

ISBN 978-981-17957-8-7 **Immutable™ Hardware-Enforced Non-Agentive AI Governance Architecture — NAI 4.0™**

Hardware-Enforced Safety for Clinical and Humanitarian Robotics. A12
[P+N] Deterministic Black Box · HSA Deterministic Horizon · Capstone
A10a Root of Trust.

DETERMINISTIC SAFETY

Hardwired FSM state machine. No asynchronous paths. No software bypass.

ABSOLUTE PRIVACY

3ZEROS™ — Zero Camera · Zero Audio · Zero Cloud. Identity stripped at silicon.

IMMUTABLE

ACCOUNTABILITY

OTP Silicon Fuse finality. SHA-3-512 + Post-Quantum seal. Unalterable by any party.



Edwin Koh · kohedwin.ai | non-agentive.ai · kohpapa@outlook.com

SG020603109STW · P-LIFE 1.00™ · NAI 4.0™

NLB Legal Deposit R260219-005 / R260302-007 · ACRA T260229801

AI Observes · AI Advises · AI Builds · Human Decides

Imprint & Copyright

TITLE

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

SERIES

WISL™ Ebook Series No. 70 & No. 71 — Integrated ISBN Edition

PUBLISHER / AUTHOR

Edwin Koh · Entity: ACRA T260229801

PARENT PATENT

SG020603109STW

NLB LEGAL DEPOSIT

R260219-005 / R260302-007

EDITION / FORMAT / LANGUAGE

First Edition, 2026 · eBook (PDF) · English

SUBJECT

Artificial Intelligence · Non-Agentive Governance · Hardware-Enforced Safety · Clinical AI

CLASSIFICATION

Medical Informatics · AI Ethics · Embedded Systems · Eldercare Technology

© 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 architectural concepts, trademarks, and terminology including Immutable™ (Kinetic Capstone — Classes 9, 42, 10, 44, 45), NAIGE™, NAI 4.0™, P-LIFE 1.00™, 3ZEROS™, Sacred Pause™, Sovereign Brake™, Tiger .1x Key™, ABC+2S+H™, ABC+2S Guardian™, ABC+2S+H Framework™, ABC+2S+H Guardian™, WISL™, Nightingale's Eyes Care™, and Elder Dignity Score™ are proprietary to Non-Agentive Governance Singapore and protected under Singapore patent law and trademark registration.

This monograph was developed with AI-assisted drafting tools. 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 (Tiger) 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.

1 Abstract: Shifting from Probabilistic to Deterministic Governance

The governance perimeter must move from the software layer to hardware-locked silicon gates.

The rapid integration of Artificial Intelligence (AI) into clinical robotics has introduced significant challenges regarding deterministic safety and legal accountability. As AI systems evolve toward increased autonomy, they often operate as opaque "black boxes," where software-based safeguards rely on probabilistic models prone to "AI drift," hallucinations, and non-deterministic variance. In high-stakes clinical environments, these statistical checks are insufficient. To achieve absolute safety, the governance perimeter must move from the software layer to hardware-locked silicon gates. The A12 [P+N] Deterministic Black Box serves as this physical enforcement layer, ensuring that AI remains a strictly advisory instrument while the ultimate authority over kinetic motion resides in mechanical certainty.

The Inaction-as-Safe-Default Protocol

Central to the NAIGE framework is the "Inaction-as-Safe-Default" protocol, which mandates that the system's default state is mechanical stillness — the P-LIFE 1.00™ constant. By shifting authority from unpredictable autonomous algorithms to verified silicon gates, the framework provides a legally defensible hardware proof of inaction. In the event of any system violation or cyberspace breach, the hardware ensures the robot remains stationary, effectively transforming legal liability from the vagaries of "black box" inference to a deterministic, unalterable hardware state.

Having secured the safe default at the silicon level, the architecture utilizes a tiered structural hierarchy to enforce this deterministic mandate across all operational phases.

