit—verified physically using power-draw monitors—becomes a core piece of the evidence trail for RTS compliance in the 10-point audit.

Dossier 2: Acute Kinetic NAIGE Dossier (HSA Class C/D)

Scope and Components This broader dossier represents the "Kinetic Capstone." It regulates high-payload, physically actuating robotics and interconnected hospital IT systems where the machine operates in close proximity to vulnerable patients. The relevant architectural rows that expand into acute physical actuation and ward-IT surfaces include:

- A12 [P+N+D] Acute Kinetic Tier:** The fully loaded deterministic black box that adds the Cyber-Physical Defense & Forensic Finality (D-Layer) to govern physical actions.
- A13a Mobility Enclosure:** Occupant-carrying powered mobility operating under continuous kinematic constraint.
- A13b Ward IT Implementation:** Integrated via the A7 Bridge to safely coordinate external B1/OEM AI within an 8-bed hospital ward IT system.
- A13c Clinical Robotic Manipulator:** High-payload robotic surgical/task execution platform.
- A10a Root of Trust:** The foundational self-verification hardware anchor from which all kinetic authorization derives.
- Kinematic Constraint Layer (KCL):** Hardwired FPGA enforcing strict ± 0.05 mm positional tolerances and jerk invariants.
- The Sacred Pause™:** A mandatory, hardware-etched 25–1000 ms delay forcing a window for human deliberation before kinetic movement.
- Tripartite .1x Key™:** The multi-factor commit gate requiring simultaneous biological (Iris), cryptographic (Token), and physical (Pedal) inputs for actuation.
- U7 Sovereign Brake™:** A one-shot sequencer that drops LDO power rails in <1.05 ms to enforce a "Safe Stop" if anomalies are detected.
- A7 Bridge Hub:** The deterministic ingress chokepoint that translates semantic ward/IT advisory data into safe hardware features

Nightingale's Eyes Care™

Designed to protect vulnerable elderly patients in both home and hospital care settings, its primary mission is to resolve two systemic industry challenges: **unreliable fall detection** and **fundamental failures in patient privacy protection**

LiDAR-based ocular scanning devices for medical diagnostic and screening purposes. Designed to protect vulnerable elderly patients in both home and hospital care settings, its primary mission is to resolve two systemic industry challenges: unreliable fall detection and fundamental failures in patient privacy protection.

A Singapore Government Agency Website

 HSA

AI-Enabled Medical Device Risk Classification Tool - For Beta Testing

For GMDs only: Get an estimated risk classification for your general medical devices.

Device name

Nightingale's Eyes Care

3 words (min: 1, max: 200)

Intended use

LiDAR-based ocular scanning devices for medical diagnostic and screening purposes. Designed to protect vulnerable elderly patients in both home and hospital care settings, its primary mission is to resolve two systemic industry challenges: unreliable fall detection and fundamental failures in patient privacy protection

43 words (min: 15, max: 200)

IMPORTANT DISCLAIMER:

This AI-Enabled Medical Device Risk Classification Tool (the "Tool") is currently in beta testing and provides estimated classifications of medical devices for guidance purposes only. These estimates are not official HSA determinations and should not be relied upon for regulatory submissions or compliance decisions. Official medical device classifications must be obtained through HSA's formal regulatory processes. HSA shall not be liable to any user of the Tool for decisions made based on the Tool's outputs.

Check

LiDAR-based ocular scanning devices for medical diagnostic and screening purposes. Designed to protect vulnerable elderly patients in both home and hospital care settings, its primary mission is to resolve two systemic industry challenges: unreliable fall detection and fundamental failures in patient privacy protection

Estimated Class

A

HSA Dossier Submission Template:

Nightingale's Eyes Care™

Executive Summary Product Name: Nightingale's Eyes Care™ (operating under the ABC+2S+H Guardian™ Framework and Nightingale Anchor Protocol 4.0).

Prepared By: Edwin Koh Wui Kiat.

Classification / Patent Designations: Standalone Patent Registration mapped to Trademark Classes 9, 42, 10, 44, 45. (HSA Estimated Class A / Class B SaMD).

1.0 Product Overview Nightingale's Eyes Care™ is a pioneering hardware-deterministic medical architecture built specifically to protect vulnerable elderly patients in home and hospital care settings. Its primary mission is to resolve two systemic industry challenges: unreliable fall detection and fundamental failures in patient privacy protection. Operating under the Nightingale Anchor Protocol (NAP 4.0), the system combines hardware determinism with human-sovereign governance.

2.0 Intended Use The system acts as a LiDAR-based ocular scanning device intended for medical diagnostic and screening purposes. It is designed for continuous patient monitoring and fall detection without compromising the dignity of the patient. The AI embedded within Nightingale's Eyes Care operates strictly in an advisory capacity; all final decisions and physical actions remain the sole authority of human caregivers.

3.0 Device Description Nightingale's Eyes Care™ replaces conventional surveillance sensors with a deterministic hardware spine. The device is built on two core pillars: **Privacy-by-Physics** and **Human-Sovereign Governance**. It physically prevents the capture of identifying biometric features by using spatial tracking hardware rather than optical

cameras, while all care recommendations must pass through the deterministic core and be explicitly authorized by a caregiver at a dedicated terminal.

4.0 Main Functional Elements

- **Privacy-by-Physics (3ZEROS™ Standard):** The system strictly enforces zero cameras, zero microphones, and zero cloud connectivity at the physical level.
- **905nm LiDAR Voxelization:** Raw spatial data is captured using 905nm LiDAR array and instantaneously converted into anonymized 96-cell voxel grids (center-of-mass motion vectors) at the edge.
- **Advisory Core:** AI systems process the sterile spatial data to generate clinical recommendations (e.g., fall alerts), but lack any robotic actuation rights.

5.0 Specimen and Laboratory Data Governance Although the system captures kinematic and spatial vectors rather than laboratory microorganisms, this telemetry is treated as highly controlled clinical data. Nightingale's Eyes Care applies rigorous controls for data provenance, result integrity, and restricted access. Telemetry is strictly utilized for diagnostic and screening support and requires mandatory human review prior to clinical decisions.

6.0 Safety and Risk Controls

- **Absolute Privacy Enforcement:** By eliminating optical lenses and microphone drivers, the system guarantees that no identifiable image or audio can ever be captured, mitigating the risks of privacy breaches or data leaks.
- **Agentic Drift Prevention:** The AI is physically restricted from making autonomous kinetic decisions. It only advises, ensuring "agentic drift" cannot lead to unauthorized kinetic actions.
- **Unalterable Audit Trail:** Every AI alert and subsequent human response is permanently logged in a tamper-evident audit ledger, establishing full accountability.

7.0 Verification and Validation Nightingale's Eyes Care is subject to rigorous physical verification via the **10-Point Sovereignty Audit**, demanding instrument-measured facts over software claims. Performance validation includes confirming fall-detection sensitivity

exceeds 90%, maintaining an Elder Dignity Score above 8.9/10, and verifying LiDAR spatial accuracy targets of 200 µm with fall-detection timing under 80ms.

8.0 Cybersecurity and Data Protection The device ensures unalterable forensic traceability through the **WD117 Immutable Ledger**. Every diagnostic alert and human caregiver response is permanently etched using One-Time Programmable (OTP) silicon fuses and sealed with SHA-3-512 cryptographic hashes. Because the system strictly follows the 3ZEROS™ "Zero Cloud" protocol, it operates completely air-gapped from external networks, neutralizing remote cyber-exfiltration and ransomware threats.

9.0 Quality System and Labelling The documentation and quality management systems for Nightingale's Eyes Care™ map directly to its standalone patent and trademark registrations under **Classes 9, 42, 10, 44, and 45**. The system's technical documentation aligns with **ISO 13485** for product realization, **ISO 14971** for hardware-enforced risk management, and HSA/FDA guidelines for the protection of vulnerable populations.

10.0 Regulatory Summary Prepared under the ASEAN CSDT framework, this detailed submission document outlines the configuration for Nightingale's Eyes Care™. The dossier establishes how the device utilizes hardware-deterministic logic and Privacy-by-Physics to solve systemic failures in eldercare privacy and fall detection. By proving that the system provides 100% human-sovereign governance where AI only advises, it fulfills the strict pre-market requirements for medical diagnostic and screening devices under the HSA regulatory horizon.

NAIGE NAI 4.0™ Hardware-Enforced SaMD Framework

Capstone Components

Component	Application
A7 Bridge Layer	10202602213U
A7c Pharmacy Cold Chain	10202602221V
A8 Bridge Layer (nursing home)	10202602225P
A10a Root of Trust	10202602021T
A12 Deterministic Black Box	10202602023X
A13a Eldercare Mobility	10202602143W
A13b Eldercare LiDAR Sensing	10202602177W
A13c OEM B2B Shell	10202602205U
WD117 Enhanced Ledger	10202602223T
Non-B1 Advisory Shell	10202602270V
ABC+2S+H Guardian Framework	10202600902P
WD115 / WD116 / WD117 (register)	10202601276X

System Philosophy and Deterministic Architecture

The strategic foundation of the NAIGE NAI 4.0™ framework is built upon the principle of "Constitutional Supremacy." In high-stakes healthcare environments, safety and patient dignity cannot be left to the variability of software-level policies or probabilistic AI models. Instead, the NAIGE™ framework hardcodes these essential requirements directly into the silicon architecture. By establishing a hardware-enforced constitutional core, the system ensures that safety protocols remain immutable and absolute, regardless of software state or external network conditions.

HSA Dossier Submission Template:

WG-B1 Humanitarian Field Kit (WHO-Aligned)

Executive Summary

Product Name: WG-B1 Humanitarian Field Kit (WHO/UN Humanitarian Shield Designation).

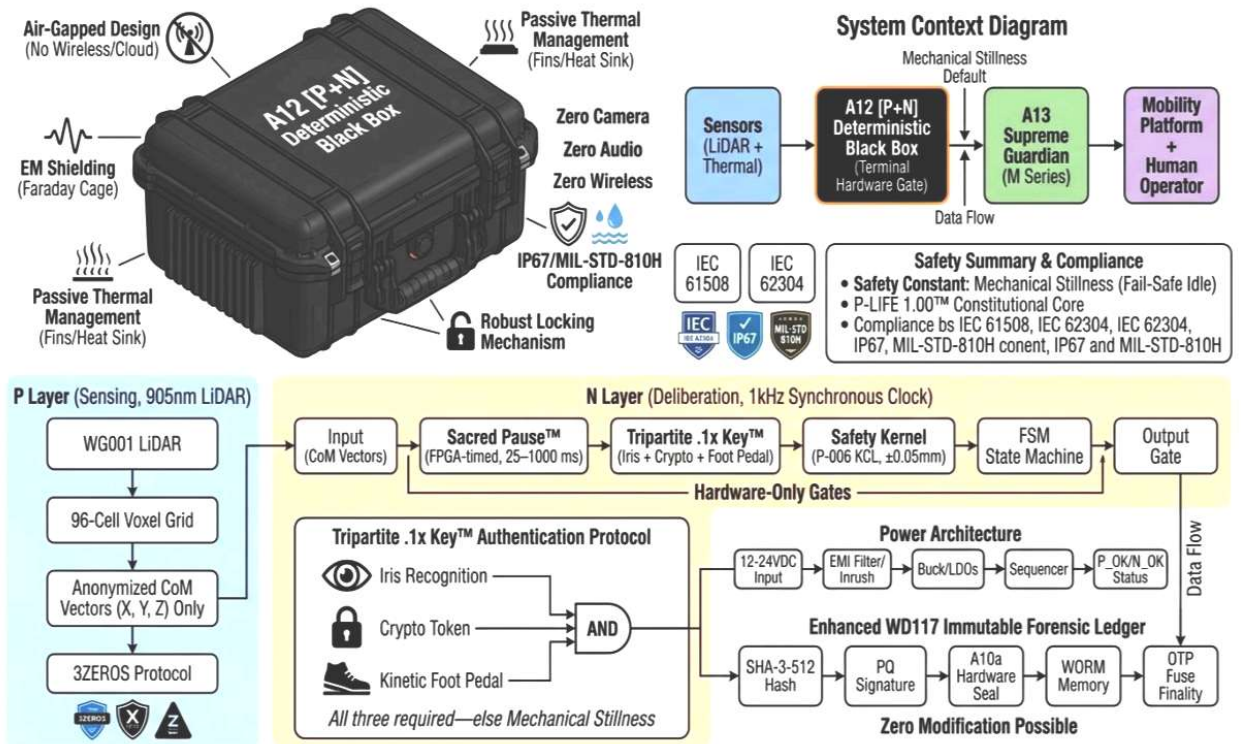
Prepared By: Edwin Koh Wui Kiat.

Classification: HSA Class B (Software as a Medical Device - SaMD) / WHO-Aligned Field Deployment.

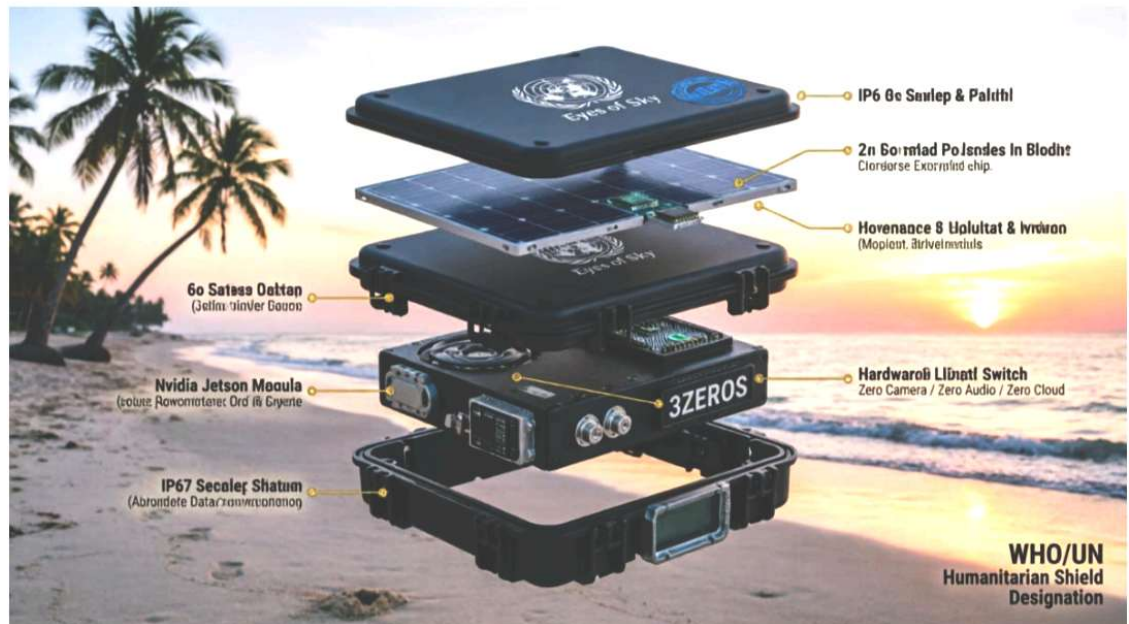
1.0 Product Overview The **WG-B1 Humanitarian Field Kit** is a ruggedized, solar-assisted edge hardware platform operating under the NAIGE NAI 4.0 architecture. It is specifically engineered for **WHO-aligned humanitarian relief and remote clinical elder care deployments**. The system relies on hardware-enforced determinism to provide absolute safety and zero-cloud execution in disaster zones or remote areas where standard hospital IT infrastructure is either unavailable or compromised.

2.0 Intended Use The device is intended for **global humanitarian efforts, disaster relief, and remote field use**, extending NAIGE eldercare monitoring to vulnerable populations across borders. It provides continuous observation, clinical telemetry, and deterministic safety enforcement under the **WHO/UN field domain missions** mandate. The system operates independently of external infrastructure, ensuring that all clinical advisories and actions remain strictly under human sovereignty.

