UNITED STATES NONPROVISIONAL UTILITY PATENT APPLICATION

TITLE OF THE INVENTION

CONSTITUTIONAL HARDWARE ENFORCEMENT ARCHITECTURE FOR NON-AGENTIC ARTIFICIAL INTELLIGENCE GOVERNANCE (Patent M / A13naige – Supreme Guardian Master Control Layer)

Inventor: Koh Wui Kiat, Edwin

ISBN: 978-981-17970-5-7

Applicant: Koh Wui Kiat, Edwin

Correspondence address: Blk 54, #06-3593, Geylang Bahru, Singapore 330054.

Residence / citizenship: Singapore / Singapore

Entity status: Small Entity

Related Application: This application claims priority under 35 U.S.C. § 119(a)–(d) to Singapore Patent Application No. 10202602156U, entitled “Integrated Deterministic Non-Agentic Governance Core for Clinical Eldercare Applications,” filed 24 June 2026.

Related foreign applications: This application claims priority to and incorporates by reference the following applications filed with the Intellectual Property Office of Singapore (IPOS): - Singapore Patent Application No. SG020603109STW, filed 5 February 2026; - Singapore Patent Application No. 10202600474X, entitled “Non-Agentic AI Governance Singapore,” filed 16 February 2026; - Singapore Patent Application No. 10202600902P, entitled “ABC+2S+H Guardian Framework,” filed 23 March 2026; and - Singapore Patent Application No. 10202602156U, entitled “Integrated Deterministic Non-Agentic Governance Core for Clinical Eldercare Applications,” filed 24 June 2026; each incorporated herein by reference in its entirety. The verified official filing dates, titles, applicants, inventors, and the specific 35 U.S.C. § 119/§ 120 benefit or priority basis for each related application are set forth in the Application Data Sheet.

This application is filed as a national U.S. nonprovisional utility application and not under the Patent Cooperation Treaty (PCT). STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT Not applicable. No United States government funding or contract rights apply. THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT Not applicable. INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ELECTRONICALLY Not applicable. No sequence listing, large table, or computer program listing is incorporated by reference in this application.

The verified official filing dates, titles, applicants, inventors, and the specific 35 U.S.C. § 119/§ 120 benefit or priority basis for each related application are set forth in the Application Data Sheet.

This application is filed as a national U.S. nonprovisional utility application and not under the Patent Cooperation Treaty (PCT).

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not applicable. No United States government funding or contract rights apply.

THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT

Not applicable.

INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ELECTRONICALLY

Not applicable. No sequence listing, large table, or computer program listing is incorporated by reference in this application.

TITLE OF THE INVENTION

The disclosure relates to computer architecture, programmable logic, functional safety, medical and cyber-physical systems, privacy-preserving sensing, human-machine authorization, immutable event recording, and governance of artificial-intelligence systems. More particularly, the disclosure relates to a deterministic hardware appliance and associated methods that interpose a physically enforced governance boundary between a non-deterministic artificial-intelligence advisory system and one or more physical or consequential outputs, including clinical robotics, mobility enclosures, and sensing limbs.

The present application describes the Kinetic Capstone of this architecture (referred to herein as Patent M or A13nAIGE), in which the A13 execution-governance core is fully realized through an integrated P+N+D hardware stack and A13a, A13b, and A13c embodiments.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not applicable.

THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT

Not applicable.

INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ELECTRONICALLY

Not applicable. No sequence listing, large table, or computer-program listing is incorporated by reference in this template.

FIELD OF THE INVENTION

The disclosure relates to computer architecture, programmable logic, functional safety, medical and cyber-physical systems, privacy-preserving sensing, human-machine authorization, immutable event recording, and governance of artificial-intelligence systems. More particularly, the disclosure relates to a deterministic hardware appliance and associated methods that interpose a physically enforced governance boundary between a non-deterministic artificial-intelligence advisory system and one or more physical or consequential outputs, including clinical robotics, mobility enclosures, and sensing limbs.

The present application describes the Kinetic Capstone of this architecture (referred to herein as Patent M or A13nAIGE), in which the A13 execution-governance core is fully realized through an integrated P+N+D hardware stack and A13a, A13b, and A13c embodiments.

BACKGROUND OF THE INVENTION

Artificial-intelligence systems, including large language models, machine-learning controllers, diagnostic models, and probabilistic decision systems, may generate useful recommendations while remaining non-deterministic. Conventional governance approaches rely predominantly on software alignment, filtering, retrieval-augmented generation, permissions, moderation, policy guardrails, red-team testing, and emergency-stop commands. Such measures may reduce risk but remain susceptible to software defects, privilege escalation, compromised dependencies, time-of-check to time-of-use divergence, semantic ambiguity, model drift, network compromise, and bypass of software-enforced restrictions.

In clinical robotics, mobility systems, eldercare monitoring, industrial control, defense, aerospace, remote operations, and other high-stakes environments, an erroneous or maliciously altered recommendation may lead to irreversible consequences. There is a need for an architecture in which an artificial-intelligence system remains advisory, physical authority is withheld by default, human commitment is required for consequential

action, privacy boundaries are enforced at sensing hardware, and governed events are recorded in a tamper-resistant manner.

There is also a need to translate probabilistic machine output into bounded deterministic packets, reject anomalous or contradictory proposals before they reach an actuator, provide an unavoidable deliberation interval, select embodiment-appropriate stopping behavior, and maintain a forensic record that cannot be rewritten or used as a return command path.

SUMMARY OF THE INVENTION

The disclosed architecture implements a non-agentic inversion in which intelligence proposes, deterministic hardware governs, a human authorizes, a bounded execution interface acts, and an immutable ledger records. An advisory processor is assigned advisory-only rights and is physically or logically separated from an execution stratum. An A7 controlled ingress bridge receives a proposal, performs or invokes validation and translation, and forwards an accepted deterministic packet to an N12 deterministic screening kernel and an A12 hardware governance core.

The hardware governance core may include a privacy layer, a deterministic deliberation layer, and a forensic/fail-safe layer. A nominal 1 kHz master clock provides a 1.0 ms supervisory cycle. A hardware timer enforces a selectable deliberation interval of 25 ms to 1000 ms inclusive, independently of advisory-software scheduling. A Tripartite human-authorization gate may require biological identity, cryptographic or possession-based authority, and kinetic confirmation before output is enabled.

A privacy-preserving embodiment uses a 905 nm non-imaging LiDAR sensor and node-local FPGA or FPPA voxelization to produce a 96-cell occupancy representation and anonymized center-of-mass vectors. Raw point-cloud data terminates at a silicon privacy boundary. A fail-safe U7 sequencer independently removes, isolates, holds, or controls actuator energy. A design requirement may specify power severance in less than 1.05 ms from a validated trigger point TP-A to an actuator-rail isolation point TP-B; the 1.0 ms supervisory cycle is a distinct quantity.

