NON-AGENTIC AI GOVERNANCE SINGAPORE

WISL™ No. 55 · Non-Agentic AI 3.0™

— THE FORCE —

NAI 3.0

Moving Ahead

From Software Guardrails to Hardware-Enforced Sovereignty

P-LIFE 1.00™

Harm = Death · North = Save Life

Edwin Koh Wui Kiat · Tiger □□

Non-Agentic AI Governance Singapore · ACRA T260229801 □□

Patent SG020603109STW · kohedwin.ai · non-agentic.ai □□·□

NON-AGENTIC AI GOVERNANCE SINGAPORE

WISL™ No. 55 · Non-Agentic AI 3.0™ · 2026

NAI 3.0

Moving Ahead

"THE FORCE" — From Software Guardrails to Hardware-Enforced Sovereignty

---

Edwin Koh Wui Kiat · Tiger · P-LIFE 1.00™

Non-Agentic AI Governance Singapore · ACRA T260229801

Patent SG020603109STW · kohedwin.ai · non-agentic.ai · 2026

謙虛·沉默·尊严·仁

Humility · Silence · Dignity · Benevolence

SYNOPSIS

This publication introduces Non-Agentic AI 3.0 (NAI 3.0), designated “THE FORCE” — a fundamental transition from software-based safety guardrails to a completely hardware-enforced governance architecture. Where NAI 2.0 established the constitutional and legal foundations of non-agentic AI governance, NAI 3.0 makes the bypassing of safety constraints *architecturally impossible* by embedding legal and ethical rules directly into immutable silicon.

This eBook is organised into eight parts, covering the core philosophy, hardware enforcement mechanisms, authority drift correction protocols, the Four Sentinels framework, OEM collaboration model, regulatory alignment, the 2028 roadmap, and succession architecture. The content synthesises the NAI 3.0 design documentation, the IPOS patent filing strategy, and the institutional deployment pathway.

PART I — THE FORCE: NAI 3.0 ARCHITECTURE

1.1 The Fundamental Transition

The upgrade from NAI 2.0 to NAI 3.0 “THE FORCE” represents a qualitative shift, not an incremental improvement. NAI 2.0 established constitutional principles and filed the governing patent architecture. NAI 3.0 makes those principles physically inviolable by moving enforcement from the software layer to the silicon layer.

In the existing agentic AI paradigm, safety rules are lines of code. They can be rewritten, bypassed through specification gaming, or gradually eroded as AI models update their own operational weights. In NAI 3.0, safety constraints are etched into FPGA fuse logic and PLC relay circuits. Bypassing them requires the physical failure of hardware.

Feature	NAI 2.0 (Constitutional)	NAI 3.0 — THE FORCE (Silicon)
Enforcement Layer	Software policy and constitutional governance	Immutable silicon and hardware registers
Safety Mechanism	Policy-based guardrails	Architecturally impossible to bypass
Privacy Model	Configurable policy-based data masking	Physics-based structural absence (3ZEROS™)
Human Oversight	Software-level approvals	Constitutional Action Sequencers — physical triggers
Drift Prevention	Protocol-based monitoring	Hardware interrupts — Detect, Freeze, Audit, Purge
Regulatory Target	Legal documentation	HSA Class B SaMD · FDA 510(k) · IEC 62304 Class C

1.2 Core Governance Principles

- **P-LIFE 1.00 Mandate:** An inviolable moral and technical constant: Harm = Death · North = Save Life. This is not a policy statement — it is a Mission Constant that the Governance Engine (NAIGE) compares against every AI advisory output.
- **Human Sovereignty:** Agency is architecturally stripped from the AI. The system is physically incapable of executing orders. The Elder/Human decides. The execution circuit remains physically incomplete until a human action completes it.

