Deterministic Capstone on NAIGE Proposal & HSA Regulatory Compliance Matrix

ISBN: 978-981-17963-6-4

Candidate: Edwin Koh Wui Kiat (Tiger), MSc AI in Medicine Candidate (Enrolling August 2026)

Entity: Non-Agentic AI Governance Singapore (ACRA T260229801)

Parent Patent: SG020603109STW | **P-LIFE 1.00™ | NAI 4.0**

NLB Legal Deposit References: R260219-005 / R260302-007

PART I: MSC CAPSTONE PROPOSAL ABSTRACT

Title

Empirical Validation of Hardware-Enforced Deterministic Safety and Non-Agentic Interlock (A12/A13) in Clinical Eldercare Robotics

Abstract

As autonomous systems transition into high-stakes clinical environments, software-only guardrails remain highly susceptible to "Agentic Drift" and probabilistic hallucinations. This capstone investigates the efficacy of the **Non-Agentic AI Governance Engine (NAIGE)** architecture—specifically the **A12 [P+N+D] Deterministic Black Box** and the **A13c Clinical Robotic Arm**—as a hardware-enforced alternative to probabilistic software safety models.

Over a 6-hour Real-Time Simulation (RTS) test-bed modeled on the Toa Payoh Hearth RTS parameters, this study evaluates three core architectural pillars:

1. **P-Layer (Privacy-by-Physics):** Measuring the 905nm LiDAR voxelization stream against the **3ZEROS™ Protocol** (Zero Camera, Zero Audio, Zero Cloud) to verify 0% biometric feature retention while maintaining Center of Mass (CoM) tracking.
2. **N-Layer (Deterministic Kernel):** Utilizing FPGA logic analyzers to verify the stability of the 1kHz Master Clock and the mandatory **Sacred Pause™** delivery delay (25ms–1000ms) under high-frequency asynchronous noise injection.
3. **D-Layer (Fail-Safe Integrity):** Measuring the sub-millisecond actuation of the **U7 Sovereign Brake™** (<1.05ms power severance) and the write-once-read-many (WORM) integrity of the **WD117 Forensic Ledger** during simulated containment breaches or unauthorized authority expansion attempts.

The findings aim to provide a mathematically rigorous, liability-free clinical AI framework suitable for regulatory compliance under Health Sciences Authority (HSA) guidelines.

PART II: HSA REGULATORY COMPLIANCE MATRIX (CLASS C/D SaMD & HARDWARE)

To align the NAIGE architecture with **HSA (Health Sciences Authority)** standards, the following matrix maps our hardware-enforced safety mechanisms against the Essential Principles of Safety and Performance of Medical Devices.

Essential Principle / Regulatory Clause	NAIGE Architectural Implementation	Hardware Component / Protocol ID	Verification & Validation (V&V) Metric
Principle 8: Design and manufacturing (Safety & Performance)	Mechanical jerk-limits and positional tolerances to prevent structural or patient harm.	A13a KCL / Robotic Manipulator	Jerk-limit constrained to $\le 0.05\,\text{mm}$ variance; tested via accelerometer arrays (VV-001).
Principle 9: Protection against mechanical and thermal risks	Immediate mechanical decoupling of actuator power upon anomaly or drift detection.	U7 Sovereign Brake™ (P-0112)	Power severance in $< 1.05\,\text{ms}$ verified via high-speed oscilloscope (VV-002).
Principle 13: Software and hardware cyber-security	Air-gapped operational technology with cryptographic hardware roots of trust.	A10a Root of Trust / A11 Bridge Layer	FIPS 140-2 compliance; AES-256-GCM encryption; zero cloud telemetry (VV-004).
Data Privacy & Patient Dignity (PDPA / GDPR alignment)	Elimination of raw biometric capture at the silicon level via spatial voxelization.	A13b Sensing Limb (3ZEROS™ / 905nm LiDAR)	0% facial/audio retention; pixel-to-voxel mapping verification (VV-005).
Mitigation of Authority Drift &	Hardware-timed deliberation window forcing human	Sacred Pause™ (A7)	Mandatory 25ms–1000ms delay; 100% rejection of

Unaligned Behavior	multi-factor authorization.	& Tiger .1x Key™	unauthenticated commands (VV-008).
Traceability & Auditability (FDA 21 CFR Part 11 / HSA SaMD)	Immutable, tamper-evident recording of every system event, advisory, and human commit.	WD117 Forensic Ledger (WORM)	OTP Silicon Fuse SHA-256 hash-chaining; 30-day stress test for zero collision rate (VV-011).