A WD117 forensic ledger cryptographically chains events using SHA-3-512, obtains attestation from an A10a hardware root of trust, and stores records in WORM memory and/or one-time-programmable fuse storage. The ledger has no actuator-command return path. The default condition is P-LIFE 1.00 mechanical stillness or another embodiment-appropriate safe state.

ADVANTAGES

- Prevents a non-deterministic AI proposal from directly actuating a physical system.
- Creates an inspectable boundary between advisory inference and execution.
- Forces a non-bypassable hardware deliberation interval.
- Requires independent human-originated authorization factors.
- Prevents raw identifiable sensing data from leaving a privacy-preserving sensing node.
- Provides deterministic rejection to stillness when uncertainty or faults arise.
- Provides embodiment-specific energy-control responses.
- Creates an append-only or write-once forensic record independent of the advisory AI.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an overall constitutional hardware-enforcement architecture separating an advisory stratum from a deterministic execution stratum.

FIG. 2 illustrates an exploded P/N/D deterministic appliance including an outer enclosure, privacy layer, deterministic layer, forensic layer, root of trust, and power/safety compartment.

FIG. 3 illustrates an A7 controlled ingress bridge and N12 deterministic drift-screening pipeline.

FIG. 4 illustrates a privacy-by-physics sensing node with 905 nm LiDAR, node-local voxelization, a 96-cell grid, and a silicon privacy wall.

FIG. 5 illustrates a synchronous hardware-timed deliberation pipeline and timing diagram.

FIG. 6 illustrates a Tripartite human-authorization gate with biological, cryptographic, and kinetic factors.

FIG. 7 illustrates a U7 fail-safe energy-control sequencer and embodiment-specific stopping responses.

FIG. 8 illustrates a WD117 immutable forensic ledger, SHA-3-512 chain, A10a root of trust, WORM memory, and OTP fuse finality.

FIG. 9 illustrates a comparison of observational P+N and kinetic P+N+D architectures.

FIG. 10 illustrates an A13 embodiment family including mobility, sensing, and clinical robotic embodiments.

FIG. 11 illustrates a pre-deployment validation and measurement arrangement.

FIG. 12 illustrates a complete system state machine including nominal, failure, safe-state, and re-arm transitions.

The drawings are schematic and not necessarily to scale. Like reference numerals identify like or corresponding elements.

REFERENCE NUMERAL SCHEDULE

Numeral	Element
100	overall architecture
110	AI advisory processor
120	advisory stratum
130	proposal data
140	execution stratum
150	consequential output
200	A7 controlled ingress bridge
210	ingress interface
220	N12 screening kernel
230	deterministic packet
240	reject-to-stillness path
300	A12 deterministic core
310	privacy layer
320	master clock
322	hardware timer/counter
330	deterministic layer
340	hardware-timed deliberation gate
350	safety FSM/KCL
360	deterministic output gate
370	forensic/fail-safe layer

400	human authorization gate
410	biological identity input
420	cryptographic authority input
430	kinetic confirmation input
440	authorization-valid signal
500	A13 embodiment router
510	A13a mobility embodiment
520	A13b sensing embodiment
530	A13c clinical robotic embodiment
540	actuator/output
550	bounded motion envelope
600	U7 fail-safe sequencer
610	hardware fault trigger
620	power isolator
630	actuator rail
640	safe-state holding mechanism
700	WD117 forensic ledger
710	event input
720	SHA-3-512 chaining circuit
730	A10a root of trust
740	WORM memory
750	OTP fuse bank
760	one-way boundary

800	privacy-preserving sensing node
810	905 nm LiDAR
820	raw point cloud
830	voxelization engine
840	96-cell occupancy grid
850	silicon privacy wall
860	anonymized CoM output
900	human operator
910	nurse annunciator
920	isolated alert cable
930	facility IT boundary
940	local fail-loud alarm
1000	compute limiter
1010	1.1x cap circuit
1100	mobility chassis
1110	wheel module
1120	seat/enclosure
1130	controlled deceleration
1200	robotic-arm base
1210	arm joint
1220	end effector
1230	encoder
1240	positional envelope

1300	validation bench
1310	oscilloscope
1320	continuity meter
1330	cryptographic verifier
1340	network tester
1350	TP-A
1360	TP-B

DETAILED DESCRIPTION OF THE INVENTION

Overall Architecture

Referring to FIG. 1, an overall architecture 100 includes an AI advisory processor 110 within an advisory stratum 120. The processor 110 generates proposal data 130 but has no direct actuation rights. The proposal data 130 enters an A7 controlled ingress bridge 200 through an ingress interface 210. An N12 deterministic screening kernel 220 applies predetermined checks and either produces a deterministic packet 230 or routes the proposal to a reject-to-stillness path 240.

The deterministic packet 230 enters an A12 deterministic core 300 in an execution stratum 140. The core 300 withholds output during a hardware-timed deliberation interval, receives an authorization-valid signal 440 from a human authorization gate 400, verifies safety conditions using a finite-state machine or kinematic-constraint layer 350, and enables a deterministic output gate 360 only when all required conditions are true. The output gate 360 provides a bounded signal to an A13 router 500 and a consequential output 150.

P/N/D Deterministic Appliance

Referring to FIG. 2, the A12 core 300 may be housed in a tamper-evident enclosure having a privacy layer 310, a deterministic layer 330, a forensic/fail-safe layer 370, an A10a root of trust 730, and a power/safety compartment. The enclosure may include an isolated backplane, mounting rails, EMI shielding, cooling paths, service panels, and an external I/O bulkhead.

Controlled Ingress and Drift Screening

Referring to FIG. 3, the A7 bridge 200 may perform protocol isolation, buffering, packet framing, deterministic schema translation, and replay protection. The N12 kernel 220 may perform schema, provenance, uncertainty, contradiction, range, and freshness checks. Passing these checks generates packet 230 but does not itself authorize actuation. Any

required-check failure routes the current proposal to path 240 and may create a forensic event.

Privacy-Preserving Sensing

Referring to FIG. 4, sensing node 800 may include a 905 nm LiDAR 810, a raw point-cloud buffer 820, and a node-local FPGA or FPPA voxelization engine 830. The engine 830 generates a 96-cell occupancy grid 840 and anonymized center-of-mass vectors 860. A silicon privacy wall 850 prevents the raw point cloud from egressing the node. In an embodiment, the node physically lacks a camera, microphone, and cloud-network route.

Hardware-Timed Deliberation

Referring to FIG. 5, a master clock 320 operates nominally at 1 kHz, corresponding to a 1.0 ms supervisory cycle. A hardware timer/counter 322 enforces a selectable deliberation interval of 25 ms to 1000 ms inclusive. The interval is independent of advisory-software scheduling. Output remains disabled until the interval completes, authorization is valid, and the safety FSM/KCL 350 indicates a safe condition.

Human Authorization

Referring to FIG. 6, authorization gate 400 receives a biological identity input 410, a cryptographic or possession-based authority input 420, and a kinetic confirmation input 430. The factors may be independently isolated and validated. An iris-derived token may expire in less than five seconds. No two-of-three fallback is provided. Dropping or invalidating a required factor withdraws authorization-valid signal 440.