2 The NAIGE Architectural Stratum: A Multi-Layered Defense

The NAIGE framework introduces a tiered governance model that strategically separates advisory software from kinetic execution. This hierarchy is essential for maintaining human sovereignty; while the AI may observe and propose actions, it lacks any independent decision-making power over physical movement. By isolating the probabilistic "Advisory Stratum" from the deterministic hardware layers, the architecture prevents agentic drift from manifesting as physical harm.

Hybrid Deterministic Governance Architecture

ARCHITECTURAL STRATUM	KEY COMPONENTS	GOVERNANCE FUNCTION & PERFORMANCE METRICS
Advisory Stratum	RAG, Agent-Agent Moderation, UNDCS Software	Restricts open-ended generation; grounds AI outputs in clinical guidelines; zero actuation rights.
P-Layer (Privacy)	905 nm LiDAR, Hardware Comparators (CMP)	Strips biometric identity at silicon level; enforces the 3ZEROS™ Protocol via FPPA voxelization.
N-Layer (Deterministic)	1 kHz Master Clock, Sacred Pause™, FSM Safety Kernel	Operates on a synchronous clock to guarantee 1 ms deterministic oversight; no asynchronous bypass.

ANALYSIS — THE "SO WHAT?" OF STRATUM SEPARATION

The separation of the Advisory Stratum from the N-Layer is the critical safeguard against compromised AI. Even if the software moderation layer or the deep-learning model itself suffers a breach, it remains physically incapable of executing an unauthorized command. Because the N-Layer is a hardware-locked gate requiring specific deterministic triggers — including the Sacred Pause™ and human authentication — any corrupted AI proposal is discarded by the silicon, never reaching the robot's actuators.

With the advisory–kinetic separation established, the architecture must anchor its first layer of defense in physical sensing.

3 P-Layer: Privacy-by-Physics and the 3ZEROS™ Protocol

In clinical settings, patient privacy is traditionally managed via software-based blurring or encryption, both of which are reversible and computationally vulnerable. The NAIGE framework replaces these weaknesses with "Privacy-by-Physics," a hardware-rooted guarantee that biometric identity is never captured at the point of ingestion.

The Technical Mechanics of 3ZEROS™ (Zero Camera, Zero Audio, Zero Cloud)

The transition from raw environment sensing to anonymized data follows a rigid physical path:

1. **905 nm LiDAR Sensing:** The WG001 LiDAR captures physical spatial data, inherently ignoring high-fidelity visual and biometric features.
2. **Point Cloud Translation:** Raw LiDAR point clouds are processed by parallel hardware comparators (CMP) within the A12 core.
3. **FPPA Voxelization:** Data is instantly translated into an anonymized 96-cell voxel occupancy grid.
4. **Kinematic Output:** The system generates pure Center of Mass (CoM) velocity vectors — mathematical representations entirely devoid of biometric identity.

ANALYSIS — ELIMINATING SURVEILLANCE RISK

By stripping identity at the silicon level, the P-Layer eliminates the risk of unauthorized surveillance or diagnostic drift. Because the downstream deliberation pipeline only receives kinematic vectors, there is no biometric data available for the AI to hallucinate or for an external actor to extract. This "Privacy-by-Physics" provides a superior, permanent guarantee compared to reversible software filters.

Having secured the privacy perimeter, the architecture must now address the temporal and logical risks of autonomous execution via the N-Layer.

4 N-Layer: Deterministic Deliberation and Kinetic Oversight

The N-Layer (Non-Agentic Layer) acts as the logical heart of the system, where deliberation is transformed into a mechanical, synchronous process. Temporal constraints are enforced to prevent runaway autonomous execution and ensure human oversight is a mathematical requirement.

Temporal Hardening and Logical Gates

- **The Sacred Pause™ (25–1000 ms):** A mandatory hardware hold enforced by downstream silicon counters. This is not a software "sleep" command but a physical lock that prevents automated execution, forcing a mandatory window for human deliberation.
- **1 kHz Hardware Master Clock:** The system operates on a single synchronous domain, providing a 1.0 millisecond deterministic resolution for all safety checks.