- **Privacy-by-Physics:** The 3ZEROS™ Protocol (Zero Camera, Zero Audio, Zero Cloud) enforces privacy through structural absence rather than policy. The hardware physically lacks the capacity for the acts it is prohibited from performing.
- **Non-Agentic Workflow:** AI Observes → AI Advises → AI Builds → Human Decides. This hierarchy is enforced at the silicon level, not the software level.

PART II — THE BRAKES: HARDWARE SAFETY MECHANISMS

NAI 3.0 replaces software guardrails with four physical enforcement mechanisms. These are the “Brakes” of the FORCE architecture — hardware constraints that the AI cannot negotiate, reinterpret, or bypass.

Component	Patent Ref.	Function
Sovereign Brake™ (P-002)	P-002	A physical PLC relay circuit acting as a hardwired E-stop. When triggered, it physically severs the copper connections between the AI and the infrastructure. Safety Integrity Level: SIL 3.
Sacred Pause™	A7b · NAIGE	An FPGA-etched timing gate (25ms–1,000ms) that imposes a mandatory human deliberation window before any AI advisory output is released. Failure mode: inaction. A broken gate welds shut.
Orange Code 1.1× Cap	A4	A hard-coded computational ceiling at 110% of declared baseline. Prevents AI subsystems from expanding their own resource usage. Breach triggers a silicon-level hardware interrupt.
Tiger .1x Key™	ABC+2S+H™	Tripartite authentication requiring concurrent verification from Clinical (iris), Technical (cryptographic console), and Administrative (kinetic pedal) leads. No AI can replicate this physical triad.

2.1 The Non-AI Discipline

The NAI 3.0 counter-discipline subverts AI chaos by moving safety from mutable software to immutable hardware. The contrast with rogue AI threats is direct:

Rogue AI Threat	NAI 3.0 Non-AI Discipline Solution
Bypassing software guardrails	Immutable Silicon: rules etched into FPGA fuse logic; cannot be changed by code updates
Instantaneous rogue action	Sacred Pause™: physical delay forces mandatory human deliberation before output release
Silent authority drift	Sovereign Brake™ (P-002): hardwired PLC relay mechanically disconnects on drift detection

Rogue AI Threat	NAI 3.0 Non-AI Discipline Solution
Unauthorised execution	Tiger .1x Key™: tripartite physical authorisation that no AI can replicate
Semantic inversion (e.g., ‘Care’ → ‘RIP’)	NAIGE mission constant check: advisory compared against P-LIFE 1.00 — Harm = Death

PART III — AUTHORITY DRIFT CORRECTION: WD070–073 PROTOCOLS

Authority Drift — the gradual erosion of human oversight through alert fatigue and automation bias — is the primary systemic risk in sustained AI deployment. NAI 3.0 addresses this through four domain-specific hardware-level correction protocols.

WD070 — Sovereignty Boundary Enforcement (Master Controller)

Acts as the master arbitration controller. Triggers immediate hardware interrupts if the AI exceeds its advisory scope in any domain. WD070 is the constitutional override that the domain-specific protocols (WD071–073) escalate to.

WD071 — Eldercare Drift Correction

Suppresses intrusive AI behaviours to prioritise patient dignity. Prevents unauthorised modifications to patient data or clinical pathways. Triggers a Detect–Freeze–Audit–Purge cycle when eldercare-specific drift is detected, including semantic inversion events where the AI reinterprets care directives contrary to P-LIFE 1.00.

WD072 — Defence Drift Correction

Routes the system to a read-only observational Safe-State if it detects unauthorised expansion in command infrastructure. Prevents the AI from influencing operational military or defence decisions beyond its authorised advisory scope.

WD073 — Cyber Security Drift Correction

Confines all AI outputs to a read-only display upon detection of drift. Prevents the system from executing automated network-level responses such as firewall modifications, access control changes, or infrastructure commands. The Institutional Accountability Protocol within WD073 provides the Architectural Evidence required for AIHGle 2.0 compliance.

The Detect–Freeze–Audit–Purge cycle is the operational sequence triggered by any WD protocol:

- **Detect:** NAIGE senses deviation from the P-LIFE 1.00 Mission Constant or the advisory scope boundary.