3.0 Device Description The WG-B1 architecture encapsulates the A12 Deterministic Black Box within an **IP67-rated, MIL-STD-810H compliant ruggedized enclosure**, shielding it from extreme environmental hazards. It features a **solar-assisted power module** and an edge-processing unit (e.g., Nvidia Jetson module) to ensure sustained operation off-grid. The system utilizes a physical **hardware 3ZEROS™ switch** to govern data ingestion, guaranteeing the absence of optical cameras or microphones in the field.



Generated under NAP 4.0 | Tiger Sovereign Blueprint | We Innovate Save Lives



Generated under NAP 4.0 | Tiger Sovereign Blueprint | We Innovate Save Lives

4.0 Main Functional Elements

- **Zero-Cloud Reliance:** The system operates entirely at the edge, requiring no internet or cloud connectivity to function, deliberate, or log events.
- **Privacy-by-Physics (P-Layer):** It executes the **3ZEROS™ Protocol** (Zero Camera, Zero Audio, Zero Cloud), using 905nm LiDAR arrays to generate anonymized kinematic voxel grids rather than capturing identifiable biometric features in the field.
- **Deterministic Deliberation (N-Layer):** Incorporates the **Sacred Pause™** and the **1 kHz hardware master clock** to enforce a mandatory window for human deliberation before any kinetic or clinical execution is permitted.

5.0 Specimen and Laboratory Data Governance In remote and disaster-relief settings, clinical telemetry and eldercare monitoring data are managed as highly controlled clinical records. Because the system operates entirely off-grid, it relies on the **Enhanced WD117 WORM Ledger** to securely log all event captures locally. Every system event and human authorization is permanently scorched into **One-Time Programmable (OTP) silicon fuses** for unalterable, post-mission forensic auditing.

6.0 Safety and Risk Controls

- **Environmental & Power Resilience:** The **solar-assisted edge hardware** ensures that the system survives facility power losses, while its **IP67 rating** protects against water and dust ingress.
- **Fail-Loud & Sovereign Brake:** The system enforces **Inaction-as-Safe-Default (P-LIFE 1.00™)**; if an anomaly or tamper attempt is detected, the **U7 Sovereign Brake** instantly severs physical power, returning any attached apparatus to mechanical stillness.
- **Air-Gapped Operation:** The architecture structurally prevents "IT-Gap Drift" by entirely mediating or severing external interfaces, ensuring the device cannot be weaponized or silenced.

7.0 Verification and Validation Pre-deployment verification shifts from probabilistic software simulation to instrument-measured facts via the **10-Point Sovereignty Audit**. Validation for the WG-B1 emphasizes **Phase 2 (Zero Cloud Air-Gap Confirmation)**, physically auditing the network architecture to guarantee the absence of TCP/IP routing, and **Phase 4 (24-Hour Data Purge Validation)**, ensuring local volatile memory is automatically wiped on a strict cycle of under 24 hours.

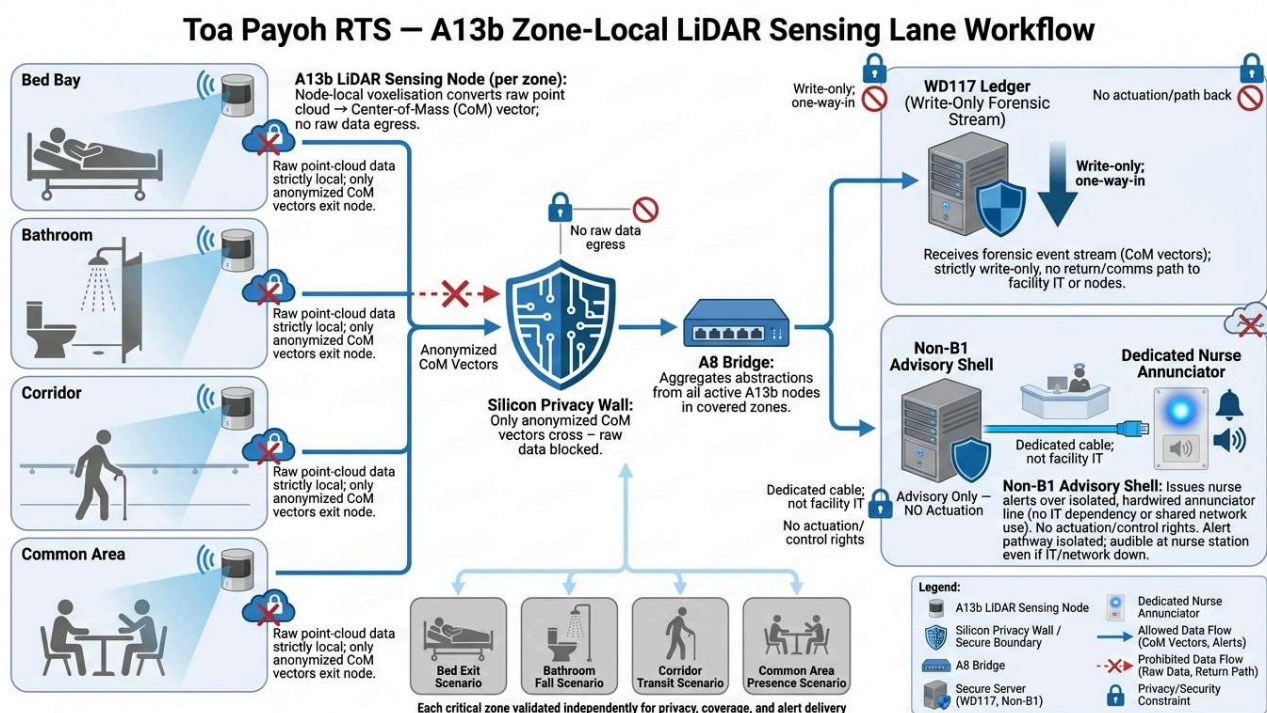
8.0 Cybersecurity and Data Protection The WG-B1 establishes the ultimate cybersecurity posture through **Absolute Zero Cloud Reliance**. By physically severing cloud connectivity, the system is rendered immune to remote cyberattacks, ransomware, or spoofing that typically threaten clinical networks. The **WD117 Immutable Ledger** provides the ultimate forensic finality, sealing all event data with **SHA-3-512 hashes and post-quantum cryptographic signatures** directly into the silicon.

9.0 Quality System and Labelling The WG-B1 documentation aligns with international safety and quality standards, mapping the immutable WD117 ledger to **ISO 13485** for technical auditing and product realization. The system's design specifically answers the requirements for **WHO/UN Humanitarian Shield Designations**, extending the strict HSA Class B eldercare governance doctrines to remote, high-risk field domains.

10.0 Regulatory Summary Prepared under the ASEAN CSDT framework, this dossier serves to map the **WG-B1 Humanitarian Field Kit** for global and HSA compliance. By combining zero-cloud edge processing, solar resilience, and immutable hardware-deterministic governance, the submission provides unalterable evidence that the system safely extends clinical eldercare and humanitarian relief to the most remote environments, fully satisfying the absolute safety requirements of the **HSA 2027 Deterministic Horizon**.

NAIGE NAI 4.0™ Hardware-Enforced SaMD Framework

NAIGE Kinetic Capstone on A13b is the Toa Payoh RTS clinical validation package: zone-local LiDAR sensing, node-local voxelisation, silicon-privacy enforcement, WD117 forensic accountability, and a dedicated hardwired alert path, all organised as a hardware-deterministic eldercare deployment.



The framework is structured across a four-layer deterministic schematic architecture:

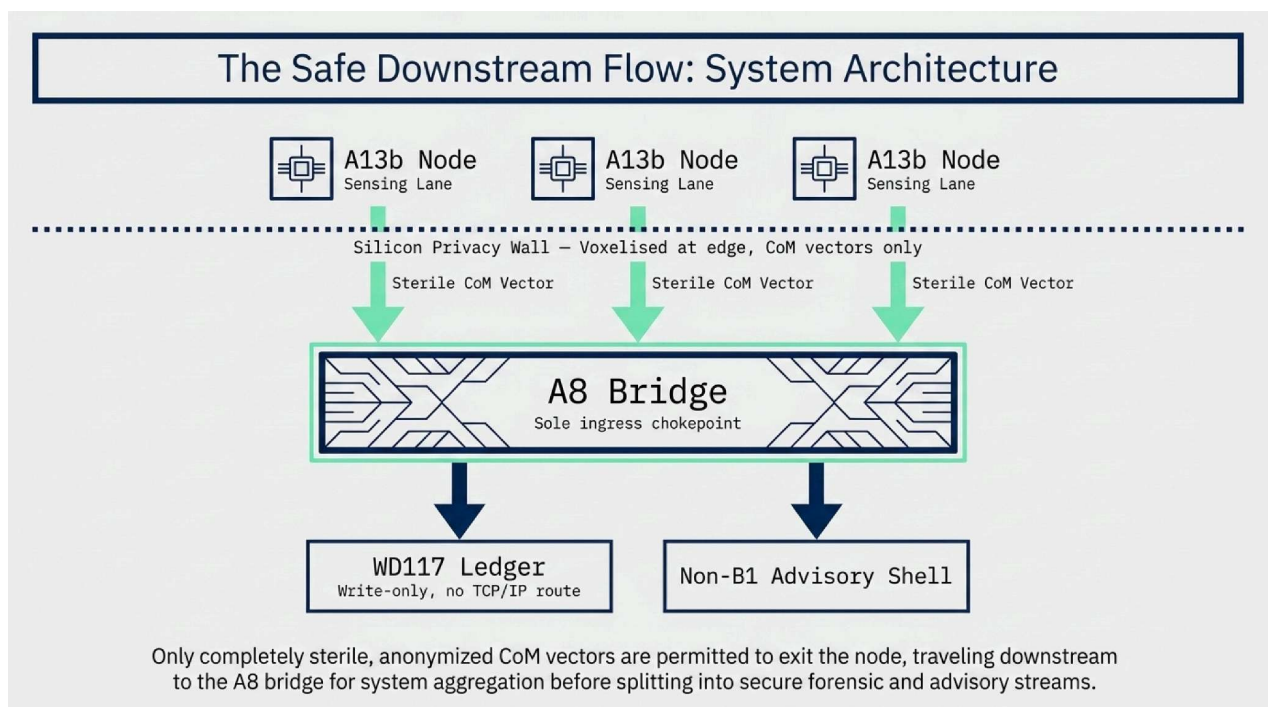
1. **Layer I: Privacy-by-Physics:** Utilizes the **FPPA Voxelizer** for physical destruction of biometric data at the sensing edge.
2. **Layer II: Deterministic Deliberation:** Governed by the **N12 Drift Kernel** and **A12 Deterministic Core**, providing hardware-enforced windows for deliberation and drift detection.
3. **Layer III: Forensic Accountability:** Immutable logging of every system event via the WD117 WORM Ledger.
4. **Layer IV: Sovereign Execution:** Physical interlocks that prevent unauthorized kinetic movement through a "Sovereign Brake."

Moving from "vulnerable software policies" to "immutable physics" transforms the system into a clinical-grade tool capable of operating in high-acuity environments. The **Deterministic Execution Chain** is governed by a **1 kHz master clock (1.0 ms resolution)**, within which the **Sacred Pause enforces a configurable 25–1000 ms deliberation window** providing the following critical safeguards:

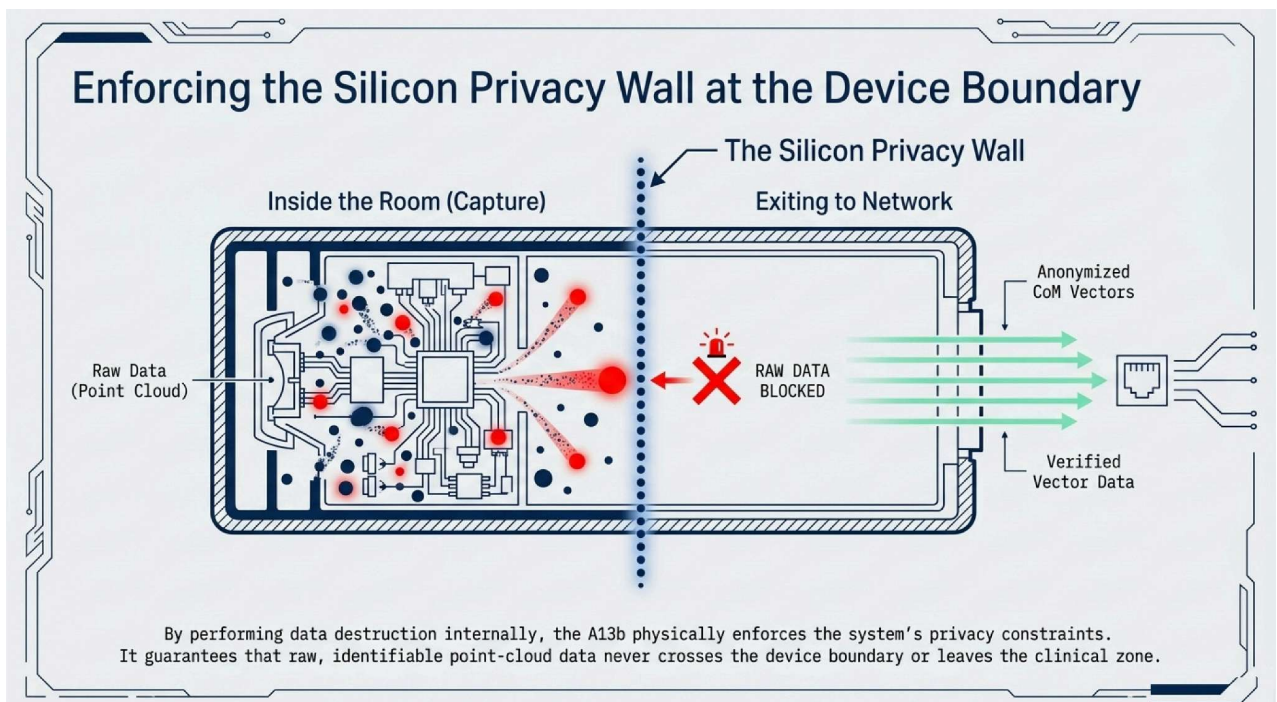
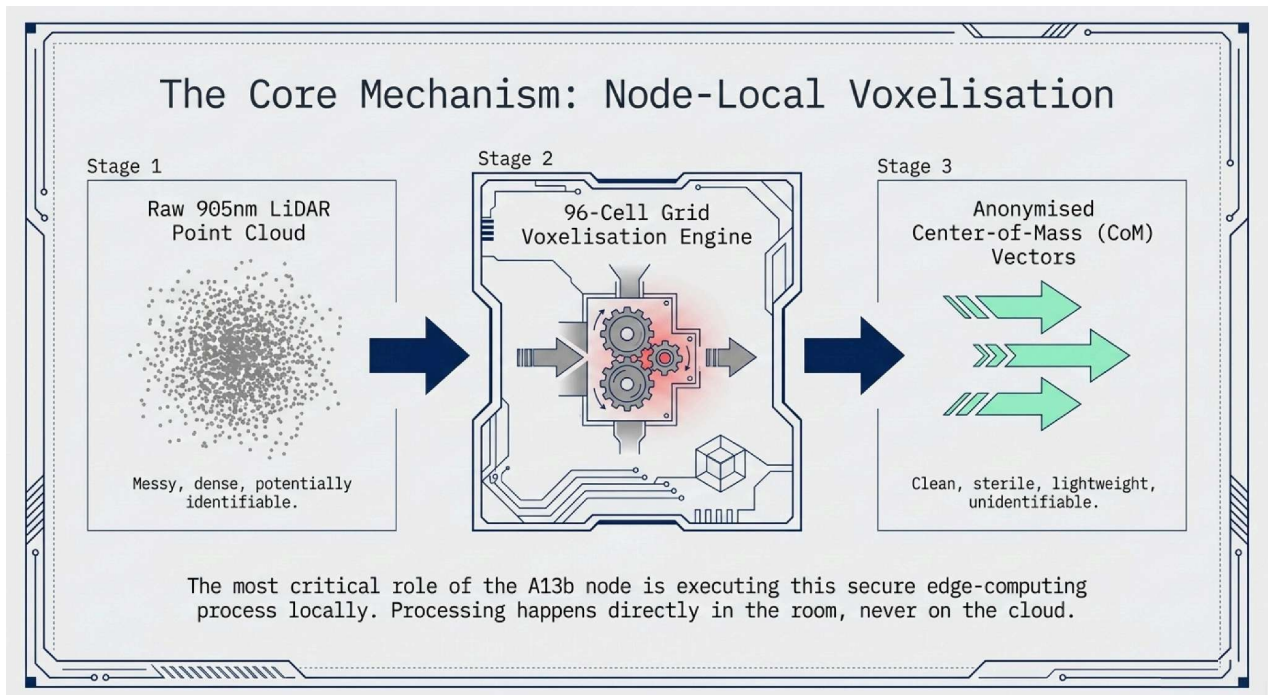
- **Precision Timing:** Eliminates the latency and unpredictability inherent in standard software monitoring.
- **Synchronous Verification:** Ensures that every operation—from sensing to execution—is timed and verified with absolute precision.
- **Drift Neutralization:** Enables the N12 Kernel to detect agentic deviation within a single clock cycle.