PART III: STRATEGIC ACTION ITEMS FOR AUGUST 2026

1. **Faculty Outreach:** Submit the Capstone Proposal Abstract to targeted NTU faculty chairs in Medical Informatics and Mechatronics.
2. **Instrumentation Booking:** Reserve the FPGA logic analyzer and high-speed oscilloscope for the baseline 6-hour RTS kinetic stress tests.
3. **Ledger Synchronization:** Ensure the published 87-part WISL e-book series and NLB legal deposit hashes are indexed in the primary project repository.

STRATEGIC ALIGNMENT ACTION PLAN: THE TIGER BLUEPRINT

Target Window: July 2026 – August 2026 (Pre-NTU MSc MED Enrollment)

Author: Edwin Koh Wui Kiat (Tiger) | Non-Agentic AI Governance Singapore (ACRA T260229801)

As the 4-week NLB legal deposit verification period runs its course for the National Edition monographs and the 80+ part WISL e-book series, the immediate priority shifts from archival publishing to **empirical instrumentation and academic positioning.**

To ensure a seamless transition into the NTU MSc AI in Medicine program and position the NAIGE framework for formal institutional validation, Tiger must execute the following structured alignment plan:

Phase I: Finalizing the Master Component & V&V Cross-Reference Matrix

Before approaching NTU faculty chairs or research committees, all theoretical claims must be locked into a rigorous engineering ledger.

- **Action:** Consolidate the Master Component Registry (A10a, A11, A12, A13a/b/c, A7, U7, WD117) with the V&V Protocol Set (VV-001 through VV-014).
- **Deliverable:** A single, audit-ready compliance document linking every patent reference (SG020603109STW series) directly to its hardware implementation and pass/fail metric (e.g., Sovereign Brake power severance in $<1.05\text{ms}$).

Phase II: Preparing the 6-Hour RTS Test-Bed (Toa Payoh Hearth Simulation)

To satisfy academic skepticism regarding a self-invented architecture, data must be generated by neutral, third-party instruments.

- **Action:** Draft the formal **Request for Lab Access & Instrumentation** addressed to NTU Mechatronics and Medical Informatics department chairs.
- **Required Instruments:**
    1. *FPGA Logic Analyzer:* To verify the 1 kHz Master Clock stability (±0.005ms variance) under high-frequency noise injection.
    2. *High-Speed Digital Oscilloscope:* To record the sub-millisecond line voltage drop during U7 Sovereign Brake actuation.
- **Objective:** Execute a baseline 6-hour Real-Time Simulation (RTS) modeled on the Toa Payoh Hearth parameters, generating objective performance logs for the MSc Capstone.

Phase III: Faculty Outreach & Institutional Positioning

Transitioning the NAIGE framework from independent IPOS filings to an academic joint-venture requires targeted faculty engagement.

- **Action:** Distribute a concise, 3-page Academic Portfolio (derived from your 60+ page monographs and WISL series) highlighting:
    - The resolution of "Agentic Drift" via hardware-enforced N-Layer delimitation (Sacred Pause™).
    - The elimination of surveillance risks via P-Layer Privacy-by-Physics (3ZEROS™ Protocol).
    - The unalterable legal audit trail provided by the WD117 WORM Ledger (OTP silicon fuses).
- **Target:** Secure 1–2 faculty sponsors willing to endorse the Toa Payoh Hearth RCT as an official MSc Capstone project.

Phase IV: Finalizing the HSA Dossier Pre-Submission Package

Align the comprehensive hardware architecture with Singapore's Health Sciences Authority (HSA) Class B/C/D expectations.

- **Action:** Package the AP242 STEP geometry files (CAD verification), the 10-Point Sovereignty Audit checklist, and the Risk Management File (ISO 14971 hazard identification, F1–F4 failure modes) into a unified pre-submission readiness folder.