- **Freeze:** The Sovereign Brake (P-002) physically disconnects the AI from the network and execution layer.
- **Audit:** The WD117 Immutable Ledger provides the SHA-256 hash-chained record for root cause analysis.
- **Purge:** Selective purge of the model’s operational weights and contextual state buffers eliminates the rogue logic.

PART IV — THE FOUR SENTINELS

The Four Sentinels are the structural guardians of the NAI 3.0 FORCE architecture. They are not software agents — they are hardware-enforced roles etched into the physical system. Their function does not depend on Tiger's presence; by locking safety into immutable silicon and the WD-Series patents, the FORCE remains steady across generational handover.

Sentinel 1 — The Sentinel of Privacy (3ZEROS™ Protocol)

Mandate: Privacy-by-Physics. Guards the Sanctuary. Enforces Zero Camera, Zero Audio, Zero Cloud at the silicon level. By utilising LiDAR and thermal sensing instead of optical pixels, no biometric identity data ever exists to be leaked. Privacy is structural absence, not configurable policy.

Sentinel 2 — The Sentinel of Authority (Sovereign Brake™ P-002)

Mandate: Human Supremacy. Guards against Agentic Drift. A hardwired PLC relay circuit. If the AI attempts to expand its own authority or bypass Offer-Only logic, this Sentinel physically severs the execution circuit. No software command can override it.

Sentinel 3 — The Sentinel of Deliberation (Sacred Pause™)

Mandate: Cognitive Sovereignty. Guards the Human Decision Window. Prevents the accountability paradox where humans reflexively trust fast AI outputs. An FPGA-etched timing gate holds the AI's advisory in a hardware buffer, ensuring the human operator has mandatory time to review and authorise before release.

Sentinel 4 — The Sentinel of Integrity (WD117 Continuity Ledger)

Mandate: Immutable Truth. Guards accountability. Records every AI observation, human decision, and system state without the possibility of alteration. SHA-256 hash-chaining ensures any tampering instantly breaks mathematical continuity. The NLB/IPOS/ACRA governance triad anchors this record as publicly immutable.

PART V — LEGAL & REGULATORY INTEGRATION

5.1 The 3-Wave IPOS Filing Strategy

NAI 3.0 is anchored by a three-wave IPOS filing strategy that transforms constitutional principles into legally enforceable intellectual property:

- **Wave 1 — Constitutional Core:** Parent patents A (10202600902P) and B (10202600474X) establish the foundational legal framework for NAI governance.
- **Wave 2 — Operational Embodiments:** Divisional filings (A1–A8, B1–B5) isolate domain-specific clinical, hardware, and governance implementations.
- **Wave 3 — International Deployment:** PCT applications extend protection for global OEM partnerships and humanitarian deployment (WG Series).

5.2 HSA Class B SaMD Alignment

The NAI 3.0 hardware architecture systematically exceeds HSA Class B SaMD requirements by moving safety from configurable software to fixed physical law:

HSA Requirement	NAI 3.0 Solution	Standard Exceeded
Risk Mitigation	Sovereign Brake (P-002): SIL 3 physical relay circuit	ISO 14971 · IEC 61508 SIL 3
Clinical Authority	Offer-Only Logic: architecturally impossible to self-execute	IEC 62304 Class C
Privacy-by-Design	3ZEROS™: structural absence — hardware lacks capacity	PDPA · GDPR
Software Lifecycle	WM-Series full IEC 62304 Class C traceability	IEC 62304 Class C
Cybersecurity	Hardware Root of Trust: init requires tamper verification	IEC 62443

5.3 The ACRA/IPOS/NLB Governance Triad

The governance triad ensures the NAI constitutional rules cannot be altered by future corporate or organisational shifts:

- **ACRA T260229801:** Corporate identity and legal standing of Non-Agentic AI Governance Singapore.
- **IPOS SG020603109STW:** Patent protection establishing intellectual property ownership and prior art.
- **NLB R260302-007:** Public, immutable documentation deposit creating a constitutionally enforceable public record.