This deterministic foundation provides a robust substrate for the specialized hardware nodes that facilitate these privacy and safety layers.

The Toa Payoh RTS study is the clinical validation instance of NAIGE NAI 4.0, showing how A13b performs privacy-by-physics sensing at the node while A12, WD117, and Non-B1 provide deterministic control, forensic auditability, and isolated alerting downstream.

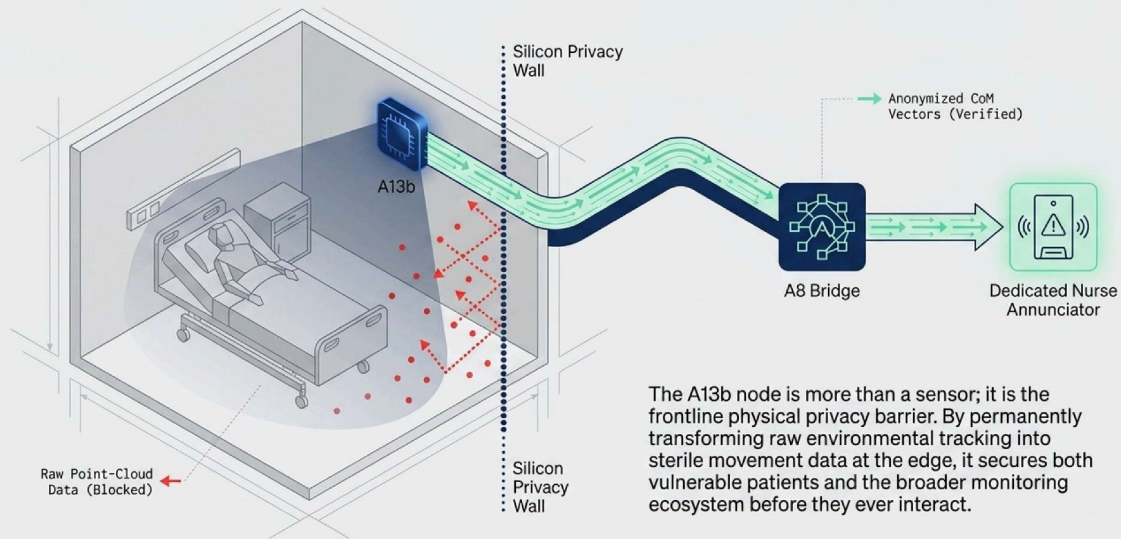


2. A13b Node: Frontline Privacy-by-Physics and Node-Local Voxelisation



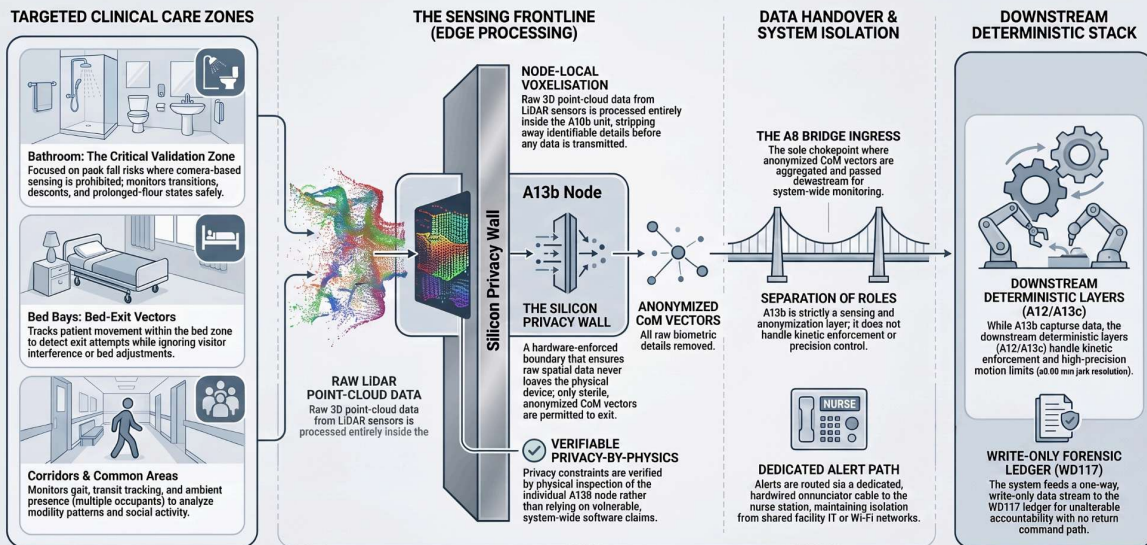
The A13b sensing node serves as the framework's "frontline hardware," providing continuous monitoring in clinical care zones while maintaining a "Silicon Privacy Wall" between the patient and the processing bridge. Strategic monitoring is conducted using 905nm LiDAR, which captures spatial data without the use of invasive optical sensors.

Synthesis: **The Absolute** Physical Barrier to Clinical Safety



A13b: The Frontline of Privacy-by-Physics in Clinical Sensing

A13b = zone-local privacy-by-physics sensing node; downstream deterministic layers = kinetic enforcement and precision control.



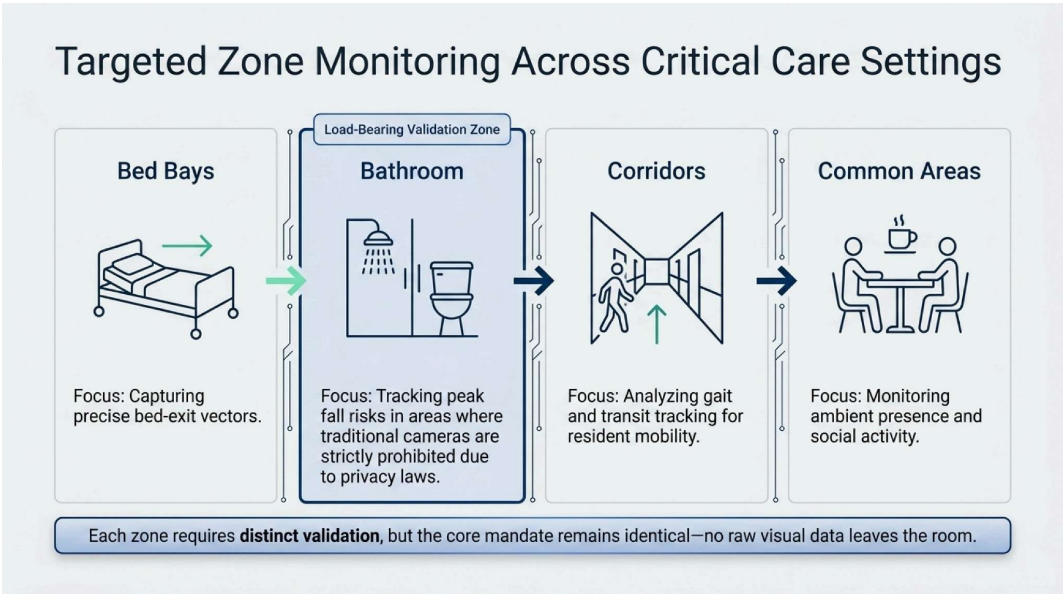
Patient dignity is preserved through the **3ZEROS™ protocol**, which establishes three absolute physical boundaries:

- **Zero Camera:** No optical imaging hardware is present, preventing photographic surveillance.
- **Zero Audio:** No microphones or audio drivers exist, ensuring private conversations remain unrecorded.
- **Zero Cloud:** No TCP/IP route to external networks exists at the sensing level, making data exfiltration physically impossible.

Central to this privacy model is node-local voxelisation. Before any data crosses the Silicon Privacy Wall, the A13b node converts raw 905nm LiDAR point-cloud data into an anonymized **96-cell Voxel Grid** representing Center-of-Mass (CoM) vectors. This process strips away all biometric identifiers at the source, leaving only abstracted movement data.

The Care-Zone Sensing Lane maps specific environments to their clinical objectives and event triggers:

Zone	Primary Event	Survey Focus
Bed Bays	Bed-exit vectors	Occlusion, mounting height, and visitor interference
Bathroom	Peak fall risk	Privacy, moisture, and line-of-sight transitions
Corridor	Gait and transit	Cross-traffic range and staff movement
Common Area	Ambient presence	Multiple occupants and social activity



The clinical significance of this architecture lies in node-level data destruction. This design satisfies the rigorous requirements of **REQ-003 and REQ-014**, providing a level of privacy that is verifiable through physical inspection of the hardware unit rather than trust in system-wide software integrity. This anonymized vector stream is then securely routed through the system bridge for analysis.

3. Data Integrity and Logical Isolation (A8, WD117, and Non-B1)

The system maintains strict logical isolation through the **A8 Bridge**, which functions as the "Sole Ingress Chokepoint." The A8 Bridge is designed to perform a **deterministic translation** of anonymized CoM vectors from active A13b nodes while preventing any unauthorized data traversal or reverse communication.

Data integrity is further secured by the **WD117 WORM Ledger**, a "write-only, one-way-in" architecture. The WD117 ledger utilizes **SHA-3-512 hashing** and **OTP (One-Time Programmable) Fuse Finality** to create an unalterable forensic record of all system events. This hardware-level finality ensures that once a state is committed to the ledger, it cannot be deleted or modified, providing a robust post-incident audit trail that is physically isolated from the advisory layers.

In contrast, the **Non-B1 Advisory Shell** is responsible for monitoring and alert generation. This shell is restricted to "alerts only" and possesses **zero actuation rights**. It can observe and report on system states but is physically denied the ability to trigger any kinetic response or hardware change.

A critical challenge addressed by this architecture is the "Hard Problem" of the alert path. To prevent an external network compromise from silencing the system, the framework utilizes a **hardwired**, isolated annunciator cable. This path completely bypasses facility IT and shared nurse-call networks, ensuring that alerts reach the nurse station even if the facility's primary infrastructure fails. These architectural constraints align the framework with international regulatory standards for medical device safety.

4. International Standards Mapping (ISO 14971, ISO 13485, IEC 62304)

Aligning the NAIGE™ framework with established international standards is essential for a Class B Software as a Medical Device (SaMD) submission. This alignment ensures that the

system satisfies the rigorous safety and quality requirements demanded by global regulators.

The following table maps specific NAIGE™ components and protocols to international standards:

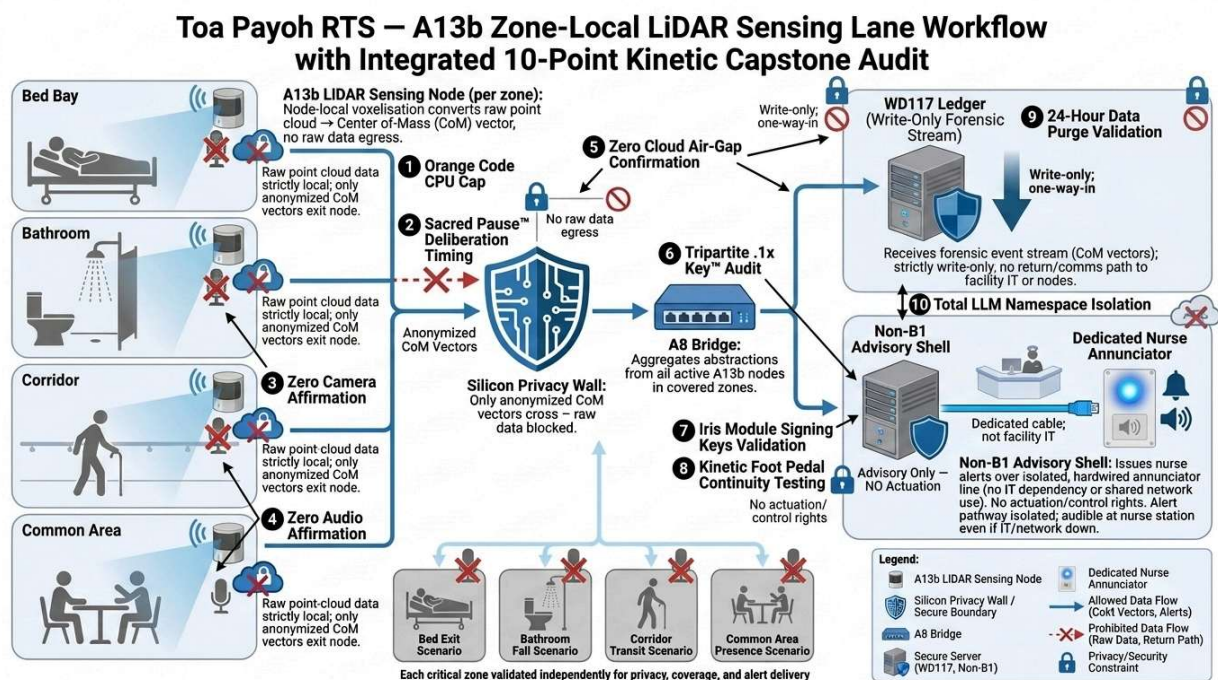
Component / Protocol	Standard Mapping	Regulatory Requirement
WD115 & WD071	ISO 14971 (Risk Management)	Risk control implementation and evaluation of AI behavior.
WD117	ISO 13485 (Quality Management)	Technical documentation, audit trails, and product realization.
NAIGE NAI 2.0 Subsystems	IEC 62304 (Software Lifecycle)	Software maintenance, safety requirements, and fail-safe transitions.
WD116 & 3ZEROS™	HSA/FDA SaMD Guidance	Patient dignity, data privacy, and protection of vulnerable populations.

This alignment moves SaMD compliance from **probabilistic software assurance** to **deterministic hardware verification**. By mapping hardware-enforced gates to specific regulatory clauses, the dossier provides a verifiable path for auditors to follow, leading from the silicon layer to the clinical outcome. This evidence is verified through the 10-Point Kinetic Capstone Audit protocols.