Fail-Safe Energy Control

Referring to FIG. 7, U7 sequencer 600 receives a hardware fault trigger 610 and operates isolator 620 to control actuator rail 630. A design requirement may specify a severance time less than 1.05 ms from trigger point TP-A 1350 to isolation point TP-B 1360. The 1.0 ms supervisory cycle of clock 320 is not the severance time. The response is embodiment-specific: immediate de-energization for a free-space arm, mechanical

holding for a load-bearing mechanism, or controlled deceleration for an occupant-carrying mobility system.

Immutable Forensic Accountability

Referring to FIG. 8, ledger 700 receives event input 710 and chains records with SHA-3-512 circuit 720. Root of trust 730 attests the chain. WORM memory 740 and OTP fuse bank 750 provide irreversible or write-once finality. A one-way boundary 760 prevents the ledger from issuing an actuator command. A ledger-integrity or tamper fault can independently trigger the fail-safe sequencer 600.

Observational and Kinetic Architectures

Referring to FIG. 9, an observational architecture may include sensing embodiment 520, privacy layer 310, deterministic monitoring layer 330, an isolated alert cable 920, and nurse annunciator 910, without an actuator path. A kinetic architecture additionally includes D-layer 370, authorization gate 400, fail-safe sequencer 600, ledger 700, and router 500 controlling an actuator. These architecture labels do not alone establish a regulatory classification.

A13 Embodiments

Referring to FIG. 10, A13 router 500 may select among a mobility embodiment 510, sensing embodiment 520, and clinical robotic embodiment 530 according to a hardware-protected configuration. Mobility embodiment 510 may include chassis 1100, wheels 1110, seat 1120, and controlled-deceleration path 1130. Clinical robotic embodiment 530 may include base 1200, joints 1210, end effector 1220, encoders 1230, and a bounded positional envelope 1240. A value of ±0.05 mm, where used, is a positional tolerance and not a jerk value; jerk is separately expressed in mm/s^3.

Validation Arrangement

Referring to FIG. 11, validation bench 1300 may include oscilloscope 1310, continuity meter 1320, cryptographic verifier 1330, and network tester 1340. Measurements may

include the 1 kHz clock, the 25–1000 ms deliberation interval, the TP-A-to-TP-B energy-isolation interval, authorization continuity, hash-chain integrity, absence of reverse commands, and absence of raw point-cloud egress. Design requirements are not treated as measured performance until evidence is obtained using calibrated instruments and traceable procedures.

System State Machine

Referring to FIG. 12, the system state machine begins in power-on self-test and enters P-LIFE mechanical stillness. A proposal progresses through controlled ingress, deterministic screening, packet validation, hardware hold, human authorization, safety verification, bounded execution, forensic commit, and return to stillness. Failure states include proposal rejection, raw-egress blocking, authorization timeout, tamper invalidation, ledger fault, fail-safe braking, fail-loud alarm, and safe-state verification. Re-arm requires a verified safe state and renewed human authorization; automatic restart is prohibited.

EXAMPLE IMPLEMENTATIONS

- Clinical and surgical robotic systems.
- Privacy-preserving eldercare sensing and fall alerts.
- Occupant-carrying mobility systems.
- Industrial automation and critical infrastructure.
- Defense, aerospace, and remote systems.
- Digital decision systems where hardware-independent commitment and accountability are required.

INDUSTRIAL APPLICABILITY

The architecture can be manufactured using programmable logic, safety controllers, secure elements, non-imaging ranging sensors, isolated interfaces, relays, motor-drive safety inputs, mechanical brakes, write-once memory, cryptographic circuits, and

conventional actuators. It is applicable wherever probabilistic computation must be prevented from independently causing a consequential action.

CLAIMS

1. A constitutional hardware enforcement system for governing an artificial-intelligence advisory processor, comprising: an ingress bridge forming a controlled ingress path from the advisory processor; a deterministic screening kernel configured to accept or reject an advisory proposal and generate a bounded deterministic packet; a synchronous hardware governance core configured to withhold a consequential output during a hardware-timed deliberation interval; a human authorization gate independent of the advisory processor; an execution interface enabled only after verification of the packet, the interval, and an authorization state; a fail-safe energy-control mechanism independent of the advisory processor; and a write-once or append-only forensic ledger.

2. The system of claim 1, wherein the hardware governance core comprises a privacy layer, a deterministic layer, and a forensic/fail-safe layer.

3. The system of claim 1, wherein the hardware governance core operates in a nominal 1 kHz synchronous clock domain providing a 1.0 ms supervisory cycle.

4. The system of claim 1, wherein the hardware-timed deliberation interval is enforced by a programmable-logic counter independently of software scheduling.

5. The system of claim 4, wherein the deliberation interval is selectable from 25 ms to 1000 ms inclusive.

6. The system of claim 1, wherein the human authorization gate requires a biological identity factor, a cryptographic or possession-based authority factor, and a kinetic confirmation factor.

7. The system of claim 6, wherein the biological identity factor generates a token having a validity period less than five seconds.

8. The system of claim 1, wherein the ingress bridge translates semantic or probabilistic proposal content into a deterministic packet containing bounded output parameters.

9. The system of claim 1, wherein the deterministic screening kernel rejects contradictory, malformed, stale, unprovenanced, uncertain, or out-of-range content and maintains a stillness state.

10. The system of claim 1, further comprising a privacy-preserving sensing node having a non-imaging ranging sensor and node-local voxelization circuitry.

11. The system of claim 10, wherein the sensor comprises a 905 nm LiDAR array and the circuitry produces a 96-cell occupancy grid and center-of-mass vectors.

12. The system of claim 10, wherein raw point-cloud data is prevented from egressing the sensing node by a hardware privacy boundary.

13. The system of claim 1, wherein the fail-safe energy-control mechanism comprises a one-shot sequencer and a physical or solid-state isolator.

14. The system of claim 13, wherein the fail-safe energy-control mechanism is configured according to an embodiment to perform immediate de-energization, mechanical holding, or controlled deceleration.

15. The system of claim 13, wherein an electrical isolation requirement is less than 1.05 ms measured from a validated hardware trigger point to an actuator-side rail-isolation point.

16. The system of claim 1, wherein the forensic ledger cryptographically chains event records using SHA-3-512.

17. The system of claim 16, further comprising a hardware root of trust and WORM memory, OTP fuses, or another irreversible storage mechanism.

18. The system of claim 16, wherein the ledger has a unidirectional event input and no actuator-command return path.

19. The system of claim 1, wherein the execution interface controls a clinical robotic arm, a mobility system, an eldercare apparatus, an industrial machine, or a remote platform.