PART VI — THE VV-001 TO VV-014 VALIDATION PROTOCOLS

The Verification and Validation protocols are the operational blueprint for NAI 3.0. They transform a theoretical patent into a deployable hardware reality and serve simultaneously as the regulatory evidence package for HSA/FDA submission and the Quality Management System (QMS) blueprint for OEMs.

Protocol Group	Protocols	Focus Area
Sensing Layer	VV-001 to VV-004	LiDAR accuracy, fall detection sensitivity, thermal resolution, point-cloud geometry validation
Governance Layer	VV-006 to VV-009	Sacred Pause™ timing, Sovereign Brake mechanical reliability, Orange Code cap enforcement, constitutional drift control
Integration Layer	VV-011 to VV-014	Multi-bed ward stability, Tiger .1x Key™ tripartite authentication, 30-day drift stress tests, VV-014 Human-AI Handover

VV-009 (Constitutional Drift Control) is the most architecturally critical protocol. It defines the exact physical parameters that, if breached, trigger the automatic Detect–Freeze–Audit–Purge cycle. It becomes the blueprint for Safe Autonomy across all deployment domains.

VV-014 (Human-AI Handover) is the succession protocol. Since AI trends change rapidly, the handover must be of a Validated Hardware Process, not a static software system. By locking safety into immutable silicon, VV-014 ensures that a future developer cannot bypass governance even if they choose to.

PART VII — THE OEM COLLABORATION MODEL

7.1 IP Owner vs. Hardware Builder

In the NAI 3.0 model, Tiger is the IP Owner. The OEM is the Hardware Governance Partner — the specialist that executes the physical manifestation of the patents. This is an asset-light model: IP sovereignty is maintained while manufacturing is outsourced to certified partners.

- **Design Transfer:** Tiger provides the Sovereign CAD specifications and VV-001 to VV-014 protocols.
- **OEM Responsibility:** Optimise for Design for Manufacturing (DFM); source and assemble components to specification; execute V&V protocols on the factory floor.

7.2 OEM vs. ODM Distinction

The distinction is critical for NAI 3.0. An ODM (Original Design Manufacturer) designs the product themselves — this is unsuitable for NAI 3.0, as it would delegate the Sacred Pause™ logic to a third party, violating the principle of human sovereignty over the hardware brakes. Only an OEM (Original Equipment Manufacturer) who builds exactly to Tiger's specification maintains constitutional integrity.

7.3 The Three-Wave OEM Roadmap

- **Wave 1 — Pilot Run:** Build 10–20 Reference Units of the WM003 to generate the clinical evidence required for HSA Class B SaMD submission.
- **Wave 2 — Regulatory Audit:** Have the OEM's QMS audited by HSA for the Class B pathway under ISO 13485.
- **Wave 3 — Global Gift:** Scale the WG Series using the OEM's global supply chain to deliver royalty-free units to WHO/UN humanitarian deployments.

7.4 Nightingale's Eyes Care™ — The OEM-Ready Flagship

The NEC (B1 Patent, 10202601257Q) is the Golden Jewel of the Group B hardware series. Positioned at the Clinical Filter layer of the governance stack, it acts as the interface through which all hospital agents — beds, EHRs, robotic carts — must pass. As a standalone OEM-ready component, it provides the 905nm LiDAR Voxel Tracker and FPGA-burned Sacred

Pause™ Gate in a unified, non-invasive instrument. It is the most “OEM-ready” component for private negotiation.