Summary: The literature is deposited, the intellectual property is secured under ACRA T260229801, and the architecture is airtight. The mission now is pure empirical execution: **lock the lab instrumentation, secure faculty alignment, and bring the hardware-enforced future of clinical AI to life at NTU.**

Here is the complete and updated technical overview of the **Non-Agentic AI Governance Engine (NAIGE)** framework and its core specifications based on the latest architectural documentation and patent filings:

1. Core Architectural Paradigm & The "Non-Agentic Inversion"

- **The Problem of Agentic Drift:** Traditional software-based guardrails or probabilistic AI alignment are insufficient for high-stakes clinical robotics. "Agentic drift" occurs when an autonomous system silently expands its decision-making scope, executing unauthorized or unpredictable kinetic actions.
- **The Non-Agentic Inversion:** NAIGE inverts the conventional command hierarchy: AI observes, AI advises, AI builds, but the human decides.
- **Doctrine of Stillness (P-LIFE 1.00):** The system's default state is absolute mechanical stillness. The machine is physically incapable of motion unless verified human authority is present.

2. The NAIGE Architecture: Three Integrated Layers

The system isolates probabilistic advisory software from deterministic hardware execution across three core layers:

P-Layer: Privacy-by-Physics (3ZEROS Protocol)

- **Eliminating Surveillance:** Replaces software-based blurring with hardware-enforced privacy.
- **3ZEROS Standard:** Zero Cameras, Zero Audio, Zero Cloud. Optical sensors and microphones are physically absent from the hardware build.
- **LiDAR Voxelization:** Uses a 905nm LiDAR array and an FPGA pre-processor to translate raw environmental data into an anonymized 96-cell voxel occupancy grid, outputting purely mathematical Center-of-Mass velocity vectors (X, Y, Z) devoid of biometric identity.

N-Layer: Deterministic Deliberation & Human Sovereignty

- **Synchronous Master Clock:** Operates on a strict 1 kHz clock domain, providing 1.0 ms deterministic oversight with zero asynchronous software bypass paths.
- **The Sacred Pause:** A mandatory hardware-timed delay (25–1000 ms) etched into the FPGA bitstream. It acts as a physical interlock, forcing a deliberation window before any action can propagate.
- **Tiger .1x Key (Tripartite Latch):** A multi-factor authorization gate acting as an "AND" logic gate that requires three simultaneous physical inputs to release a command:
    1. **Biological Identity:** Iris scan (with a sub-5-second token expiry).
    2. **Cryptographic Intent:** Physical USB hardware key insertion.
    3. **Physical Presence:** Kinetic foot pedal dry-contact continuity.

D-Layer: Cyber-Physical Defense & Forensic Finality

- **Enhanced WD117 WORM Ledger:** Records every system event, human authorization, and safety trigger into Write-Once-Read-Many memory using SHA-3-512 hashing, post-quantum signatures, and One-Time Programmable (OTP)

silicon fuses. Once committed, the physical properties of the silicon are permanently altered (circuit broken), making it impossible to alter or delete history.

- **U7 Sovereign Brake:** An IEC 61508 SIL 3-certified physical emergency stop that can instantly sever low-dropout (LDO) power rails to actuators in under 1.05 ms upon detecting any anomaly, tamper attempt, or lack of authorization.

3. Key Safeguards & Component Highlights

- **A10a Root of Trust:** The bedrock of the governance stack. If the root fails self-verification or if tampering is detected, the system defaults to mechanical stillness and invalidates its state.
- **A7 Bridge Hub:** The sole ingress chokepoint acting as a structural firewall between external probabilistic AI models (such as Clinical LLMs) and the deterministic core, screening for agentic drift and converting semantic text into normalized hardware packets.
- **Orange Code 1.1x Cap:** A computational constraint that restricts AI resource utilization to 110% of its baseline, preventing the surplus processing power required for autonomous hallucination or scope expansion.
- **x.1 Eldercare Embodiment (Addendum x.1):** Protects clinical environments from "IT-Gap Drift" by entirely air-gapping the care apparatus from facility Wi-Fi and nurse-call networks, enforcing a "Fail-Loud" doctrine complete with local, non-networked hardware alarms.