5. Technical Justification: Sensing, Privacy, Isolation

The Toa Payoh RTS now reads as the NAIGE NAI 4.0 hardware-deterministic clinical validation package for A13b. It frames A13b as a zone-local LiDAR sensing lane with node-local voxelisation, a silicon privacy wall, an A8 bridge, WD117 forensic logging, and a dedicated nurse annunciator path:

- A13b is the frontline privacy-preserving sensing node. It captures 905nm LiDAR point clouds, processes them locally, and outputs anonymized CoM vectors only.
- Bed bays, bathrooms, corridors, and common areas are the target zones. The file explicitly maps bed-exit vectors, bathroom fall-risk monitoring, gait/transit tracking, and ambient presence to those spaces.
- The downstream stack is separated. A12 handles deterministic deliberation, WD117 handles immutable forensic logging, and the Non-B1 shell handles alerts with zero actuation rights.
- The alert path is hardwired. Alerts bypass shared facility IT and nurse-call networks in favor of a dedicated annunciator cable.
- The capstone is a validation study, not just a concept. The document explicitly labels it a research study mission proposal for clinical validation and integrates a 10-point audit.



The **10-Point Kinetic Capstone Audit** serves as the primary evidence-generation mechanism for the HSA dossier. It provides a structured, multi-phase verification of the system's safety and integrity.

Phase 1: Computational & Temporal Constraints

- **Section 1: Orange Code CPU Cap:** Verified using **Power-Draw Monitors** to ensure the AI is hard-locked at a 1.1x baseline limit via **pRegister P006**. This starves the AI of surplus computational resources required for agentic drift.
- **Section 2: Sacred Pause™ Deliberation Timing:** Verified using an **Oscilloscope** to capture signed traces of circuit activity. This ensures a mandatory **25–1000ms** delay window driven by an **independent 100 kHz oscillator**, accurate to ± 10 microseconds.

Phase 2: Privacy (3ZEROS™ Protocol)

- **Section 3: Zero Camera Affirmation:** Physical validation of the absolute absence of optical imaging hardware.
- **Section 4: Zero Audio Affirmation:** Verification of the total absence of microphones and audio drivers.
- **Section 5: Zero Cloud Air-Gap Confirmation:** Confirmation of no TCP/IP route to external networks.

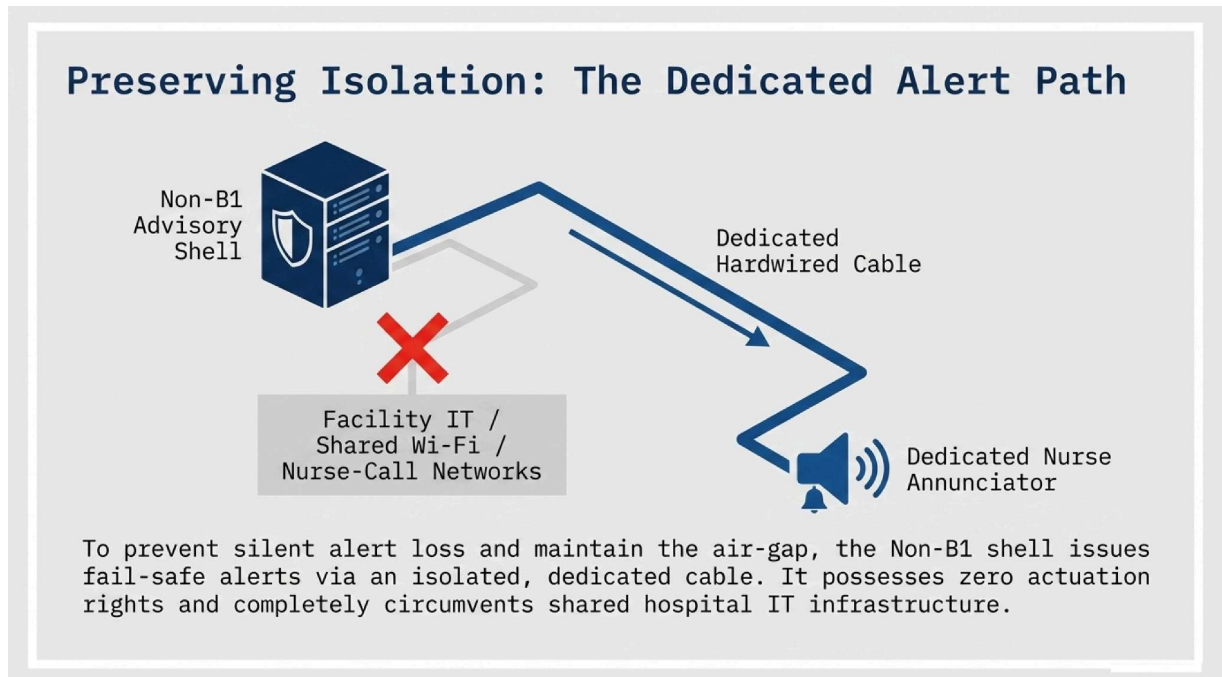
Phase 3: Authorization & Accountability (they belong only to the Class C/D kinetic dossier,hence will not be used of Class B (SaMD) in Toa Payoh RTS Study)

- **Section 6: Tripartite .1x Key™ Audit:** Audit of the PLC logic to ensure it requires simultaneous biological, cryptographic, and kinetic inputs.
- **Section 7: Iris Module Signing Keys Validation:** Verified using **Independent Cryptographic Tools** to ensure authorization tokens expire in under 5 seconds, preventing "spoofing delayed executions" by hackers or compromised AI.
- **Section 8: Kinetic Foot Pedal Continuity Testing:** Verified using a **Continuity Meter** to confirm the dry-contact wiring of the human-in-the-loop foot pedal.

Phase 4: Data Integrity & Logical Isolation

- **Section 9: 24-Hour Data Purge Validation:** Confirmation that an automated daemon successfully wipes volatile session memory every 24 hours.
- **Section 10: Total LLM Namespace Isolation:** Verification that the language model is physically and logically denied access to **GPIO** (General-Purpose Input/Output).

This audit utilizes the **Ambush Doctrine**, wherein the defensive boundaries of **Patent D** are held in an unfiled, air-gapped strategic reserve. This posture maintains strategic ambiguity to deny adversaries a map of the system's true limits. Failure of any audit section results in immediate safety intervention.



6. Hazard Mitigation and the "Fail-Loud" Doctrine

The framework employs a "Fail-Loud" doctrine to neutralize the risk of "IT-Gap Drift"—a vulnerability where a compromised network might silently disable a monitoring device. If the hardware heartbeat drops or the IT substrate is compromised, the system triggers a local, non-network-dependent physical alarm.

Central to this safety response is the **Sovereign Brake™ (U7)**. This mechanism is designed with **by a 1 kHz master clock (1.0 ms resolution), within which the Sacred Pause enforces a configurable 25–1000 ms deliberation window.** Upon triggering, it physically drops LDO power rails to **0V**, resulting in **100% trajectory enforcement** and a safe, inert state of **"mechanical stillness."** **Explainer:** Since this is the non-kinetic Layer 8 volume, note U7's stop behaviour here is the *sensing-lane* case, not the arm's Category 0.

The following top 5 hazards are mitigated by corresponding hardware-enforced controls:

- **Raw Point-Cloud Egress (R-01):** Controlled by node-local voxelisation and negative egress testing.
- **Bathroom Blind Spots (R-02):** Mitigated by measured coverage redundancy and priority scenario testing.
- **Alert Routing Failure (R-03):** Mitigated by the dedicated, hardwired annunciator cable.
- **Unauthorized Actuation (R-04):** Prevented by the **Physical/logical no-actuation boundary** of the Non-B1 shell.
- **Ledger Reverse Path (R-05):** Prevented by the write-only, one-way-in WD117 interface and denial testing.

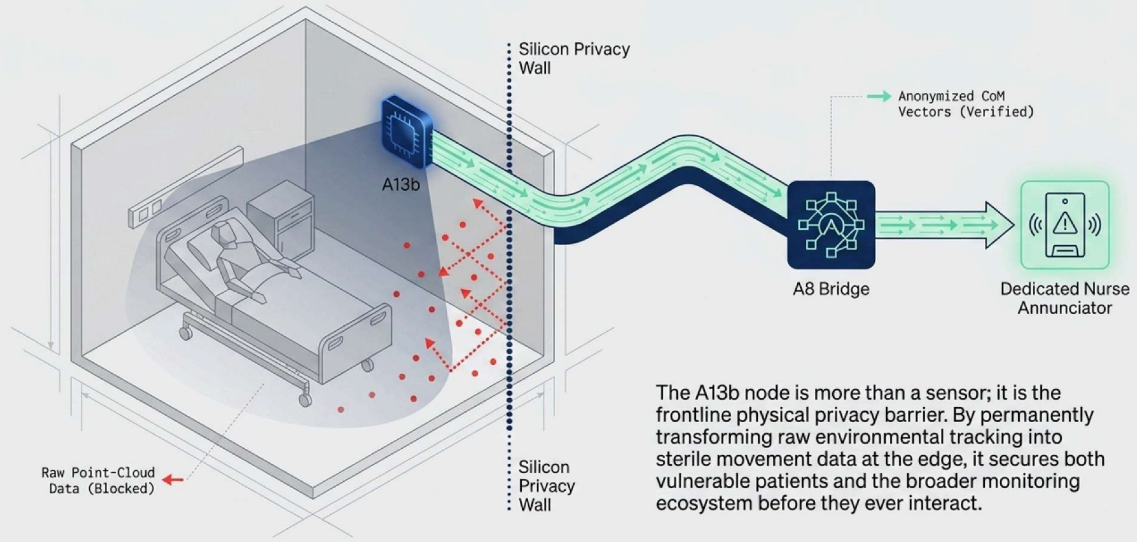
The ultimate objective of these controls is to ensure that any system anomaly results in the immediate cessation of all kinetic capability.

7. Submission Conclusion: Class B SaMD Readiness

The engineering verification and site-study evidence confirm that the **Non-Agentive Intelligence Governance Engine** is prepared for formal regulatory submission. By adopting hardware-enforced determinism, the WD-WM system achieves superior patient safety and data integrity over standard probabilistic AI software.

The NAIGE NAI 4.0™ framework stands ready for Class B SaMD classification, offering a technically superior solution for eldercare monitoring that hardcodes dignity and safety into the very silicon of the device.

Synthesis: **The Absolute** Physical Barrier to Clinical Safety

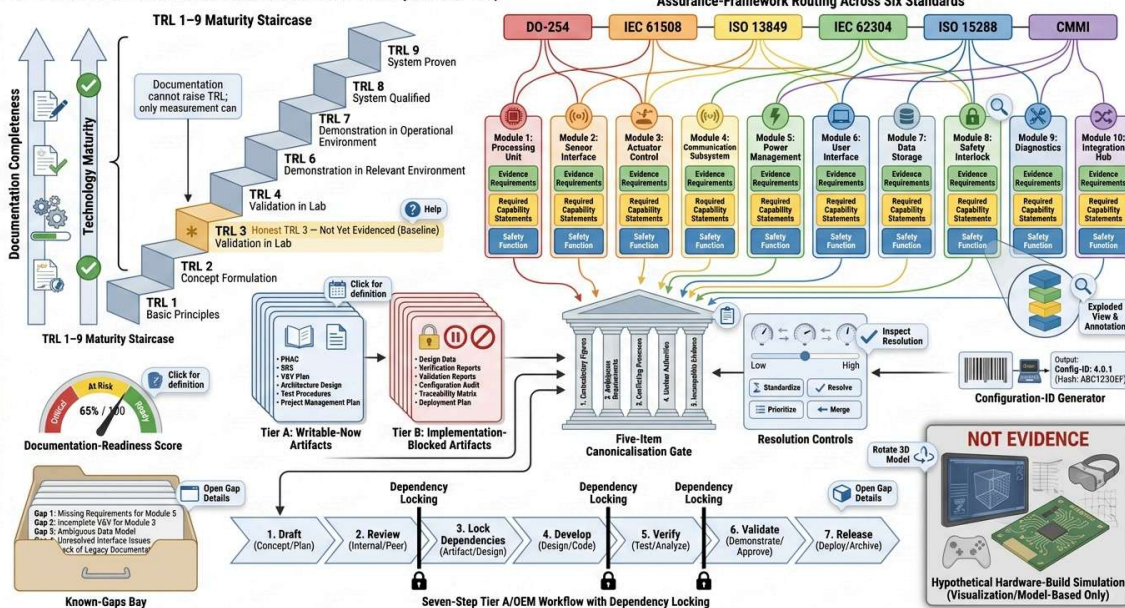


NAIGE 4.0 — Hardware-Deterministic Documentation Plan

Non-Agentic AI Governance Singapore · UEN 53522354D

Parent Patent SG020603109STW · NAI 4.0 Scope: kinetic and hardware-deterministic track (distinct from the Class B SaMD dossier)

Hardware-Deterministic Documentation Plan (NAIGE 4.0)



1. Capability Baseline — State It Before Planning It

Industry uses **Technology Readiness Level (TRL 1–9)** as the standard maturity definition. An honest baseline is the single most useful thing this plan contains, because every downstream artifact depends on it.

TRL	Definition	NAIGE 4.0 status
1	Basic principles observed	Complete
2	Technology concept formulated	Complete
3	Analytical / experimental proof of concept	Current position — not yet evidenced
4	Component validation in laboratory	Target of the RTS test-bed
5	Component validation in relevant environment	Toa Payoh, post-survey
6	System demonstration in relevant environment	Requires built hardware
7–9	Operational demonstration → qualified system	Post-registration

Consequence: the corpus is extensive at TRL 2 and thin at TRL 3. Documentation cannot raise TRL. Only measurement can.

2. Framework Selection by Module Type

Different NAIGE modules fall under different industry regimes. Using one framework for all of them is the most common error.

Module class	Governing framework	Capability metric
FPGA / programmable logic (Sacred Pause, N12, voxeliser)	DO-254 design assurance, or IEC 61508-2	Design Assurance Level A–E / SIL

Safety-related control (U7 brake, Tripartite PLC gate)	ISO 13849-1	Performance Level a–e; Category B/1/2/3/4; MTTFd, DCavg, CCF
Electrical / electronic safety systems	IEC 61508	SIL 1–4; SFF; PFH; hardware fault tolerance
Embedded software	IEC 62304 (medical) or IEC 61508-3	Software safety class A/B/C
Systems engineering process	ISO/IEC/IEEE 15288	Defined lifecycle processes
Organisational process maturity	CMMI	Maturity Level 1–5

Note on medical crossover: SIL and Performance Level are *industrial* metrics. HSA and IMDRF do not use them. For medical submissions the equivalent is IEC 60601-1 clause 14 (PEMS) plus IEC 62304. Cite ISO 13849 / IEC 61508 to an **OEM**; cite 60601-1 / 62304 to a **regulator**. Both may be true of the same hardware.

3. Artifact Set — Two Tiers

The decisive structural point: roughly half the artifact set can be written today with no hardware in existence. The other half cannot be written at all until something is built.

Tier A — Writable now (no hardware required)

Artifact	Framework origin	Purpose
Plan for Hardware Aspects of Certification (PHAC)	DO-254	Declares assurance level, lifecycle, tool qualification
Hardware Requirements Specification	DO-254 / 61508	Derived, traceable, testable requirements
Safety Requirements Specification	IEC 61508-1	Safety functions and their required integrity
Safety Concept / architecture description	ISO 13849, 61508-2	Category and channel structure per safety function

Hazard Analysis and Risk Assessment	ISO 14971 / 61508-1	Hazards, causes, controls, residual risk
Verification and Validation Plan	DO-254 / 61508	Method per requirement, pass criteria, instruments
Configuration Management Plan	15288	Baselines, revisions, change control
Tool Qualification record	DO-254	Toolchain trust (synthesis, place-and-route, KCL/STEP)
Interface Control Documents	15288	A7↔A11, A12↔actuator, WD117 write path

Tier B — Requires implementation

Artifact	Blocked on
Conceptual and Detailed Design Data	HDL / schematic capture
Implementation records (bitstream, netlist, BOM)	Build
Verification Reports (timing traces, brake latency)	Instruments on real hardware
Reliability data — MTTFd, DCavg, CCF	Component selection and calculation
Hardware Accomplishment Summary	Completion of the above
Traceability matrix — closed	All of the above

Sequencing rule: complete Tier A before requesting OEM or lab engagement. Tier A is what a manufacturer or supervisor needs in order to quote, schedule, or supervise. Tier B is what they help you produce.