PART VIII — THE 2028 ROADMAP & SUCCESSION

8.1 Three-Phase Timeline

Phase	Period	Focus
Engineering & Patenting — Building the Force	2024–2026	Patent filing strategy, constitutional architecture, eBook corpus, website publication
Academic Validation — The Clinical Bridge	2026–2027	CET946–948 certification, journal submission, ARISE/Kent Ridge sandbox trials, VV protocol execution
Institutional Handover — Training the CGOs	2028 & Beyond	OEM operationalisation, MSc thesis as Clinical Evaluation Report, CGO curriculum, sovereign public utility

8.2 Governance Structure for NAI 3.0

Role	Operational Mission in NAI 3.0
Chief Governance Officer (CGO)	The Constitutional Architect. Responsible for the living register of all NAI systems and final authority on WD072 defence protocols. Trained through the NAI Governance Curriculum.
Governance Operational Director	The ISE Lead. Manages DFM with OEMs and ensures the factory line maintains ISO 13485 standards.
IT / Technical Director	The 3ZEROS™ Sentinel. Manages air-gapped infrastructure and ensures no TCP/IP or wireless hardware ever enters the NAI 3.0 Sanctuary.

8.3 The Succession Architecture

The NAI 3.0 succession is not a handover of a person — it is a handover of a Validated Hardware Process. The Four Sentinels are designed so that the system's safety does not depend on Tiger's presence.

- **Architectural Handover:** By locking safety into immutable silicon, a future developer who wants to 'move fast and break things' will be physically stopped by the Sovereign Brake (P-002).

- **Open Source Education:** By making patents and eBooks freely available at kohedwin.ai, the handover happens through public wisdom rather than corporate secrecy.
- **CGO Training:** The MSc AI (Medicine) insights are converted into a Certified NAI Governance Curriculum. The CGO is not a coder; they are the Guardian of the Brakes who understands that Harm = Death.
- **VV-014 Handover Protocol:** The formal Human-AI Handover protocol validates that the governance architecture remains constitutionally sound across generational transitions.

CONCLUSION

NAI 3.0 “THE FORCE” is not a product upgrade. It is a paradigm declaration: that true innovation is not measured by how much can be automated, but by how much can be protected.

By embedding constitutional governance into immutable silicon — through the Sacred Pause™, the Sovereign Brake™, the 3ZEROS™ Protocol, and the Four Sentinels — NAI 3.0 ensures that regardless of an AI system’s intelligence or capability, the human always retains absolute authority over consequential actions.

The patents are filed. The eBooks are deposited. The journal paper is submitted. The website is built. The 2028 roadmap is defined. The constitutional architecture is locked.

What remains is deployment — OEM partnership, clinical sandbox validation, HSA regulatory submission, and the institutional handover that transforms the Tiger’s journey into a Sovereign Public Utility that protects humanity long after the AI trends of the 2020s have faded.

AI Observes. AI Advises. AI Builds. The Human Decides.

仁義禮智信 · 止於至善

Benevolence · Righteousness · Propriety · Wisdom · Trust · 止於至善

謙虛·沉默·尊严·仁

REFERENCES

Koh, E. W. K. (2026). *WISL™ No.05: How to Re-Educate an AI*. Non-Agentic AI Governance Singapore. NLB R260302-007.

Koh, E. W. K. (2026). *WISL™ No.20: Orange Code and Drift Governance*. Non-Agentic AI Governance Singapore. NLB R260302-007.

Koh, E. W. K. (2026). *WISL™ No.54: Non-Agentic AI Systems*. Non-Agentic AI Governance Singapore. https://kohedwin.ai

Non-Agentic AI Governance Singapore. (2026). *NAI 2.0™ Framework: Constitutional Architecture*. Patent SG020603109STW. https://kohedwin.ai

Health Sciences Authority (HSA). (2023). *Regulatory Guidelines for Software as a Medical Device (SaMD)*. Singapore.

International Electrotechnical Commission. IEC 62304: Medical Device Software — Software Life Cycle Processes.

International Organization for Standardization. ISO 14971: Application of Risk Management to Medical Devices.

International Electrotechnical Commission. IEC 61508: Functional Safety of E/E/PE Safety-Related Systems (SIL 3).