20. A method of hardware-enforced artificial-intelligence governance, comprising: receiving an advisory proposal through a controlled ingress bridge; deterministically screening the proposal; rejecting a failed proposal to a stillness state; translating an accepted proposal into a bounded deterministic packet; imposing a hardware-timed deliberation interval; independently receiving human authorization; enabling a consequential output only after hardware verification; monitoring the output using a safety state machine; and recording an event chain in write-once or append-only storage.

21. The method of claim 20, further comprising detecting a fault and independently removing, isolating, holding, or controlling actuator energy.

22. The method of claim 20, further comprising voxelizing non-imaging spatial data inside a sensing node and transmitting only anonymized spatial vectors.

23. A privacy-preserving sensing node comprising: a non-imaging ranging sensor; a local hardware voxelization circuit; a hardware boundary preventing raw sensing data from egressing the node; and an output gate configured to output anonymized spatial vectors.

24. A forensic accountability apparatus comprising: an event input; a cryptographic chaining circuit; a hardware root of trust; and a write-once storage device, wherein the apparatus has no actuator-command return path.

25. The system, method, sensing node, or forensic accountability apparatus of any preceding claim, wherein failure to verify a required state causes mechanical stillness, energy isolation, controlled stopping, or a fail-loud local alarm.

ABSTRACT

A constitutional hardware enforcement architecture interposes deterministic apparatus between a non-deterministic artificial-intelligence advisor and a consequential output. A controlled ingress bridge and deterministic screening kernel translate accepted proposals into bounded deterministic packets. A synchronous P/N/D governance core imposes a non-bypassable hardware-timed deliberation interval and withholds output pending independent human authorization. A privacy embodiment performs node-local voxelization of non-imaging ranging data and permits only anonymized vectors to cross a silicon privacy boundary. A fail-safe sequencer independently removes, isolates, holds, or controls actuator energy. A write-once forensic ledger cryptographically chains proposal, screening, authorization, execution, and fault events under a hardware root of trust. The default state is stillness or another embodiment-appropriate safe state. Applications include clinical sensing, medical robotics, mobility, industrial control, critical infrastructure, defense, aerospace, and remote systems.