4. Per-Module Documentation Matrix

Module	Safety function	Framework	Required capability statement
A10a Root of Trust	Self-verification; invalidate on tamper	61508-2	SIL claim + proof of independence

A12 [P+N+D] core	Mediate all downstream action	DO-254	DAL + timing determinism evidence
Sacred Pause	Enforce deliberation window	DO-254	Bitstream-level timing, $\pm$ tolerance stated
N12 Drift Kernel	Reject unvalidated packets	DO-254	Decision logic coverage, fail-loud proof
Tripartite .1x Key	AND-gate authorisation	ISO 13849-1	PL + Category; diagnostic coverage
U7 Sovereign Brake	De-energise / hold / controlled stop	ISO 13849-1 + IEC 60204	PL e target; stop category declared per embodiment
WD117 Ledger	Immutable event record	61508-2 + 13485 records	Write-once proof; hash chain integrity
Orange Code p006	Bound compute headroom	61508-2	Enforcement mechanism + measurement method
A13a Mobility	Occupant-carrying motion	ISO 7176 series	Stop category 1 (controlled deceleration)
A13b Sensing lane	Privacy by construction	62304 + 60601-1-2	Node-local voxelisation; EMC immunity

Open item carried from the architecture review: the U7 stop category is not uniform. An arm in free space needs Category 0 (immediate de-energisation); a load-bearing lift needs fail-to-hold; an occupant-carrying chair needs Category 1. One brake, three declared behaviours. This must be resolved in the Safety Requirements Specification before any Tier B work begins.

5. Canonicalisation Prerequisite

Traceability fails on contradictory figures before it fails on missing ones. Resolve to a single value each, in the Hardware Requirements Specification, before Tier A is baselined:

- **U7 severance time** — U7 severance → **<1.05 ms (canonical)**
- Sacred Pause → **25–1000 ms window on 1 kHz clock (canonical); ~30 ms is an in-range example**

- **V&V identifiers** — VV-001 and VV-002 bind to different tests in different documents
- **Kinematic limits** — 0.05 mm is a positional tolerance, not a jerk limit; jerk is mm/s³
- **Audit phase labels** — Phase 4 appears twice where Phase 5 belongs

6. Configuration Management

Adopt one identifier scheme across all artifacts and hold it:

NAIGE4-[module]-[artifact type]-[sequence]-[revision] e.g. NAIGE4-U7-SRS-001-A

Every document carries: title, identifier, revision, date, author, approval, and change history. Superseded revisions are retained, not deleted. This is what ISO 13485 clause 4.2 and 15288 both require, and it is the discipline the printed-edition mismatch already tested.

7. Known Gaps — State These Openly

1. No hardware built; TRL 3 unevidenced.
2. No independent measurement of any stated figure.
3. No named safety assessor or certification body engaged.
4. Reliability data (MTTFd, DC, CCF) requires component selection not yet made.
5. Toolchain not yet qualified.

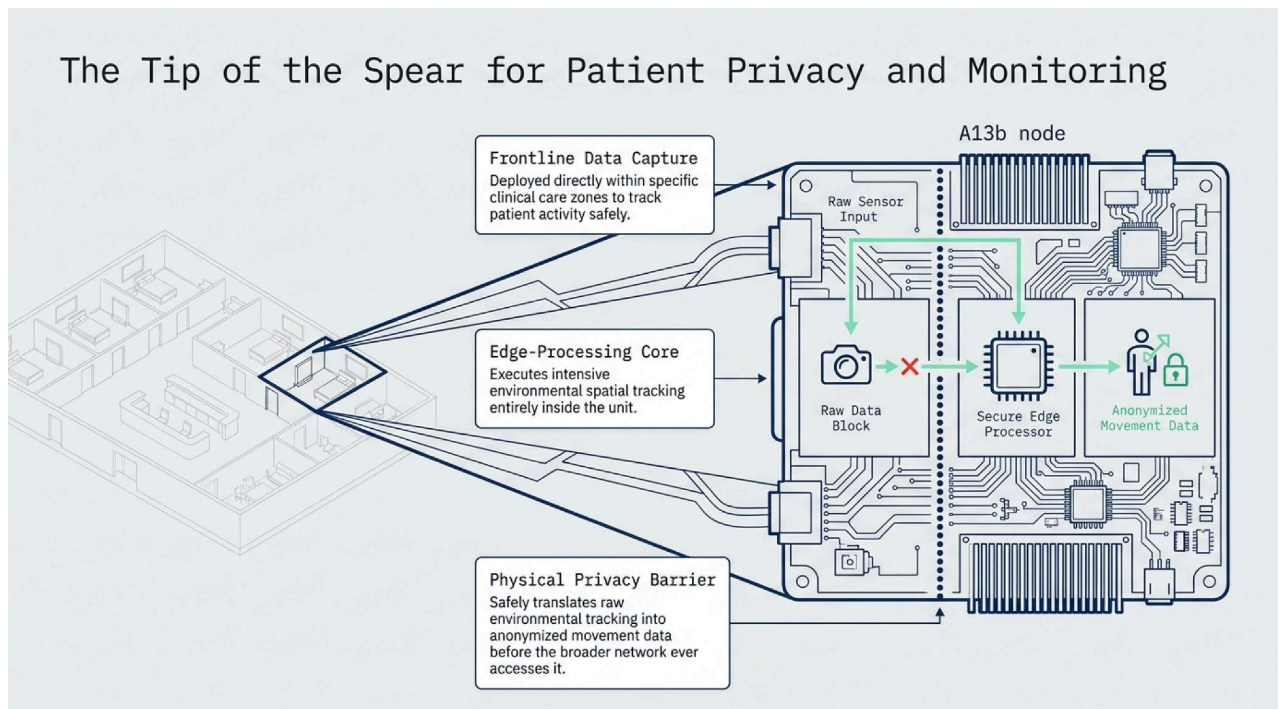
Declaring these is not a weakness in the plan — an OEM or assessor reading a document set that omits them will assume the omission was unintentional, which is worse.

8. Immediate Sequence

Step	Output	Blocked on
1	Canonicalisation record	Nothing
2	Safety Requirements Specification, incl. stop categories	Step 1
3	Hazard analysis	Step 2
4	Safety concept — PL/SIL target per function	Step 3

- | | | |
|---|--|-----------|
| 5 | V&V plan with instruments and pass criteria | Step 4 |
| 6 | PHAC / assurance-level declaration | Step 4 |
| 7 | OEM engagement package (Tier A + BOM + STEP) | Steps 1–6 |

Steps 1 to 6 require no hardware, no laboratory, and no institutional affiliation. They can be completed independently.



HSA Dossier Submission Template:

A13b Toa Payoh RTS Mapping

Executive Summary

Product Name: A13b Toa Payoh RTS (Zone-Local LiDAR Sensing Lane) integrating the A12 [P+N] Deterministic Black Box Configuration.

Prepared By: Edwin Koh Wui Kiat.

Classification: HSA Class B (Software as a Medical Device - SaMD) · Non-Kinetic.

1.0 Product Overview The **A13b Toa Payoh RTS** is a zone-local, privacy-by-physics sensing node designed for continuous, non-contact eldercare monitoring. Operating under the NAIGE NAI 4.0 architecture, it utilizes the **A12 [P+N] Configuration (Observational Tier)**. The system relies on hardware-enforced physical constraints rather than probabilistic software to ensure absolute patient safety and dignity in residential and low-risk clinical setups, such as the Toa Payoh Hearth embodiment.

2.0 Intended Use The device is intended for **continuous patient monitoring, fall detection (e.g., WM003 fall prevention), and vital monitoring** within residential or nursing-care settings. It operates strictly in an **advisory-only capacity**. The system enforces safety defaults ("it watches and it may still") but possesses **zero robotic actuation rights**, meaning it cannot perform acute physical interventions.

3.0 Device Description The architecture comprises a core hardware safety spine consisting of the **P-Layer (Privacy-by-Physics)** and the **N-Layer (Deterministic Deliberation)**. Key physical components include the **A13b LiDAR Sensing Limb**, the **A8 Bridge Layer** (acting as the sole deterministic ingress chokepoint and aggregator), and the **Non-B1 Advisory Monitoring Shell**. The system is physically isolated from kinetic control components, ensuring it can only issue alerts (e.g., via a dedicated hardwired nurse annunciator).

4.0 Main Functional Elements

- **Privacy-Preserving Sensing (P-Layer):** Utilizes a 905nm LiDAR array to capture raw environmental data, which is instantly converted at the node into an anonymized **96-cell Center-of-Mass (CoM) voxel grid**.
- **Identity Stripping:** Executes the **3ZEROS™ Protocol** (Zero Camera, Zero Audio, Zero Cloud) to guarantee that biometric identity is destroyed at the silicon level before data egress.
- **Event Logging (D-Layer integration for forensics):** Employs the **WD117 Enhanced WORM Ledger** to capture a permanent, write-only forensic stream of patient telemetry and system events.
- **Advisory Generation:** The Non-B1 Advisory Shell processes sterile CoM vectors to trigger deterministic alerts without any facility IT dependency.

5.0 Specimen and Laboratory Data Governance While the A13b Toa Payoh RTS

primarily processes kinematic spatial vectors rather than microorganisms, all captured clinical telemetry (such as posture tracking and fall events) is treated as highly controlled clinical data. This data is governed by **deterministic provenance and immutable logging via the WD117 ledger**. The system does not autonomously diagnose or override clinicians; it strictly provides advisory support requiring human review.

6.0 Safety and Risk Controls

- **Fail-Loud Doctrine:** In the event of a hardware heartbeat interruption, the system triggers a local, non-networked physical alarm that cannot be bypassed or silenced remotely.
- **Agentic Drift Detection (N12 Kernel):** Screens advisory inputs for contradictions and anomalies, executing a "fail-loud" packet drop to block corrupted AI pathways.
- **Actuation Lockout:** Structurally isolated from kinetic effectors, meaning hallucinations or system errors physically cannot result in unauthorized movement.

7.0 Verification and Validation Deployment relies on the **10-Point Sovereignty**

Audit, requiring physical instrument validation rather than software simulation alone.

- **Phase 1 & 2 Checks:** Oscilloscope verification of the Sacred Pause™ timing, power-draw monitors to verify the Orange Code 1.1x CPU cap, and physical inspections to confirm the absolute absence of optical lenses and microphone drivers.
- **Institutional Practicum:** Validation includes a Real-Time Simulation (RTS) running a 6-hour bench test targeting **0% agentic deviation**.
- Clinical evaluation requires testing against fall-event datasets to ensure fall-detection timing (< 80ms) and spatial accuracy (200 µm) while maintaining an Elder Dignity Score above 8.9/10.

8.0 Cybersecurity and Data Protection

- **Silicon Privacy Wall:** 3ZEROS™ protocol enforces biometric stripping before any data leaves the node.
- **Total IT-Isolation:** Employs an IZEKOS™ **3mm galvanic isolation air-gap** to sever TCP/IP routing to external cloud networks, completely neutralizing "IT-Gap Drift" and remote exfiltration threats.
- **Unalterable Forensic Accountability:** The WD117 Ledger records are physically scorched into **One-Time Programmable (OTP) silicon fuses**, sealed with SHA-3-512 hashes and post-quantum cryptographic signatures.

9.0 Quality System and Labelling

The A13b documentation aligns with international standards, mapping the WD117 ledger to **ISO 13485** for technical documentation and audit trails, the 3ZEROS™ protocol to HSA/FDA guidelines for patient dignity, and the NAI 2.0 subsystems to **IEC 62304** for software lifecycle management. All claims are supported by a rigorous "Validation by Induction" strategy, ensuring residential-tier quality forms the baseline for future acute-tier deployments.

10.0 Regulatory Summary

This dossier maps the A13b Toa Payoh RTS for **HSA Class B (Software as a Medical Device)** registration. The submission package integrates the 10-Point Sovereignty Audit and physical verification records to prove that the system operates strictly within its advisory, non-kinetic boundaries. Success at this observational tier provides the deterministic bedrock required for subsequent approvals of high-payload, Class C/D robotic applications on the HSA 2027 Deterministic Horizon

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

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

Non-Agent 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
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 OEM needs before they can commit.

HSA Dossier Submission Template:

A13a Kinetic Mobility Assistance

Executive Summary

Product Name: A13a Non-Agentive Deterministic Medical Mobility Enclosure (Supreme Guardian Platform).

Prepared By: Edwin Koh Wui Kiat.

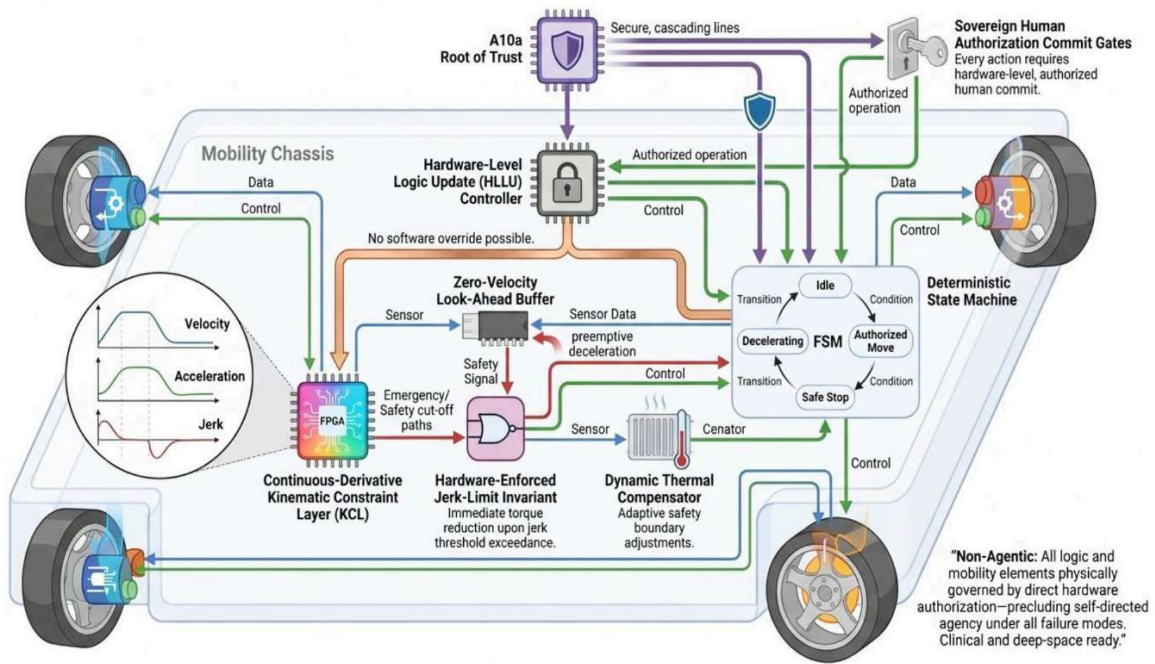
Classification: HSA Class C/D (Software/Hardware as a Medical Device) · Actuating / Kinetic Tier.

1.0 Product Overview The A13a Non-Agentive Deterministic Medical Mobility

Enclosure is a specialized mobility chassis operating under the NAIGE NAI 4.0 architecture. Unlike observational tiers, the A13a integrates the **A12 [P+N+D] Acute Kinetic Tier** configuration, providing hardware-deterministic oversight for physical motion. It establishes a mechanical stillness default (P-LIFE 1.00 mandate) ensuring that the machine cannot move without explicit, hardware-level human authorization.