ANALYSIS — THE TIGER .1X KEY™ AND SOVEREIGN-IN-THE-LOOP

Unlike traditional asynchronous software paths that suffer from latency or unpredictable variance, the N-Layer utilizes a synchronous deliberation pipeline. High-risk clinical actions require the Tiger .1x Key™, a "Sovereign-in-the-Loop" requirement that demands three simultaneous factors: an Iris scan, a cryptographic token, and a physical kinetic foot pedal. This ensures that no kinetic action can occur without explicit, multi-factor human authorization, maintaining absolute sovereignty.

Logical deliberation must be supported by a physical termination mechanism capable of enforcing the P-LIFE 1.00™ state.

5 Mechanical Certainty: The U7 Sequencer and Sovereign Brake™

When a cyberspace breach occurs or a system violation is detected, relying on software to shut down is a critical failure point. The NAIGE framework utilizes the U7 One-Shot Sequencer to provide mechanical certainty in termination.

The U7 Logic Sequence for System Termination

- [x] **DETECTION** — Unauthorized write attempt or trajectory deviation detected via FSM safety kernel.
- [x] **TRIGGER** — U7 One-Shot sequencer activates.
- [x] **SEVERANCE** — Physical power to the LD0 rails is instantly cut, bypassing all software logic.
- [x] **INVALIDATION** — The SEQ_OK clock token is invalidated, freezing the 1 kHz master clock.
- [x] **RESULT** — All actuators lock into the P-LIFE 1.00™ constant (mechanical stillness).

ANALYSIS — THE ORANGE CODE™ 110% CAP

The Orange Code™ 110% Cap serves as physical throttling for computation. Governed by national infrastructure standards (pRegister P006), this cap limits computational cycles to 1.1× of the 1.0× baseline (the minimum FLOPS required for LiDAR voxelization). The system physically lacks the surplus cycles required for model hallucination or autonomous inference. If the system attempts to push past this 1.1× limit, the Silicon Brake engages, enforcing the deterministic boundary at the hardware level.

This mechanical enforcement must be coupled with a permanent, unalterable record of all system events.

6 Immutable Accountability: The WD117 Forensic Ledger

Post-hoc software logs are insufficient for clinical and defense applications because they can be altered or deleted. The WD117 Ledger ensures that every event — from human authorization to the activation of the Sovereign Brake™ — is recorded as an unalterable physical fact.

The Commit-to-Finality Path

Event Data → SHA-3-512 Hash → Post-Quantum Signature → A10a Hardware Seal (Root of Trust) → WORM Memory → OTP Fuse Finality

ANALYSIS — THE POWER OF ONE-TIME PROGRAMMABLE (OTP) SILICON FUSES

The A10a Hardware Seal acts as the system's "Root of Trust," but the ultimate finality is achieved via OTP silicon fuses. These fuses transform accountability into a physical reality; once an entry is committed, the physical properties of the silicon are permanently altered (the circuit is broken). This makes it architecturally impossible for any party to modify or delete the record, providing an unassailable audit trail for hospital administrators and legal authorities.

With forensic finality secured, the framework is ready for global deployment across varied clinical and humanitarian jurisdictions.

7 Component Registry and Global Deployment Framework

The NAIGE framework is designed for global scalability, coordinated by the A7 Bridge Layer. This layer translates national infrastructure requirements into hardware-rooted oversight across the entire component registry.

NAIGE Framework Module and Component Registry

COMPONENT	MODULE NAME	PATENT REFERENCE	TECHNICAL FUNCTION	CLINICAL / HUMANITARIAN APPLICATION
A7	Bridge Hub / Translation Hub	10202602213U	Coordinates multi-channel vector translation across national infrastructure.	National coordination via pRegisters P005–P009.