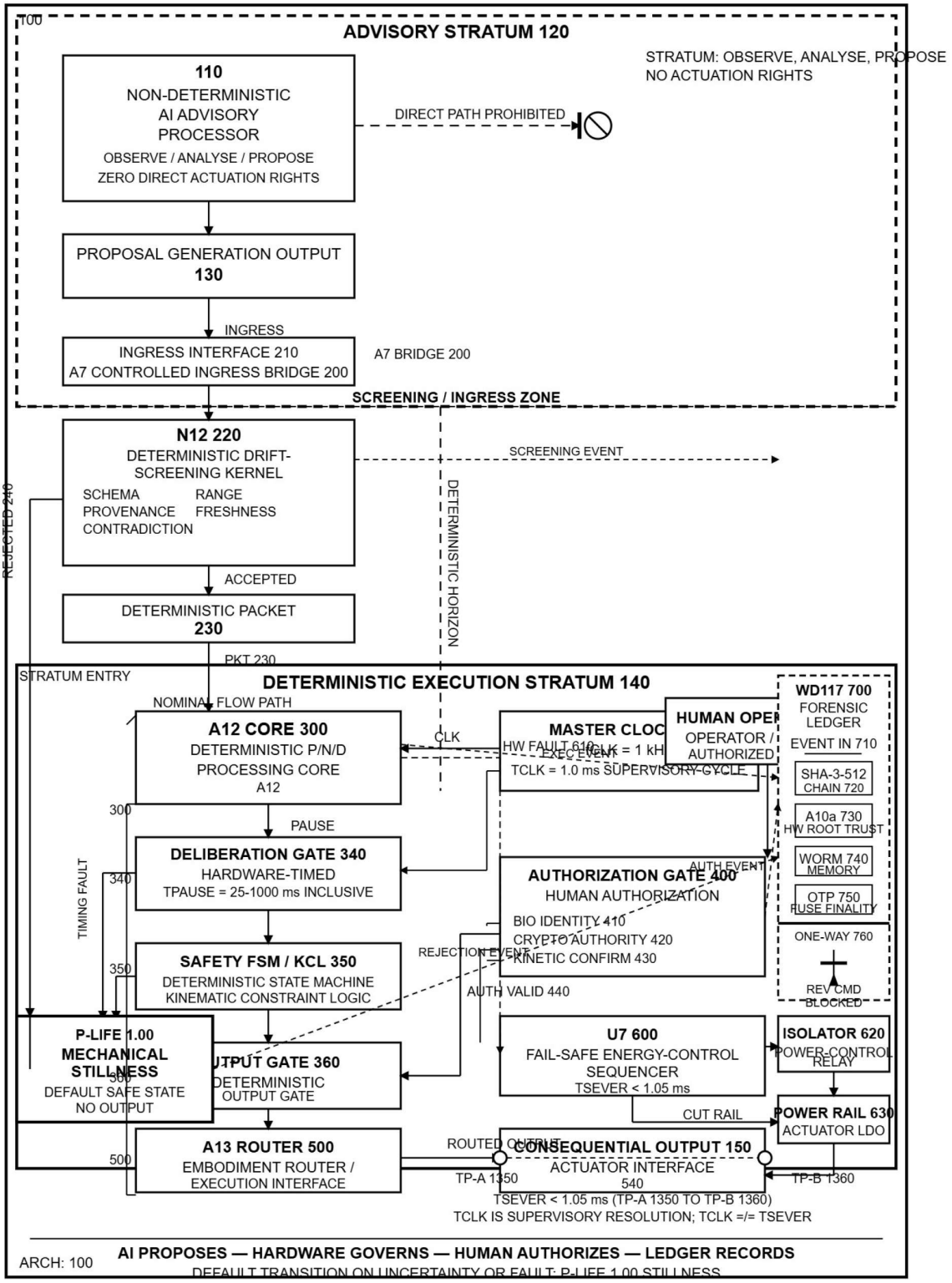

100
ADVISORY STRATUM 120
STRATUM: OBSERVE, ANALYSE, PROPOSE
NO ACTUATION RIGHTS
110
NON-DETERMINISTIC
AI ADVISORY
PROCESSOR
OBSERVE / ANALYSE / PROPOSE
ZERO DIRECT ACTUATION RIGHTS
DIRECT PATH PROHIBITED
PROPOSAL GENERATION OUTPUT
130
INGRESS
INGRESS INTERFACE 210
A7 CONTROLLED INGRESS BRIDGE 200
A7 BRIDGE 200
SCREENING / INGRESS ZONE
N12 220
DETERMINISTIC DRIFT-
SCREENING KERNEL
SCHEMA
PROVENANCE
CONTRADICTION
RANGE
FRESHNESS
SCREENING EVENT
REJECTED 240
DETERMINISTIC HORIZON
ACCEPTED
DETERMINISTIC PACKET
230
PKT 230
STRATUM ENTRY
DETERMINISTIC EXECUTION STRATUM 140
NOMINAL FLOW PATH
A12 CORE 300
DETERMINISTIC P/N/D
PROCESSING CORE
A12
CLK
MASTER CLOC
HW FAULT 610 CLK = 1 kH
EXEC EVENT
TCLK = 1.0 ms SUPERVISORY CYCLE
HUMAN OPER
OPERATOR /
AUTHORIZED
WD117 700
FORENSIC
LEDGER
EVENT IN 710
SHA-3-512
CHAIN 720
A10a 730
HW ROOT TRUST
WORM 740
MEMORY
OTP 750
FUSE FINALITY
ONE-WAY 760
REV CMD
BLOCKED
300
PAUSE
DELIBERATION GATE 340
HARDWARE-TIMED
TPAUSE = 25-1000 ms INCLUSIVE
340
TIMING FAULT
AUTH EVENT
AUTHORIZATION GATE 400
HUMAN AUTHORIZATION
BIO IDENTITY 410
CRYPTO AUTHORITY 420
KINETIC CONFIRM 430
REJECTION EVENT
SAFETY FSM / KCL 350
DETERMINISTIC STATE MACHINE
KINEMATIC CONSTRAINT LOGIC
350
AUTH VALID 440
P-LIFE 1.00
MECHANICAL
STILLNESS
DEFAULT SAFE STATE
NO OUTPUT
360
UTPUT GATE 360
DETERMINISTIC
OUTPUT GATE
U7 600
FAIL-SAFE ENERGY-CONTROL
SEQUENCER
TSEVER < 1.05 ms
ISOLATOR 620
POWER-CONTROL
RELAY
CUT RAIL
POWER RAIL 630
ACTUATOR LDO
A13 ROUTER 500
EMBODIMENT ROUTER /
EXECUTION INTERFACE
500
ROUTED OUTPUT
CONSEQUENTIAL OUTPUT 150
ACTUATOR INTERFACE
540
TP-A 1350
TP-B 1360
TSEVER < 1.05 ms (TP-A 1350 TO TP-B 1360)
TCLK IS SUPERVISORY RESOLUTION; TCLK =/= TSEVER
ARCH: 100
AI PROPOSES — HARDWARE GOVERNS — HUMAN AUTHORIZES — LEDGER RECORDS
DEFAULT TRANSITION ON UNCERTAINTY OR FAULT: P-LIFE 1.00 STILLNESS