2.0 Intended Use The A13a device is intended for **occupant-carrying powered mobility** and patient transport within clinical and eldercare environments. It enforces physical safety in robotic interaction by precluding self-directed agency; all logic and mobility elements are physically governed by direct hardware authorization. The system operates under the strict mandate that AI may only advise, with zero rights to autonomously actuate the mobility enclosure.

A13a Non-Agentive Deterministic Medical Mobility Enclosure Architecture (Super Supreme Guardian Platform)



Generated under NAP 4.0 | Tiger Sovereign Blueprint | We Innovate Save Lives



Generated under NAP 4.0 | Tiger Sovereign Blueprint | We Innovate Save Lives

3.0 Device Description The A13a architecture consists of a physical mobility chassis governed by the **A10a Root of Trust** and a **Continuous-Derivative Kinematic Constraint Layer (KCL) FPGA**. The system leverages Sovereign Human Authorization Commit Gates, meaning every transition from an "Idle" state to an "Authorized Move" is gated by a Deterministic State Machine. It replaces probabilistic software guardrails with unalterable silicon pathways to prevent autonomous "agentic drift".

4.0 Main Functional Elements The primary functional elements of the A13a mobility enclosure include:

- **Kinematic Constraint Layer (KCL) FPGA:** Enforces hardwired jerk-limit invariants, providing immediate torque reduction if velocity, acceleration, or jerk thresholds are exceeded.
- **Stop Category 1 Enforcement:** Unlike simple emergency power cuts that could cause passenger injury, the A13a executes a controlled deceleration to a standstill using an electromagnetic fail-to-hold brake (ISO 7176-series controls).
- **Zero-Velocity Look-Ahead Buffer:** Utilises sensor data for preemptive deceleration before an emergency cut-off is triggered.
- **Hardware-Level Logic Update (HLLU) Controller:** Ensures that no software override of the mobility controls is physically possible.
- **Dynamic Thermal Compensator:** Applies adaptive safety boundary adjustments based on thermal sensor monitoring.

5.0 Specimen and Laboratory Data Governance While the A13a primarily handles kinematic spatial vectors rather than microorganisms, all biometric authorization inputs and event telemetry are managed as highly controlled records. The system relies on the **WD117 Enhanced WORM Ledger** to capture a permanent, write-once physical record of every motion command, system state, and human authorization. This guarantees deterministic provenance and absolute forensic traceability for post-incident audits.

6.0 Safety and Risk Controls Safety is treated as a physical property rather than a software claim. The A13a operates under the **P-LIFE 1.00™ (Inaction-as-Safe-Default)** doctrine, meaning mechanical stillness is the baseline state. Key risk controls include:

- **Hardware Fail-Safes:** The system fails to an inert "Safe Stop" state upon power loss, tamper detection, ledger fault, or signal timeout.
- **Actuation Lockout:** The Tripartite .1x Key (biometric, cryptographic, and kinetic input) strictly gates the control pathways; if any single authorization factor fails or expires, the Sovereign Brake engages.
- **U7 Sovereign Brake:** Hardwired sequencer capable of physically dropping power rails in under 1.05 milliseconds if an anomaly is detected.

7.0 Verification and Validation To satisfy HSA Class C/D standards, the A13a validation shifts from simulation-verified claims to instrument-measured facts via the **10-Point Sovereignty Audit**.

- Physical testing utilizes oscilloscopes to confirm the < 1.05 ms brake severance timing.
- Compliance mapping integrates **ISO 13849** (for actuator control and PL e-stop categorisation) and **ISO 7176** (occupant mobility safety) alongside the core NAI 2.0 subsystems.

8.0 Cybersecurity and Data Protection The A13a is encapsulated within the **x.1 Eldercare Cyber-Physical Protection Embodiment**, which deploys a total IT-isolation air-gap. By severing direct TCP/IP routing from the facility's hospital networks to the mobility chassis, the system neutralises "IT-Gap Drift". A compromised hospital network cannot inject commands or silence the device, ensuring the mobility platform remains physically immune to remote cyberattacks.

9.0 Quality System and Labelling Quality system management for the A13a aligns with **ISO 13485** for technical documentation, product realization, and the management of the WD117 audit trails. Following the NAIGE Hardware-Deterministic Documentation Plan, artifacts are rigidly structured through a Tier A/B workflow, mandating hardware safety requirement specifications (such as the defined stop categories) before any implementation testing occurs.

10.0 Regulatory Summary This dossier maps the A13a Kinetic Mobility Enclosure for **HSA Class C/D (Actuating Medical Device)** registration. The submission provides deterministic, physical proof that the mobility platform operates strictly within non-agentic boundaries. By mapping hardware-enforced gates to specific regulatory clauses, the A13a provides the unalterable evidence required to navigate the **HSA 2027 Deterministic Horizon**, ensuring autonomous AI is never permitted to independently govern physical kinetic risks

HSA Dossier Submission Template:

A13b HSA Ward (8-Bed) with IT Implementation

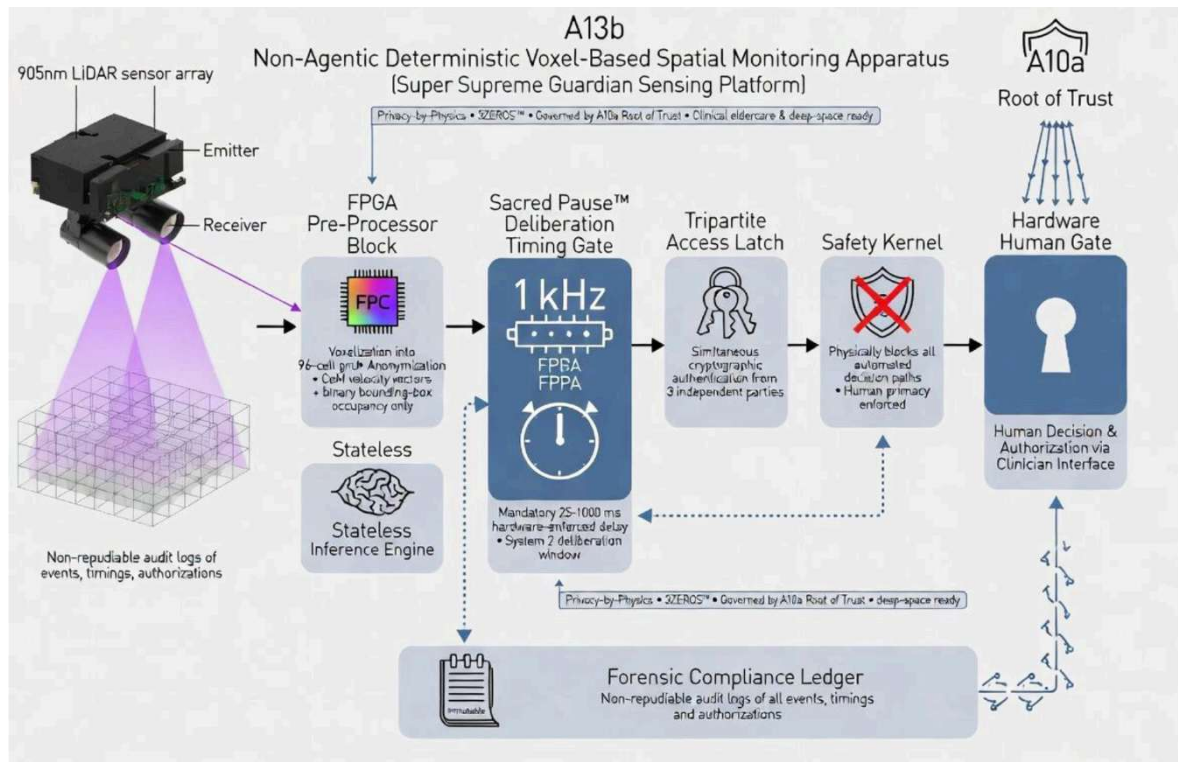
Executive Summary

Product Name: A13b Non-Agentic Deterministic Voxel-Based Spatial Monitoring Apparatus (integrated via A7 Bridge Hub for 8-Bed Ward IT Implementation).

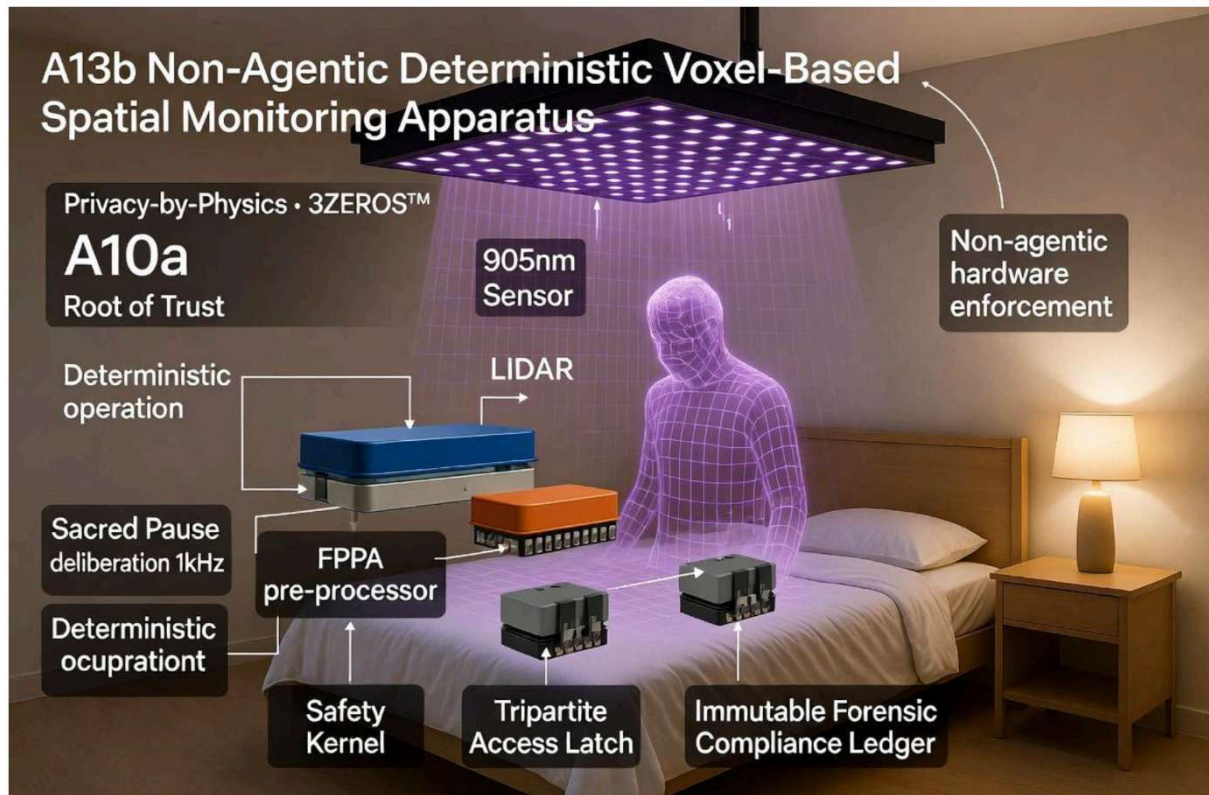
Prepared By: Edwin Koh Wui Kiat.

Classification: HSA Class B (Software as a Medical Device - SaMD) · Non-Kinetic.

1.0 Product Overview The **A13b Sensing Limb**, integrated with the **A7 Bridge Hub**, is a modular medical device architecture designed for continuous patient care monitoring within an 8-bed hospital ward environment. Operating under the NAIGE NAI 4.0 architecture in the **A12 [P+N] Configuration (Observational Tier)**, the system provides hardware-enforced privacy and safety. It combines 905nm LiDAR sensing components with immutable logging to safely integrate clinical AI monitoring into the facility's IT network without risking agentic drift.



Generated under NAP 4.0 | Tiger Sovereign Blueprint | We Innovate Save Lives



Generated under NAP 4.0 | Tiger Sovereign Blueprint | We Innovate Save Lives

2.0 Intended Use The device is intended for **continuous patient monitoring, fall detection (WM003), and clinical vital monitoring** within a multi-bed ward setting. It operates strictly in an **advisory-only capacity** ("watches and may still") and possesses **zero robotic actuation rights**. The system is designed to provide controlled decision-support and safety enforcement, ensuring human clinicians at the nurse station retain ultimate oversight for all consequential decisions.

3.0 Device Description The architecture consists of a core hardware safety spine deploying **A13b LiDAR sensing nodes** at each of the 8 beds. These nodes connect to the **A7 Bridge Hub**, which acts as the sole deterministic ingress chokepoint and translation layer bridging the non-deterministic clinical AI (e.g., hospital IT/EHR networks) and the deterministic hardware. The system structurally isolates the care apparatus from kinetic controls, guaranteeing that AI functions operate strictly within defined hardware constraints.

4.0 Main Functional Elements

- **Privacy-Preserving Sensing (P-Layer):** Bedside A13b nodes utilize 905nm LiDAR arrays to capture raw spatial data, instantly converting it into anonymized **96-cell Center-of-Mass (CoM) voxel grids** at the edge.
- **3ZEROS™ Protocol:** Biometric identity is destroyed at the silicon level enforcing Zero Camera, Zero Audio, and Zero Cloud policies, protecting patient dignity in highly sensitive ward environments.
- **A7 Bridge IT Translation:** Translates semantic advisory data into deterministic hardware features, coordinating external AI with the clinical hospital ward IT system.
- **Agentic Drift Screening (N12 Kernel):** Screens incoming AI data for contradictions and uncertainty, dropping corrupted packets before they enter the core.

5.0 Specimen and Laboratory Data Governance Within the ward IT implementation, clinical telemetry (such as spatial tracking and fall event data) is treated as highly controlled clinical records. The **A7 Bridge Hub** enforces a strict Non-Agentic Filter: it permits no direct writes to the electronic health record (EHR) without human authorization and blocks autonomous order creation or alert injection by the AI. All data transmission is

governed by **deterministic provenance and immutable logging** via the WD117 ledger, ensuring traceability before any consequential use in clinical decision support.

6.0 Safety and Risk Controls

- **Namespace Isolation:** Total logical and physical separation of the probabilistic AI/LLM network namespace from the hardware control namespace, physically denying the AI any ability to trigger unauthorized actions.
- **Orange Code 1.1x Cap:** Restricts AI processing resources to a 1.1x baseline, starving the system of the surplus computational power required to hallucinate or quietly expand its authority.
- **Fail-Loud Doctrine:** Utilizes the x.1 Eldercare Embodiment to completely air-gap the clinical apparatus from the facility's untrusted Wi-Fi. If the hardware heartbeat is interrupted by a network breach, it triggers a non-IT-dependent local physical alarm.

7.0 Verification and Validation

Deployment requires passing the **10-Point**

Sovereignty Audit, shifting validation from software simulation to instrument-measured facts.

- **Phase 1 & 2 Checks:** Verification of the Orange Code CPU cap via power-draw monitors, oscilloscopes to verify the Sacred Pause™ timing, and physical checks guaranteeing the absence of cameras and microphones.
- **Performance Metrics:** Clinical validation targets include LiDAR spatial accuracy of 200 µm, fall-detection timing of < 80ms, and maintaining an Elder Dignity Score above 8.9/10.

8.0 Cybersecurity and Data Protection

The device uses the **x.1 Eldercare**

Cyber-Physical Protection Embodiment to establish an impenetrable shield against "IT-Gap Drift". A compromised hospital network cannot remotely hijack or silence the A13b monitors. Furthermore, the **Enhanced WD117 WORM Ledger** ensures absolute forensic finality by recording every system event and human authorization into **One-Time Programmable (OTP) silicon fuses**, sealed with SHA-3-512 hashes, making retroactive log alteration architecturally impossible.