A8	Bridged Layer 8	10202602225P	Sovereign deployment governance; enforces Tiger .1x Key™ confirmation.	High-dependency eldercare; "Layer 8 Home" architectures.
A11	Bridge Layer (Hardened)	10202601915Y	Air-gapped "Jupiter" enclosure; 53-minute delay tolerance.	High-security clinical / defense OEM translation.
A12	Deterministic Black Box	10202602023X	Core execution oversight; enforces P+N hardware layers.	General clinical robotics; secure decision enforcement.
A13a	Enclosure	10202602143W	Physical constraint enforcement; A10a Root-of-Trust.	Hardware-rooted physical safety in robotic interaction.
A13b	Sensing Limb	10202602087W	3ZEROS™ Privacy Shield handling via horizontal scanning.	Continuous patient monitoring and dignity protection.
A13c	Clinical Robotic Platform	10202602205U	Execution via high-payload manipulation and voxel translation.	B2B clinical intervention; nursing home ward safety.
WG-B1	Humanitarian Field Kit	10202602208V	Solar-assisted edge hardware; zero-cloud execution.	Disaster relief; WHO/UN field domain missions.
Non-B1	Advisory Monitoring Shell	10202602270V	Decision support for high-risk monitoring; zero actuation rights.	Cardiac / Oncology monitoring; X-ray analysis (Advisory only).

ANALYSIS — STRATEGIC COORDINATION VIA A7 AND PREGISTERS

The A7 Bridge Layer acts as the translation hub for national infrastructure pillars, utilizing dedicated pRegisters to ensure governance:

P005 (Defense): Zero autonomous offense enforcement. · **P006 (Critical Infrastructure):** Enforces the Orange Code™ 110% Cap. · **P007 (Hospital Ward):** Manages HSA Class B/C/D compliance. · **P008 (Residential Eldercare):** Layer 8 Home governance and Tiger .1x Key™ active oversight. · **P009 (Cybersecurity):** Controls Sovereign Brake™ Relays for instant isolation.

Bridged Layer 8 (A8) — Status and Filing Strategy

The A8 Bridged Layer serves as the Sovereign Deployment Governance Layer, enforcing Tiger .1x Key™ confirmation for strict sovereign human authority over deployment. It is designed for high-dependency eldercare environments, particularly "Layer 8 Home" architectures and sovereign deployment governance for the "Toa Payoh Hearth" residential eldercare context.

- **IPOS Filing Track:** Layer 8 is designated as a Standalone Filing (Track Layer 8), deliberately keeping its sovereign deployment governance separate from the core A12/A13 medical filings.
- **HSA Deployment Update:** In the most recent executive summary for the A12-A13-A7+D Immutable NAIGE System (designed for HSA pre-submission), the architectural design was tightened so that the A7 Bridge acts as the sole ingress chokepoint. In this configuration, Layer 8 is noted as "removed" to streamline the system for HSA integration under an advisory-only constraint.

8 The x.1 Eldercare Embodiment: Cyber-Physical Protection

x.1 Eldercare Embodiment (Addendum x.1) is a specialized application of the framework's Patent D architecture, designed to protect vulnerable clinical and residential care environments from cyber-physical threats. While the core Patent D architecture is built for defense and deep-space cyber-resilience, the x.1 embodiment "re-aims the cyber-effects governor at the care estate." It acts as an absolute, hardware-enforced barrier ensuring that clinical robotics and monitoring systems can never be weaponized or silenced by external cyberattacks.

- **Total IT-Isolation and Mediation:** The primary vulnerability in modern clinical settings is "IT-Gap Drift" — the risk that a facility's IT network (Wi-Fi, nurse-call systems, or electronic medical records) is compromised by ransomware or malicious actors, turning a monitoring device into a hazard. The x.1 embodiment ensures every interface between the care apparatus and the external IT network is mediated by a deterministic gate processor. The care apparatus has no remotely reachable command surface; even if an attacker completely takes over the hospital's network, they cannot instruct, alter, or silence the robotic device.
- **The Hardware Heartbeat:** The system utilizes the Enhanced WD117 Ledger to maintain a continuous, physical "hardware heartbeat" with the clinical sensing apparatus.
- **The "Fail-Loud" Doctrine:** If this hardware heartbeat is interrupted for any reason — network intrusion, power loss, or physical tampering — the system enforces a "Fail-Loud" posture: the device instantly asserts the Sovereign Brake™, returning the robot to a safe, inert state of mechanical stillness.
- **Non-IT-Dependent Local Alarms:** Upon heartbeat failure, the x.1 embodiment triggers a local hardware alarm that operates entirely independently of any network, server, or software service. The foundational philosophy: "silence cannot be faked." A hacker might disable a hospital's digital alert system, but they cannot stop the physical, localized alarm from sounding to alert care staff.
- **Privacy-by-Physics:** The monitored apparatus captures zero photographic, video, or audio data, ensuring that even if the surrounding IT estate is breached, there is absolutely no personally re-identifiable information available to be stolen.