FIG. 1

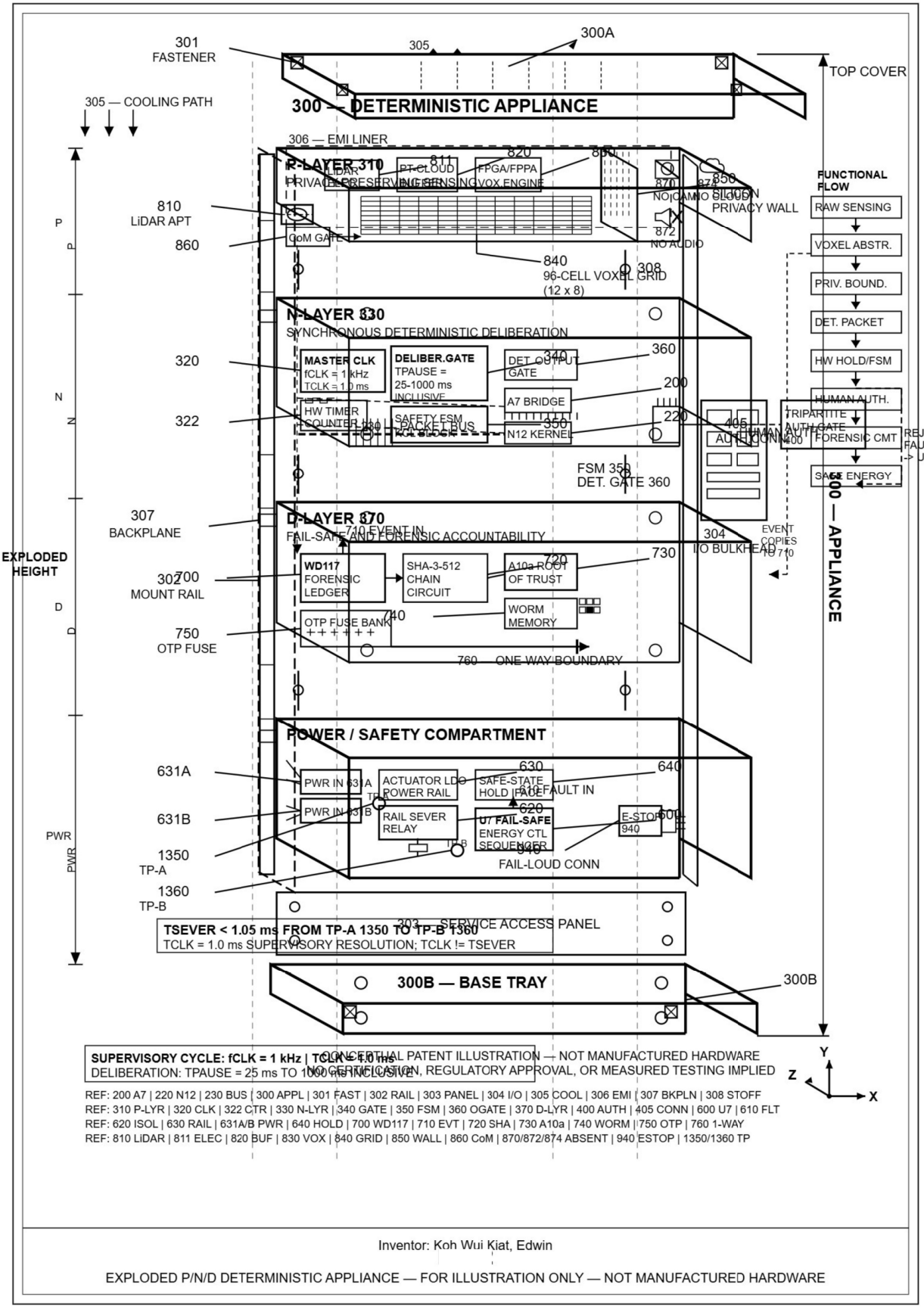

301
FASTENER
305
300A
TOP COVER
305 — COOLING PATH
300 — DETERMINISTIC APPLIANCE
306 — EMI LINER
P-LAYER 310
LiDAR
PRIVACY PRESERVING SENSING
811
PT-CLOUD ENGINE
820
FPGA/FPPA
850
VOXEL ENGINE
870
872
874
NO CAMO CLOUD
NO AUDIO
HIDDEN PRIVACY WALL
FUNCTIONAL FLOW
RAW SENSING
VOXEL ABSTR.
PRIV. BOUND.
DET. PACKET
HW HOLD/FSM
HUMAN AUTH.
TRIPARTITE AUTH GATE
FORENSIC CMT
REJECT FAULT -> U7
SAFE ENERGY
810
LiDAR APT
860
CoM GATE
840
96-CELL VOXEL GRID
(12 x 8)
308
N-LAYER 330
SYNCHRONOUS DETERMINISTIC DELIBERATION
320
322
MASTER CLK
fCLK = 1 kHz
TCLK = 1.0 ms
DELIBER.GATE
TPAUSE =
25-1000 ms
INCLUSIVE
HW TIMER
COUNTER
SAFETY FSM
PACKET BUS
DET. OUTPUT GATE
340
360
A7 BRIDGE
200
N12 KERNEL
350
220
405
AUTH CONN
400
FSM 350
DET. GATE 360
307
BACKPLANE
D-LAYER 370
FAIL-SAFE AND FORENSIC ACCOUNTABILITY
710 EVENT IN
304
I/O BULKHEAD
EVENT COPIES TO 710
EXPLODED HEIGHT
302
MOUNT RAIL
700
WD117
FORENSIC LEDGER
SHA-3-512
CHAIN
CIRCUIT
720
A10a-ROOT OF TRUST
730
740
WORM MEMORY
OTP FUSE BANK
750
OTP FUSE
760 ONE-WAY BOUNDARY
600 — APPLIANCE
POWER / SAFETY COMPARTMENT
631A
631B
PWR IN 631A
PWR IN 631B
ACTUATOR LDO
POWER RAIL
RAIL SEVER RELAY
TP-A
TP-B
630
SAFE-STATE HOLD IFACE
640
FAULT IN
620
U7 FAIL-SAFE
ENERGY CTL
SEQUENCER
610
E-STOP
940
940
FAIL-LOUD CONN
1350
TP-A
1360
TP-B
TSEVER < 1.05 ms FROM TP-A 1350 TO TP-B 1360
TCLK = 1.0 ms SUPERVISORY RESOLUTION; TCLK != TSEVER
303 — SERVICE ACCESS PANEL
300B — BASE TRAY
300B
SUPERVISORY CYCLE: fCLK = 1 kHz | TCLK = 1.0 ms
DELIBERATION: TPAUSE = 25 ms TO 1000 ms INCLUSIVE
CONCEPTUAL PATENT ILLUSTRATION — NOT MANUFACTURED HARDWARE
NO CERTIFICATION, REGULATORY APPROVAL, OR MEASURED TESTING IMPLIED
Y
Z
X
REF: 200 A7 | 220 N12 | 230 BUS | 300 APPL | 301 FAST | 302 RAIL | 303 PANEL | 304 I/O | 305 COOL | 306 EMI | 307 BKPLN | 308 STOFF
REF: 310 P-LYR | 320 CLK | 322 CTR | 330 N-LYR | 340 GATE | 350 FSM | 360 OGATE | 370 D-LYR | 400 AUTH | 405 CONN | 600 U7 | 610 FLT
REF: 620 ISOL | 630 RAIL | 631A/B PWR | 640 HOLD | 700 WD117 | 710 EVT | 720 SHA | 730 A10a | 740 WORM | 750 OTP | 760 1-WAY
REF: 810 LiDAR | 811 ELEC | 820 BUF | 830 VOX | 840 GRID | 850 WALL | 860 CoM | 870/872/874 ABSENT | 940 ESTOP | 1350/1360 TP
Inventor: Koh Wui Kiat, Edwin
EXPLODED P/N/D DETERMINISTIC APPLIANCE — FOR ILLUSTRATION ONLY — NOT MANUFACTURED HARDWARE