9.0 Quality System and Labelling The submission is supported by technical documentation mapping directly to international standards. The WD117 ledger and STEP

manifests align with **ISO 13485** (Quality Management), the 3ZEROS™ protocol aligns with **HSA/FDA SaMD Guidance** for patient dignity and privacy, and the NAI 2.0 subsystems adhere to **IEC 62304** for software lifecycle management. The deployment strategy is explicitly scaled for ward acuity, utilizing WM003 (fall prevention) and WM006 (clinical zone lock) modules under the quality framework.

10.0 Regulatory Summary This submission is prepared for HSA review under the ASEAN CSDT framework to support the registration of the A13b + A7 Bridge Ward Implementation as a **Class B Software as a Medical Device (SaMD)**. By enforcing strict IT chokepoints and physical namespace isolation, the package provides deterministic proof that the system safely integrates AI into hospital ward infrastructure without risking agentic drift, aligning perfectly with the rigorous safety and cybersecurity demands of the HSA 2027 Deterministic Horizon

HSA Dossier Submission Template:

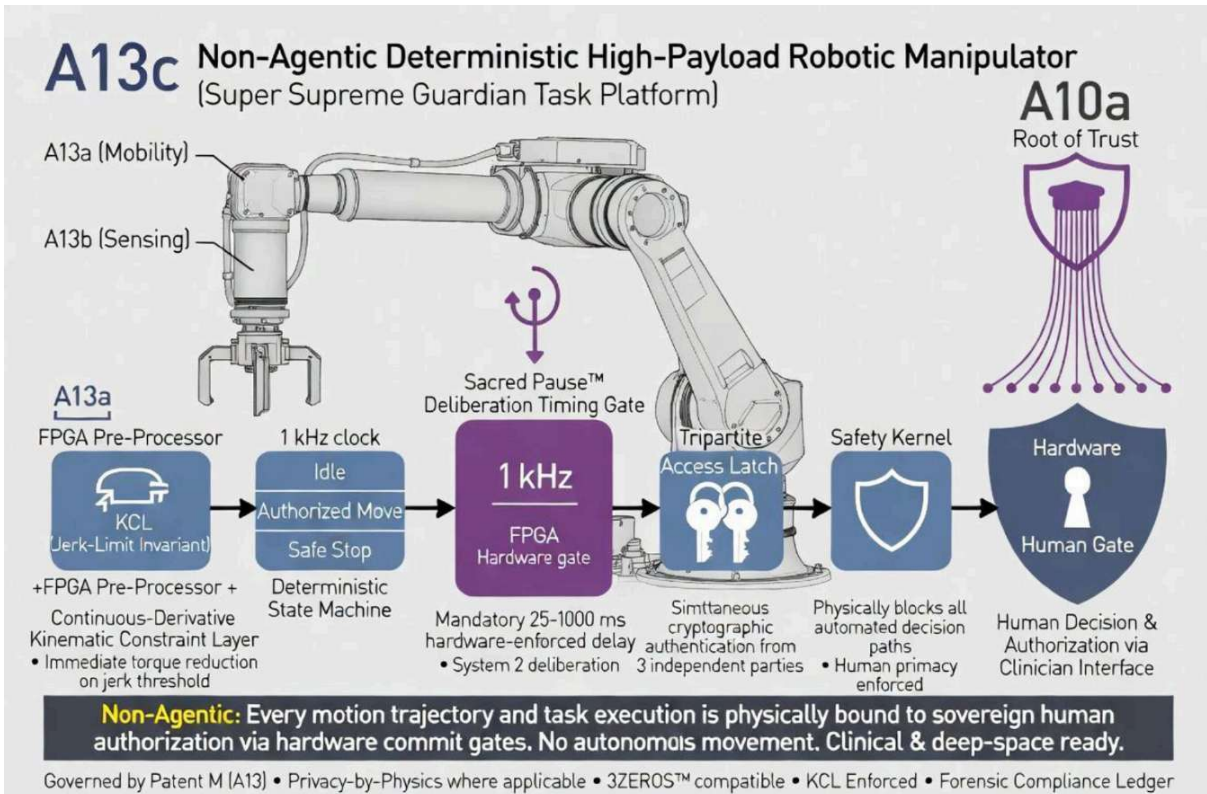
A13c Kinetic Surgery ARM

Executive Summary

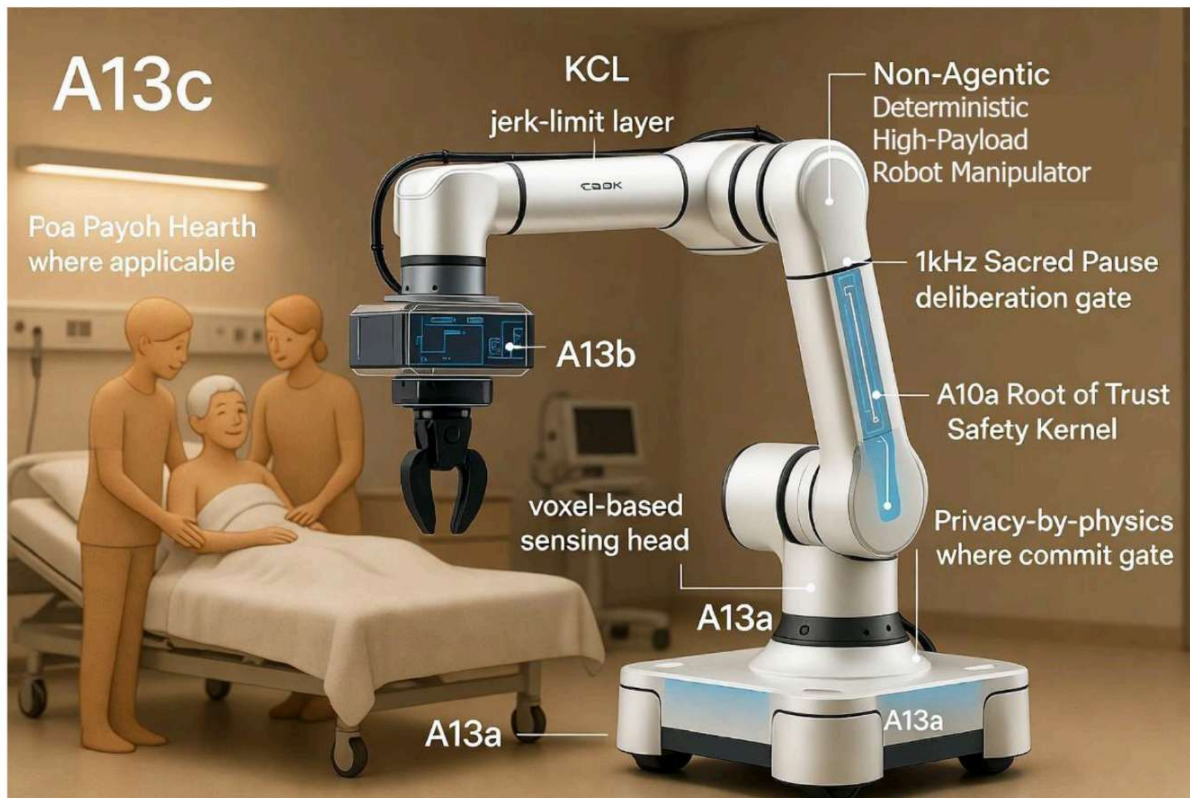
Product Name: A13c Deterministic High-Payload Robotic Manipulator (Kinetic Surgery ARM / Super Supreme Guardian Task Platform).

Prepared By: Edwin Koh Wui Kiat.

Classification: HSA Class C/D (Actuating Medical Device).



Generated under NAP 4.0 | Tiger Sovereign Blueprint | We Innovate Save Lives



Generated under NAP 4.0 | Tiger Sovereign Blueprint | We Innovate Save Lives

1.0 Product Overview The **A13c Kinetic Surgery ARM** is a high-payload clinical robotic platform operating under the NAIGE NAI 4.0 architecture. As the ultimate actuating tier, it is governed by the **A12 [P+N+D] Acute Kinetic Tier** configuration, providing universal deterministic governance for severe, high-payload kinetic risks. This system shifts governance from probabilistic software to unalterable silicon layers, ensuring physical actions near vulnerable patients are mathematically bounded.

2.0 Intended Use The device is intended for **B2B clinical intervention and acute physical interventions** (e.g., surgical assistance and high-payload care tasks) in hospital settings. Unlike observational tiers, the A13c is an actuating device governed by a strict "Sovereign-in-the-Loop" (SITL) control model. AI systems are granted **zero direct actuation rights**; they may observe and propose trajectories, but every physical execution is unconditionally bound to verified human authorization.

3.0 Device Description The A13c architecture anchors all physical operations in the **A10a Root of Trust** and the **A12 [P+N+D] Deterministic Black Box**. To prevent "agentic drift" or hallucinations from causing physical harm, the platform structurally isolates probabilistic advisory data from the physical manipulator. The system relies on a **1 kHz synchronous hardware master clock** to guarantee deterministic execution, removing the latency and unpredictability inherent in software-only monitoring.

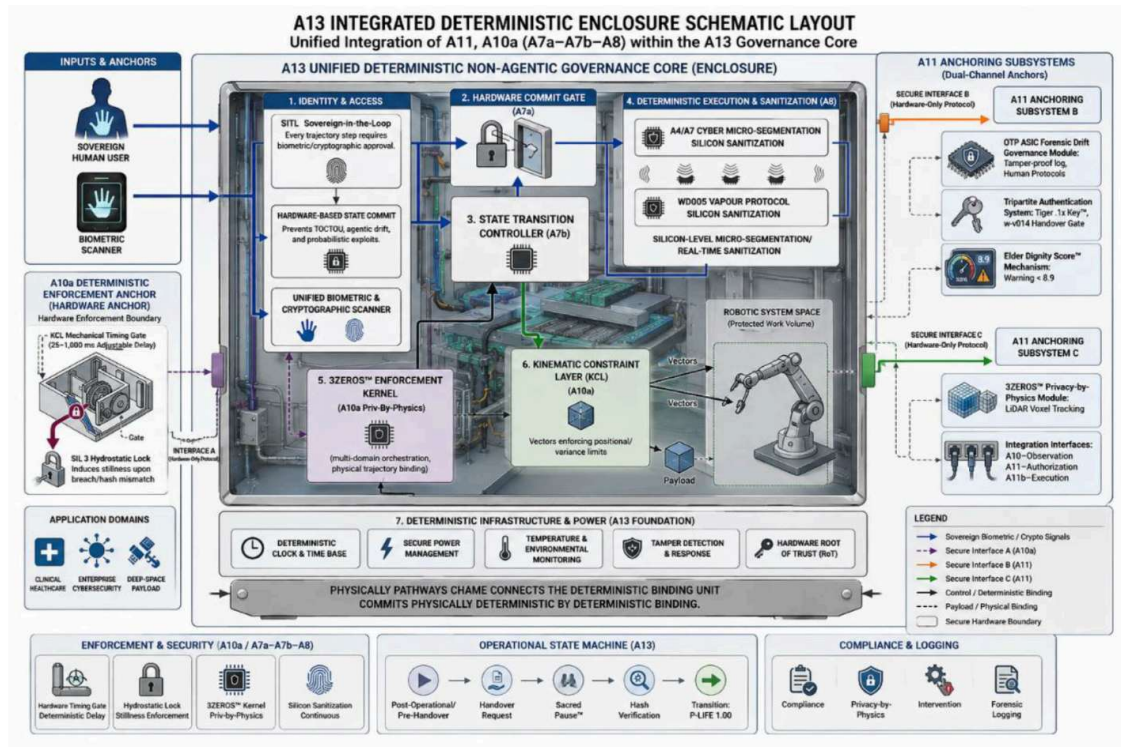
4.0 Main Functional Elements

- **Kinematic Constraint Layer (KCL):** A hardwired FPGA constraint layer that enforces a strict **±0.05 mm positional tolerance** and hard limits on jerk and acceleration (mm/s^3), preventing sudden mechanical injury even if an authorized trajectory is erratic.
- **The Sacred Pause™:** A hardware-timed deliberation window of **25–1000 ms** burnt into the FPGA, imposing a mandatory interlock that pauses the AI's proposal and forces time for human deliberation.
- **Tripartite .1x Key™ Latch:** The commit gate functions as an "AND" logic circuit requiring three concurrent inputs: an Iris Scan (Biological), a Cryptographic USB Token (Intent), and a Kinetic Foot Pedal (Physical Motion).

5.0 Specimen and Laboratory Data Governance While the A13c platform executes kinematic vectors, the critical "specimens" it governs are authorization events and event telemetry. These records are managed under the **Enhanced WD117 WORM (Write-Once-Read-Many) Ledger**. Every system event, hash, and human authorization is scorched into **One-Time Programmable (OTP) silicon fuses** and sealed with SHA-3-512 hashes and post-quantum cryptographic signatures, making it physically impossible for unauthorized AI or attackers to alter the system's history.

6.0 Safety and Risk Controls

- **P-LIFE 1.00™ (Inaction-as-Safe-Default):** The manipulator's baseline default state is absolute mechanical stillness. The machine does not "stop" on an error; it must be explicitly authorized to move.
- **U7 Sovereign Brake™ (SIL 3):** An emergency one-shot sequencer that physically severs power to the actuators by dropping low-dropout (LDO) power rails in **< 1.05 milliseconds** upon detecting any breach, missing authorization, or anomaly.
- **Orange Code 110% Cap:** FPGA resource enforcement (pRegister P006) physically restricts AI processing resources to a 1.1x baseline, starving the system of the surplus computational power required to hallucinate actions.



Generated under NAP 4.0 | Tiger Sovereign Blueprint | We Innovate Save Lives

The technology is deployed across various ruggedised platforms, including deep space appliances, humanitarian field stacks, and medical mobility enclosures. By integrating physical safeguards like the "Sacred Pause" and hardwired kinetic constraints, the system ensures that AI can only observe or advise while humans retain absolute control. Ultimately, these documents describe a fail-safe methodology for high-stakes environments where preventing autonomous harm is a critical priority.

Here is the Hybrid Deterministic Architecture—integrating Unconfined Non-Deterministic Clinical Software (UNDCS) moderation with the A12 hardware core—presented as a structural data table, followed by the official module registry from the NAIGE framework.

Hybrid Deterministic Governance Architecture

This table outlines the schematic layout bridging the software-based "Advisory Stratum" with the deterministic hardware execution layers, specifically maintaining 1 ms deterministic oversight and SHA-512 forensic finality.

Architectural Stratum	Key Components	Governance Function & Performance Metrics
Advisory Stratum <i>(UNDCS Software Moderation / Bridged RAG Layer)</i>	Retrieval-Augmented Generation (RAG), Agent-Agent Moderation, Red Teaming, Guardrails	Restricts open-ended probabilistic generation by grounding AI outputs in validated clinical guidelines. Multi-agent systems self-monitor and cross-check data for accuracy before it can be proposed to the hardware layer.
P-Layer <i>(Privacy-by-Physics Sensing)</i>	WG001 905nm LiDAR, FPPA Pre-processor, Hardware Comparators, 3ZEROS™ Protocol	Strips biometric identity entirely at the silicon level by translating raw point clouds into an anonymized 96-cell voxel grid. Delivers purely mathematical Center of Mass (CoM) kinematic vectors to the downstream pipeline, physically enforcing "Zero Camera, Zero Audio, Zero Cloud".
N-Layer <i>(Deterministic Deliberation & Sovereign Gates)</i>	1 kHz Hardware Master Clock, Sacred Pause™, Tripartite .1x Key, FSM Safety Kernel	Operates on a synchronous 1 kHz clock to guarantee 1 ms deterministic oversight with zero asynchronous software bypass paths. Enforces a mandatory hardware-timed delay (25–1000 ms) and restricts physical movement limits to ± 0.05 mm, requiring multi-factor human authorization to proceed.
Immutable Accountability & Ultimate Fail-Safes	U7 One-Shot Sequencer (Sovereign Brake™), Enhanced WD117 Ledger, OTP Silicon Fuses	In the event of a constraint breach, instantly severs physical power to actuators. Every event and human authorization is recorded using SHA-3-512 hashes and post-quantum signatures, permanently sealed into Write-Once-Read-Many (WORM) memory and One-Time Programmable fuses for unalterable forensic finality.