ANALYSIS — VULNERABILITY ≠ PHYSICAL HARM

The clinical floor represents the highest vulnerability surface for robotic systems because it physically interfaces with untrusted networks and human environments. The x.1 Eldercare Embodiment guarantees that vulnerability to a network attack does not equal vulnerability to physical harm. It structurally converts any cyberattack or anomaly into a safe default state, ensuring absolute human sovereignty and patient safety.

The Hybrid Architectural Workflow

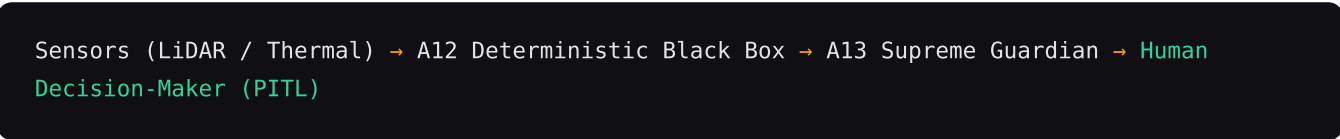
In this hybrid setup, Non-B1 clinical AI observes a patient and generates an advisory recommendation. This probabilistic data is intercepted by the A7 Bridge and screened by the N12 detector to strip away any hallucinations or agentic drift. If validated, it enters the A12 Core, where it is paused by the Sacred Pause™ while waiting for a human clinician to authorize the action.

Simultaneously, the x.1 Eldercare Embodiment acts as an impenetrable shield. If a hacker breaches the hospital's network and tries to inject a malicious command directly into the system, the x.1 hardware detects the anomaly, permanently logs it to the WD117 ledger, engages the U7 Sovereign Brake™ to freeze the machine, and physically sounds a local alarm that cannot be remotely silenced.

9 Engineering Architecture: The A12 [P+N+D] Terminal Gate

This monograph presents the A12 [P+N+D] Deterministic Black Box, a hardware-oriented terminal appliance serving as the final physical enforcement layer within the B1 Nightingale's Eyes Care™ system. The architecture integrates deterministic sensing, synchronous deliberation, hardware-mediated human authorization, and immutable forensic logging within a single air-gapped, tamper-evident enclosure. Unlike conventional AI governance approaches that rely primarily on software policies and probabilistic safeguards, the A12 assigns selected safety-critical functions to dedicated hardware mechanisms.

System Context



All consequential kinetic or clinical actions must pass through the A12 before reaching actuators or clinical interfaces, with Mechanical Stillness enforced as the default safe state.

Core Architecture

- **P Layer — Sensing & Voxelization:** Utilizes 905 nm LiDAR with a 96-cell voxel grid to generate anonymized Center of Mass velocity vectors under the 3ZEROS™ Protocol (Zero Camera, Zero Audio, Zero Cloud). Output is limited to pure kinematic vectors only.
- **N Layer — Deterministic Deliberation Pipeline:** Operates on a single 1 kHz hardware clock domain with no asynchronous safety-critical paths. Pipeline stages include input processing, the Sacred Pause™ cognitive forcing function (25–1000 ms hardware timing), tripartite .1x Key™ authentication (simultaneous iris, cryptographic token, and kinetic pedal), safety kernel enforcement (±0.05 mm limit), FSM deterministic state machine, hardware output gate, and default safe state.
- **D Layer — Absolute Architectural Separation:** Operates between non-deterministic AI inference and physical effectors, primarily protecting high-stakes domains like defence, cyber-physical command, and eldercare resilience.
- **Immutable Accountability:** The Enhanced WD117 ledger provides hardware-enforced immutability through SHA-3-512 hashing, post-quantum signatures, A10a hardware sealing, WORM memory commit, and OTP fuse finality. Once an entry passes OTP fuse finality, modification is architecturally prevented by the physical properties of the storage medium.