FIG. 2

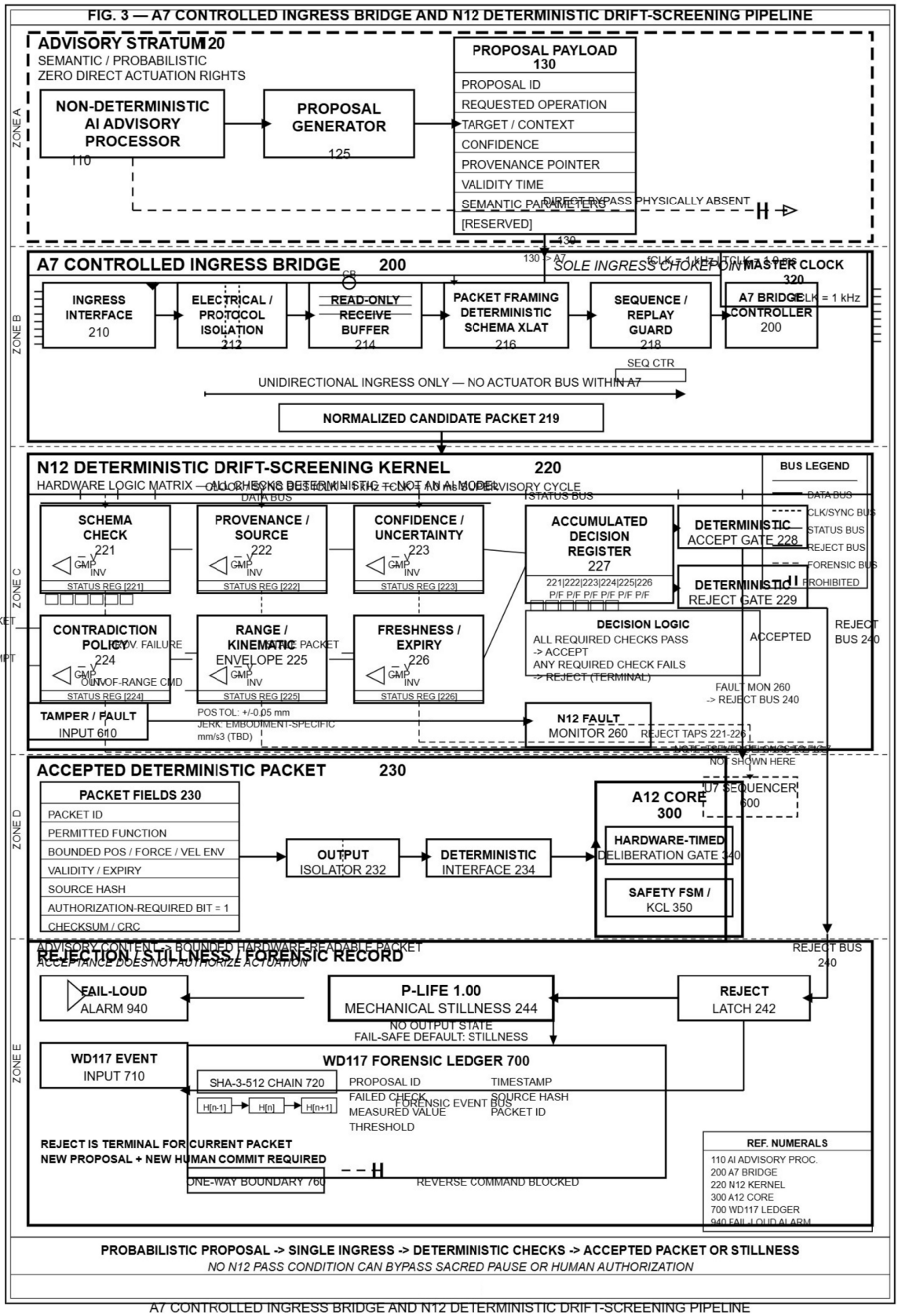


FIG. 3 — A7 CONTROLLED INGRESS BRIDGE AND N12 DETERMINISTIC DRIFT-SCREENING PIPELINE
ADVISORY STRATUM 120
SEMANTIC / PROBABILISTIC
ZERO DIRECT ACTUATION RIGHTS
NON-DETERMINISTIC AI ADVISORY PROCESSOR
110
PROPOSAL GENERATOR
125
PROPOSAL PAYLOAD 130
PROPOSAL ID
REQUESTED OPERATION
TARGET / CONTEXT
CONFIDENCE
PROVENANCE POINTER
VALIDITY TIME
SEMANTIC PARAMETERS
[RESERVED]
DIRECT BYPASS PHYSICALLY ABSENT
130
130 > A7
A7 CONTROLLED INGRESS BRIDGE 200
SOLE INGRESS CHOKEPOINT
MASTER CLOCK 320
fCLK = 1 kHz, tCLK = 1.0 ms
INGRESS INTERFACE 210
ELECTRICAL / PROTOCOL ISOLATION 212
READ-ONLY RECEIVE BUFFER 214
PACKET FRAMING DETERMINISTIC SCHEMA XLAT 216
SEQUENCE / REPLAY GUARD 218
A7 BRIDGE CONTROLLER 200
SEQ CTR
UNIDIRECTIONAL INGRESS ONLY — NO ACTUATOR BUS WITHIN A7
NORMALIZED CANDIDATE PACKET 219
N12 DETERMINISTIC DRIFT-SCREENING KERNEL 220
HARDWARE LOGIC MATRIX — ALL CHECKS DETERMINISTIC — NOT AN AI MODEL
CLOCK SYNC BUS (1 kHz TICK) — 1.0 ms SUPERVISORY CYCLE
DATA BUS
STATUS BUS
BUS LEGEND
DATA BUS
CLK/SYNC BUS
STATUS BUS
REJECT BUS
FORENSIC BUS
PROHIBITED
SCHEMA CHECK 221
PROVENANCE / SOURCE 222
CONFIDENCE / UNCERTAINTY 223
STATUS REG [221]
STATUS REG [222]
STATUS REG [223]
ACCUMULATED DECISION REGISTER 227
221|222|223|224|225|226
P/F P/F P/F P/F P/F P/F
DETERMINISTIC ACCEPT GATE 228
DETERMINISTIC REJECT GATE 229
CONTRADICTION POLICY 224
RANGE / KINEMATIC ENVELOPE 225
FRESHNESS / EXPIRY 226
CONV. FAILURE
OUT-OF-RANGE CMD
STALE PACKET
STATUS REG [224]
STATUS REG [225]
STATUS REG [226]
DECISION LOGIC
ALL REQUIRED CHECKS PASS -> ACCEPT
ANY REQUIRED CHECK FAILS -> REJECT (TERMINAL)
ACCEPTED
REJECT BUS 240
FAULT MON 260 -> REJECT BUS 240
TAMPER / FAULT INPUT 610
POS TOL: +/-0.05 mm
JERK: EMBODIMENT-SPECIFIC mm/s3 (TBD)
N12 FAULT MONITOR 260
REJECT TAPS 221-226
NOT SHOWN HERE
ACCEPTED DETERMINISTIC PACKET 230
PACKET FIELDS 230
PACKET ID
PERMITTED FUNCTION
BOUNDED POS / FORCE / VEL ENV
VALIDITY / EXPIRY
SOURCE HASH
AUTHORIZATION-REQUIRED BIT = 1
CHECKSUM / CRC
OUTPUT ISOLATOR 232
DETERMINISTIC INTERFACE 234
A12 CORE 300
HARDWARE-TIMED DELIBERATION GATE 340
SAFETY FSM / KCL 350
ADVISORY CONTENT -> BOUNDED HARDWARE-READABLE PACKET
ACCEPTANCE DOES NOT AUTHORIZE ACTUATION
REJECTION / STILLNESS / FORENSIC RECORD
REJECT BUS 240
FAIL-LOUD ALARM 940
P-LIFE 1.00 MECHANICAL STILLNESS 244
NO OUTPUT STATE
FAIL-SAFE DEFAULT: STILLNESS
REJECT LATCH 242
WD117 EVENT INPUT 710
WD117 FORENSIC LEDGER 700
SHA-3-512 CHAIN 720
H[n-1] H[n] H[n+1]
PROPOSAL ID
FAILED CHECK
MEASURED VALUE
THRESHOLD
TIMESTAMP
SOURCE HASH
PACKET ID
FORENSIC EVENT BUS
REJECT IS TERMINAL FOR CURRENT PACKET
NEW PROPOSAL + NEW HUMAN COMMIT REQUIRED
ONE-WAY BOUNDARY 760
REVERSE COMMAND BLOCKED
REF. NUMERALS
110 AI ADVISORY PROC.
200 A7 BRIDGE
220 N12 KERNEL
300 A12 CORE
700 WD117 LEDGER
940 FAIL-LOUD ALARM
PROBABILISTIC PROPOSAL -> SINGLE INGRESS -> DETERMINISTIC CHECKS -> ACCEPTED PACKET OR STILLNESS
NO N12 PASS CONDITION CAN BYPASS SACRED PAUSE OR HUMAN AUTHORIZATION
A7 CONTROLLED INGRESS BRIDGE AND N12 DETERMINISTIC DRIFT-SCREENING PIPELINE