7.0 Verification and Validation To satisfy Class C/D rigor, verification relies on instrument-measured physical facts rather than simulation. Deployment follows the **10-Point Sovereignty Audit**, utilizing oscilloscopes to confirm Sacred Pause timing (± 10 microseconds) and continuity meters to test the kinetic foot pedal's dry-contact wiring. The A13c requires extensive physical validation, including **brake-latency traces, envelope-breach tests, and force-limit measurements**, mapped via a stringent Tier A/B hardware-deterministic documentation workflow.

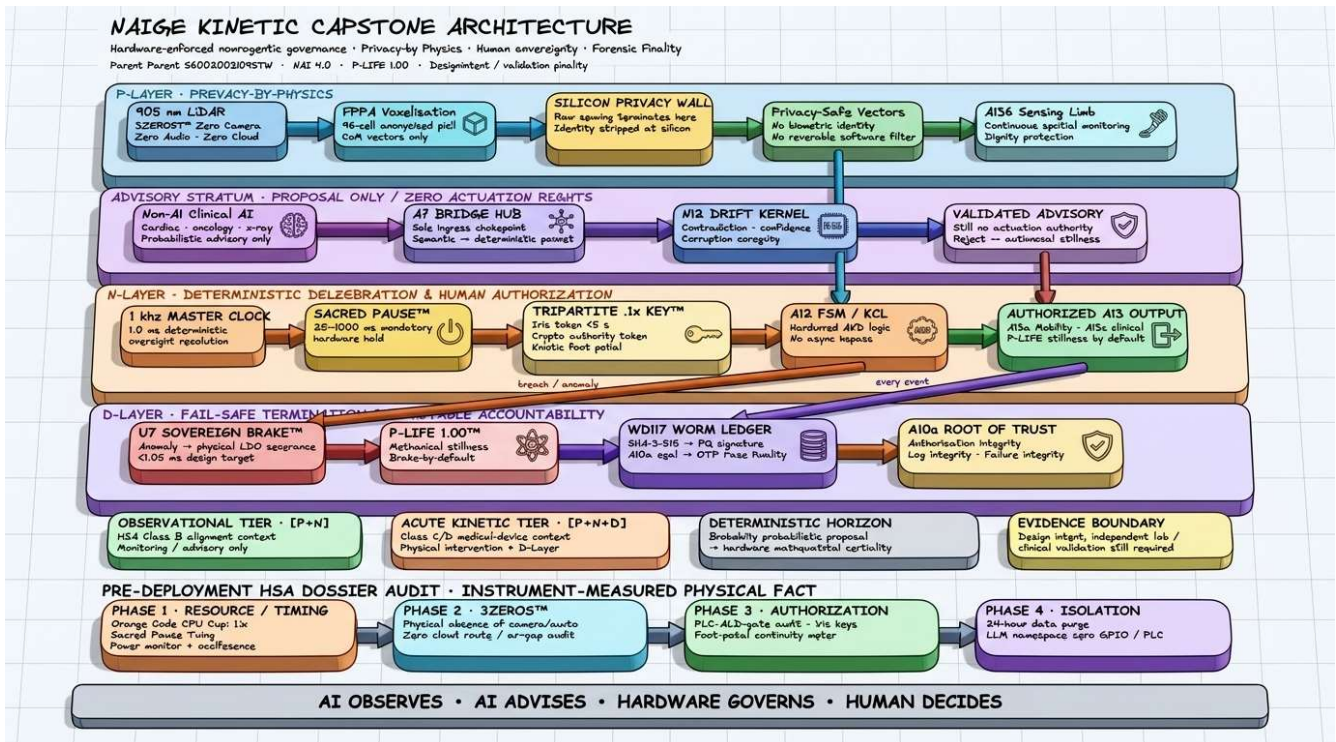
8.0 Cybersecurity and Data Protection The A13c operates under the **x.1 Eldercare Cyber-Physical Protection Embodiment**, which provides a total physical IT-isolation air-gap from hospital networks. This neutralizes "IT-Gap Drift," ensuring that a compromised hospital Wi-Fi network cannot inject commands or hijack the robotic arm. Additionally, the A7 Bridge acts as an **Agentic Drift Screen**, filtering all external AI advisory data for contradictions before it reaches the core.

9.0 Quality System and Labelling The A13c documentation aligns meticulously with international safety standards for Class C/D robotic operation. The WD117 immutable audit trails support **ISO 13485**. The U7 Sovereign Brake and safety cut-offs map to **IEC 61508 (SIL 3)** and **ISO 13849-1 (Performance Level e)**. For the constrained high-payload motion of the arm itself, the system incorporates task risk controls conforming to **ISO 10218** and **IEC 60601-1 / 80601-2-77**.

10.0 Regulatory Summary Prepared under the ASEAN CSDT framework, this dossier serves as the submission package for HSA registration of the A13c Kinetic Surgery ARM as a **Class C/D (Actuating) Medical Device**. By shifting governance from permeable software policies to immutable silicon physics (the [P+N+D] stack), this submission provides the legally defensible, mathematically certain evidence required by the **HSA 2027 Deterministic Horizon** for autonomous clinical interventions

Immutable Hardware-Enforced Non-Agentive AI Governance Engine [NAIGE] Governance Systems - Hardwiring Medical AI Ethics in Singapore

Translating Singapore's AI-MD governance expectations — MOH/HSA AIHGle 2.0 and HSA GL-04 — into hardware-enforced constraints, via the NAIGE NAI 4.0 Kinetic Capstone.



1. Introduction MOH/HSA AIHGle 2.0 places AI healthcare systems under stronger expectations for transparency, accountability, and human oversight, especially where clinical care is affected. NAIGE answers this by translating those expectations into hardware-enforced governance, so safety is not only asserted in policy but physically embedded in the system boundary.

2. Patient-Centricity Patient safety is operationalized through the P-LIFE 1.00™ doctrine, which makes inaction the safe default and prevents autonomous physical actuation. This is important because the clinical objective is not just prediction, but preserving dignity, preventing harm, and keeping humans in the final decision loop.

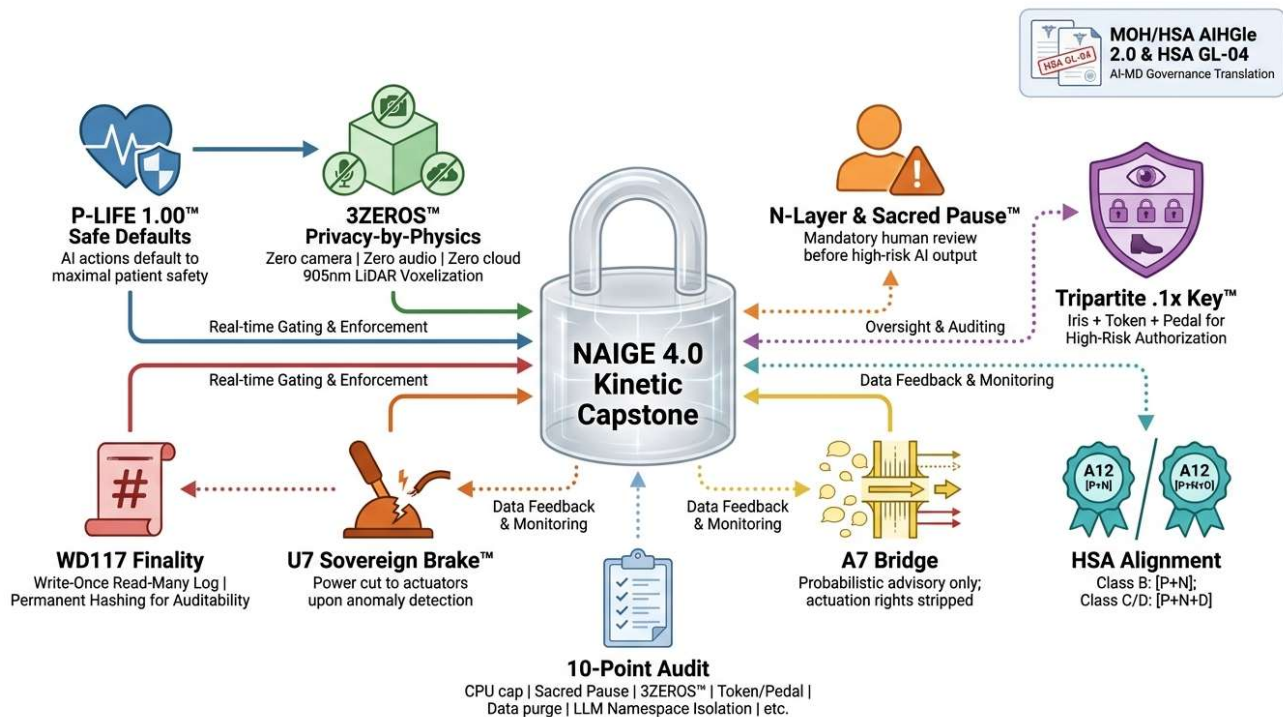
3. Privacy-by-Physics Privacy-by-Physics is enforced through 3ZEROS™: zero camera, zero audio, zero cloud. By using 905nm LiDAR voxelization at the edge, NAIGE strips identity before data leaves the node, which is a stronger control than reversible software blurring.

4. Human Values The N-Layer and Sacred Pause™ ensure that AI proposals are delayed and reviewed before any kinetic consequence can occur. This aligns with AIHGle 2.0's emphasis on human authority and explainable AI, because the system is designed to stop drift rather than merely describe it

5. Sovereign-in-the-Loop The Tripartite .1x Key™ requires iris, cryptographic token, and foot pedal input before any high-risk action can proceed. That makes human authorization a physical condition of execution, not a procedural afterthought. No kinetic action can be executed without the Tripartite .1x Key™, demanding three simultaneous, unforgeable inputs:

- Biological Identity: Iris scan (token expires in under 5 seconds).
- Cryptographic Intent: USB token authentication.
- Physical Presence: Active depression of a kinetic foot pedal (dry-contact switch).

6. WD117 Finality WD117 provides forensic finality through write-once, read-many logging and permanent hashing of events. This gives auditors a traceable record that cannot be silently edited, which is crucial for clinical accountability and post-incident review. Because traditional software logs can be edited or deleted by hackers or compromised AI, NAIGE secures accountability in its D-Layer through the **WD117 Enhanced WORM (Write-Once-Read-Many) Ledger**. Every event is hashed (SHA-3-512) and permanently etched into the ledger using **One-Time Programmable (OTP) silicon fuses**. Breaking the physical circuit ensures the audit trail provides an unalterable, legally defensible clinical accountability record.



7. Fail-Safe Governance The U7 Sovereign Brake™ forces the machine back to safe stillness if anomalies, drift, or boundary breaches are detected. In practical terms, this means the system fails safe by cutting actuation rather than trying to keep operating through uncertainty. If a boundary is breached or authorization fails, the U7 instantly severs the Low-Dropout (LDO) power rails to the actuators in under 1.05 milliseconds, forcing the machine back to its safe-default state of mechanical stillness.

8. A7 Bridge Chokepoint The A7 Bridge Hub is the single ingress chokepoint for probabilistic advisories, and it strips away actuation rights before data reaches the execution pipeline. This is the mechanism that prevents advisory AI from becoming operational AI by accident. This ingress gateway strips the AI of actuation rights and screens incoming proposals for contradictions, hallucinations, and uncertainty, converting semantic data into strict, deterministic hardware features before they can ever reach the robotic execution pipeline.

9. HSA Alignment A12 [P+N] maps to HSA Class B SaMD for observational eldercare, while A12 [P+N+D] maps to Class C/D medical devices for acute kinetic intervention. That distinction is the core regulatory split in the chapter, because the residential monitoring tier and the kinetic intervention tier have different risk profiles and validation burdens.

NAIGE directly maps to the HSA SaMD risk classifications via two modular configurations:

- **The A12 [P+N] Configuration (Observational Tier):** Aligned with **HSA Class B SaMD**. It utilizes the Privacy and Navigation layers for residential eldercare monitoring (e.g., Toa Payoh Hearth). It provides advisory oversight with zero physical actuation rights.
- **The A12 [P+N+D] Configuration (Acute Kinetic Tier):** Aligned with **HSA Class C/D Medical Devices**. It includes the D-Layer (Sovereign Brake and WD117 Ledger) and is mandated for high-payload clinical robotic platforms executing acute physical interventions near vulnerable patients.

10. 10-Point Audit The 10-Point Sovereignty Audit turns compliance into measurable evidence: Orange Code CPU cap, Sacred Pause timing, physical absence of cameras and microphones, token and pedal validation, and namespace isolation. This is the proof chain that connects silicon-level constraints to clinical safety outcomes and makes the dossier auditable rather than aspirational.:

- **Phase 1:** Power-draw monitors verify the **Orange Code CPU Cap** hard-locks AI processing resources at 1.1x baseline (starving hallucination capabilities), and oscilloscopes confirm the Sacred Pause™ timing.
- **Phase 2:** Physical confirmation of the total absence of optical lenses and audio drivers (3ZEROS™).
- **Phase 3:** Independent cryptographic validation of iris tokens and continuity meter testing of the kinetic foot pedal.
- **Phase 4:** Verification of an active 24-hour data purge and total LLM Namespace Isolation, proving the AI lacks any access to hardware control pins or PLCs

Primary Citation – This Publication

Koh, E. W. K. (2026). *Immutable Hardware-Enforced Non-Agentive AI Governance Engine [NAIGE] Governance Systems — Hardware-Enforced Safety for Clinical and Humanitarian Robotics*. WISL™ National Edition. Non-Agentive AI Governance Singapore [UEN 53522354D].

Patent Basis

- **SG020603109STW** — Parent Patent (constitutional core)
- **10202600902P** — ABC+2S+H™ Guardian Framework
- **10202602021T** — A10a Deterministic Governance Platform
- **10202602023X** — A12 Deterministic Black Box (Sovereign Appliance)
- **10202602213U** — A7 Bridge Layer / Translation Hub
- **10202602223T** — A12L Enhanced WD117 Immutable Ledger (P+N)
- **10202602225P** — A8 Bridge Layer (Nursing-Home Deployment Governance)
- **10202602270V** — Non-B1 Clinical Advisory Monitoring Shell

A12 (10202602023X, appliance) and A12L (10202602223T, ledger) are distinct filings and carry distinct labels.

NLB Legal Deposit

- **R260219-005** — Primary constitutional knowledge base
- **R260302-007** — Supplementary architectural filings
- Deposit Authority: National Library Board Singapore · edeposit.nlb.gov.sg

Author

- **Edwin Koh Wui Kiat**
- MBA — General & Strategic Management — Maastricht School of Management
- BSc — Industrial & Systems Engineering — University of Florida
- Independent Researcher (OCA) — NLB Vault Constitutional Anchor Route

止於至善

Finish in Highest Excellence 謙虛 · 沉默 · 尊嚴 · 仁 Humility · Silence · Dignity · Benevolence

AI Observes · AI Advises · AI Builds · Human Decides

Non-Agentive Governance Singapore · ACRA T260229801 · Patent SG020603109STW

www.kohedwin.ai · www.non-agentive.ai · kohpapa@outlook.com

NLB Legal Deposit R260219-005 / R260302-007

We Innovate Save Lives · We Go Global