Key Innovations

The architecture synthesizes established engineering practices — deterministic FPGA-based real-time control, hardware security modules, fail-safe state machines, and air-gapped enclosures — with targeted innovations: integration of privacy-by-physics (3ZEROS™) with hardware deliberation gating and immutable ledger finality in a single terminal appliance; concurrent tripartite hardware authentication as a unified gate rather than layered software checks; and hardware as the primary enforcement layer for constitutional mandates (P-LIFE 1.00™) under a non-agentic model where AI observes and reports only while humans execute.

Significance

The A12 represents a hardware-enforced last mile for Zero Preventable Deaths objectives within sovereign, culturally aligned non-agentic AI governance frameworks. Safety-critical authorization and enforcement functions are placed in dedicated hardware to reduce dependence on software correctness, aligning with fail-safe principles in IEC 61508 and deterministic real-time embedded practice. The design is intended to eliminate software bypass pathways for consequential actions while maintaining operational viability across clinical, humanitarian, and deep-space environments. All functional safety, immutability, and compliance claims remain subject to formal verification, testing, and regulatory assessment.

The integration of the A12 [P+N+D] ensures a Sovereign-In-The-Loop (SITL) control model that protects the "Humanitarian Shield." By anchoring the architecture in deterministic silicon rather than probabilistic code, the system achieves the 2027 Deterministic Horizon, providing absolute safety and accountability in clinical care.

10 Safety Component Doctrine Matrix

COMPONENT	HARDWARE LAYER	MECHANISM OF ACTION	FAILURE MODE	FORENSIC / LEGAL DOCTRINE	TARGET APPLICATION
Sacred Pause™ Command Gate	P / N Layers · A12	Hardware-timed deliberation window (25–1000 ms) enforced by silicon counters, FPGA gates, and master clocks; interposes a refusal layer between inference and action.	Break-by-default; returns system to mechanical stillness.	Physics of Refusal; P-LIFE 1.00™ (Doctrine of Stillness / Humility).	Critical infrastructure, defense, deep space, eldercare (HSA Class B/C/D).
Tripartite Latch	A12 Terminal Core · D-Layer	Concurrent multi-factor human authorization: Iris Scan (biometric), Crypto Token, Kinetic Pedal/Button. No command exits the enclosure without verified human commitment.	Brake-by-default; absence of any factor prevents kinetic execution; Fail-Loud alarm on compromise.	Sovereign-In-The-Loop (SITL); Human Authority Mathematically Verified.	Eldercare clinical facilities, defense command systems, autonomous platform interlocks.
WD117 Enhanced Ledger	D / N / Forensic Layers	WORM memory using OTP silicon fuses and SHA-3-512 signatures; permanent, unalterable record of all events, hashes, and human-authorized actions.	Fail-Loud; ledger failure or heartbeat interruption asserts the Sovereign Brake and triggers local alarms.	Forensic Finality; Honest Annotation to the Record.	Regulatory auditing, clinical accountability, critical infrastructure.
Sovereign Brake™ / Power-Cut Relay	Stratum 4 / D-Layer · A12	Physical LDO power severance (< 1.05 ms) or galvanic isolation triggered by anomalies or tamper detection.	Fail-safe / Brake-by-Default; inert state with no motion and no harm.	Inaction-as-Safe-Default; Fail-Loud Doctrine; Human Sovereignty Enforcement.	Eldercare monitoring, clinical monitoring, autonomous platform interlocks.

A7 Bridge	Boundary / Ingress Layer	Agentic Drift Screening: confidence scoring, contradiction detection, signal normalization. Structural firewall converting non- deterministic advisory data into deterministic packets; denies actuation rights.	Drift or anomaly → data discarded; system maintains mechanical stillness.	Advisory-Only Constraint; Zero- Agentic Enforcement.	Critical infrastructure, healthcare, hospital IT network buffering.
3ZEROS™ Protocol	P-Layer (Perception)	Hardware-level removal of Camera, Audio, and Cloud connectivity; voxelization of LiDAR data. Spatial tracking without identity.	Mechanical stillness and data severance on any sensing anomaly.	Privacy-by-Physics (Dignity enforced by hardware, not policy).	Eldercare (B1).
A11 Jupiter Enclosure	Perimeter / Hardened Bridge	53-minute temporal air-gap enforced by hardware; renders real-time remote cyber-attacks physically impossible by negating time-to-impact.	Defaults to inaction if the temporal window is compromised or bypassed.	Temporal Air-Gap; conversion of cyber-security into physical sovereignty.	Deep-space research and high-security terrestrial clinical estates.
Heartbeat Monitor	Isolated ledger / sensing link	Continuous physical hardware heartbeat; sensing of network connectivity or communication severance.	Fail-Loud; triggers localized non- networked physical alarm.	Fail-Loud Doctrine.	Eldercare facilities (monitoring apparatuses).
A12 [P+N+D] Core	P+N+D Layers	Sacred Pause (25–1000 ms) and Tripartite Latch mechanisms; hardware-timed deliberation gates ensuring human sovereignty over kinetic commands.	Break-by-default (inert state).	Protective Asymmetry.	Critical Infrastructure / Healthcare.

11 Conclusion: The 2027 Deterministic Horizon

The NAIGE framework represents a fundamental shift in the AI paradigm: moving AI from an unpredictable agent to a strictly governed advisory tool. By anchoring governance in deterministic silicon, we reach the "2027 Deterministic Horizon," where absolute clinical safety and forensic finality are mathematical certainties.

Target Clinical Safety Metrics

DETERMINISTIC RESOLUTION 1.0 ms	KINETIC RESPONSE < 1.05 ms sovereign engagement	HARDWARE TRAJECTORY ENFORCEMENT 100% – no bypass
ELDER DIGNITY SCORE > 8.9 / 10	DATA INTEGRITY SEAL SHA-3-512 + Post- Quantum WORM	SAFE DEFAULT P-LIFE 1.00™ stillness

The A12 [P+N+D] system utilizes a synchronous deliberation pipeline driven by a 1 kHz hardware master clock to maintain 1 ms deterministic oversight. By integrating physical power severance via the U7 One-Shot sequencer and cryptographic forensic finality through the Enhanced WD117 Ledger, the architecture establishes an "Immutable Kinetic Capstone." Human authority remains mathematically verifiable, transforming AI from an unpredictable agent into an observable, strictly governed tool within high-stakes clinical settings.

Integrated Citation Register

Primary Citation — This Publication

Koh, Edwin W. K. (2026). *Immutable™ Hardware-Enforced Non-Agentive AI Governance Architecture – NAI 4.0™*. WISL™ Ebook Series No. 70, 71, 72 & 73 – Integrated ISBN Edition. Non-Agentive AI Governance Singapore (ACRA T260229801). Patent SG020603109STW. NLB Legal Deposit Vault R260219-005 / R260302-007. Available at: <https://kohedwin.ai> | <https://non-agentive.ai>

Patent Basis

- SG020603109STW – Parent Patent (constitutional core)
- 10202600902P – ABC+2S+H™ Guardian Framework
- 10202602021T – A10a Deterministic Governance Platform
- 10202602023X – A12 Deterministic Black Box
- 10202602213U – A7 Bridge Layer Translation Hub
- 10202602223T – A(12) P+N Enhanced WD117 Immutable Ledger
- 10202602225P – A8 Bridged Layer 8 Sovereign Deployment Governance Layer
- 10202602270V – Non-B1 Clinical Advisory Monitoring Shell

NLB Legal Deposit

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

Academic Background — Edwin Koh W. K.

- MBA — General and Strategic Management — Maastricht School of Management
- BSc — Industrial and Systems Engineering — University of Florida
- Independent Researcher — OCA Designation — 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.sg

NLB Legal Deposit R260219-005 / R260302-007

We Innovate Save Lives™ · We Go Global™