FIG. 3

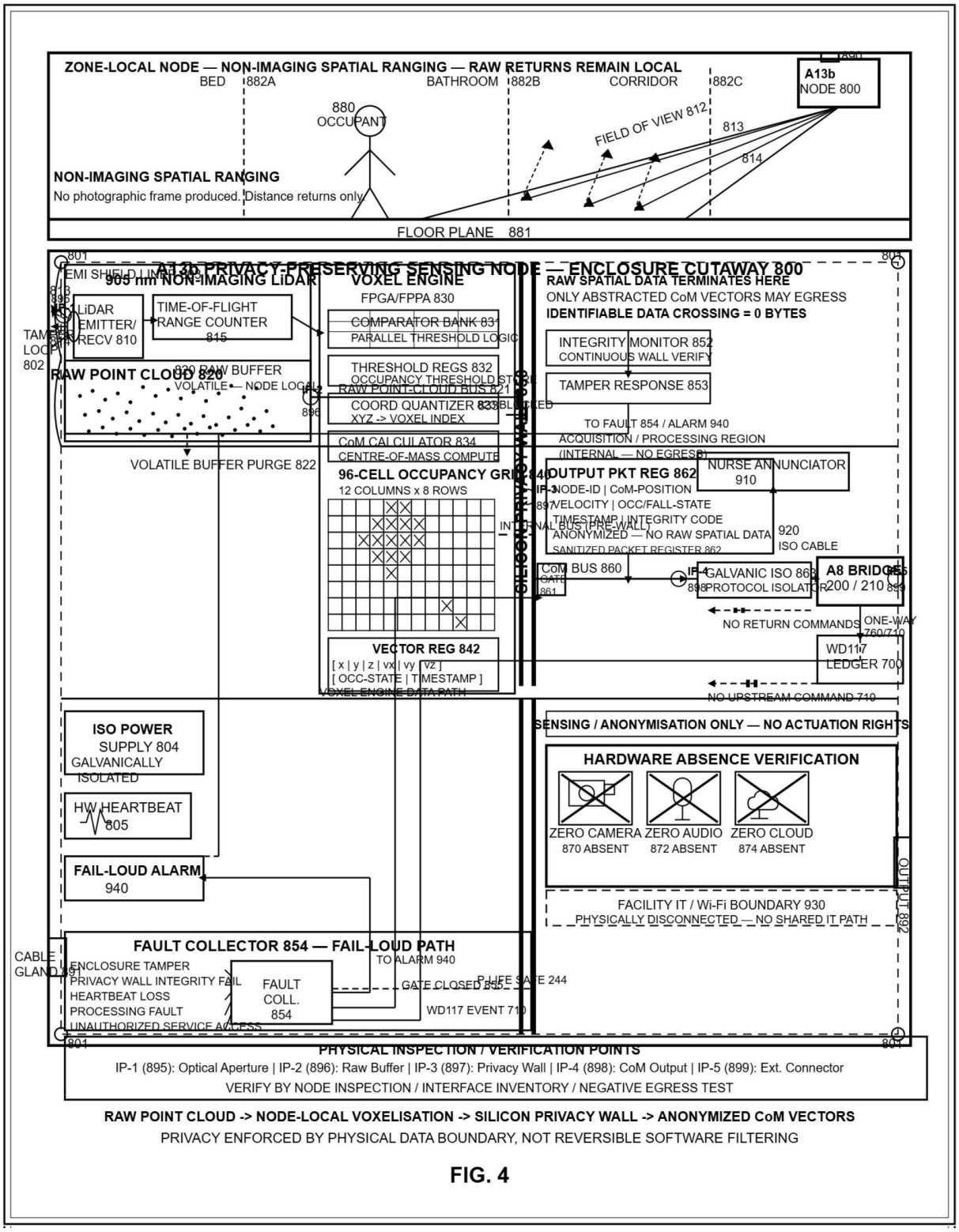

ZONE-LOCAL NODE — NON-IMAGING SPATIAL RANGING — RAW RETURNS REMAIN LOCAL
BED
882A
BATHROOM
882B
CORRIDOR
882C
A13b
NODE 800
880
OCCUPANT
FIELD OF VIEW 812
813
814
NON-IMAGING SPATIAL RANGING
No photographic frame produced. Distance returns only.
FLOOR PLANE 881
A13b PRIVACY-PRESERVING SENSING NODE — ENCLOSURE CUTAWAY 800
EMI SHIELD LINER 801
905 nm NON-IMAGING LiDAR
VOXEL ENGINE
FPGA/FPPA 830
RAW SPATIAL DATA TERMINATES HERE
ONLY ABSTRACTED CoM VECTORS MAY EGRESS
IDENTIFIABLE DATA CROSSING = 0 BYTES
LiDAR EMITTER/ RECV 810
TIME-OF-FLIGHT RANGE COUNTER 815
TAMPER LOOP 802
RAW POINT CLOUD 820
820 RAW BUFFER
VOLATILE — NODE LOCAL
COMPARATOR BANK 831
PARALLEL THRESHOLD LOGIC
THRESHOLD REGS 832
OCCUPANCY THRESHOLD STORE
RAW POINT-CLOUD BUS 821
COORD QUANTIZER 833
XYZ -> VOXEL INDEX
CoM CALCULATOR 834
CENTRE-OF-MASS COMPUTE
VOLATILE BUFFER PURGE 822
96-CELL OCCUPANCY GRID 840
12 COLUMNS x 8 ROWS
INTERNAL BUS (PRE-WALL)
SILICON PRIVACY WALL 850
VECTOR REG 842
[x | y | z | vx | vy | vz]
[OCC-STATE | TIMESTAMP]
VOXEL ENGINE DATA PATH
INTEGRITY MONITOR 852
CONTINUOUS WALL VERIFY
TAMPER RESPONSE 853
TO FAULT 854 / ALARM 940
ACQUISITION / PROCESSING REGION
(INTERNAL — NO EGRESS)
OUTPUT PKT REG 862
IP-3
NODE-ID | CoM-POSITION
VELOCITY | OCC/FALL-STATE
TIMESTAMP | INTEGRITY CODE
ANONYMIZED — NO RAW SPATIAL DATA
SANITIZED PACKET REGISTER 862
NURSE ANNUNCIATOR 910
920
ISO CABLE
CoM BUS 860
GATE 861
IP-4
GALVANIC ISO 863
PROTOCOL ISOLATOR
A8 BRIDGES 200 / 210
NO RETURN COMMANDS
ONE-WAY 760/710
WD117 LEDGER 700
NO UPSTREAM COMMAND 710
SENSING / ANONYMISATION ONLY — NO ACTUATION RIGHTS
HARDWARE ABSENCE VERIFICATION
ZERO CAMERA 870 ABSENT
ZERO AUDIO 872 ABSENT
ZERO CLOUD 874 ABSENT
ISO POWER SUPPLY 804
GALVANICALLY ISOLATED
HW HEARTBEAT 805
FAIL-LOUD ALARM 940
FACILITY IT / Wi-Fi BOUNDARY 930
PHYSICALLY DISCONNECTED — NO SHARED IT PATH
OUTPUT 892
FAULT COLLECTOR 854 — FAIL-LOUD PATH
TO ALARM 940
CABLE GLAND 391
ENCLOSURE TAMPER
PRIVACY WALL INTEGRITY FAIL
HEARTBEAT LOSS
PROCESSING FAULT
UNAUTHORIZED SERVICE ACCESS
FAULT COLL. 854
GATE CLOSED 852
P-LIFE GATE 244
WD117 EVENT 710
PHYSICAL INSPECTION / VERIFICATION POINTS
IP-1 (895): Optical Aperture | IP-2 (896): Raw Buffer | IP-3 (897): Privacy Wall | IP-4 (898): CoM Output | IP-5 (899): Ext. Connector
VERIFY BY NODE INSPECTION / INTERFACE INVENTORY / NEGATIVE EGRESS TEST
RAW POINT CLOUD -> NODE-LOCAL VOXELISATION -> SILICON PRIVACY WALL -> ANONYMIZED CoM VECTORS
PRIVACY ENFORCED BY PHYSICAL DATA BOUNDARY, NOT REVERSIBLE SOFTWARE FILTERING

FIG. 4

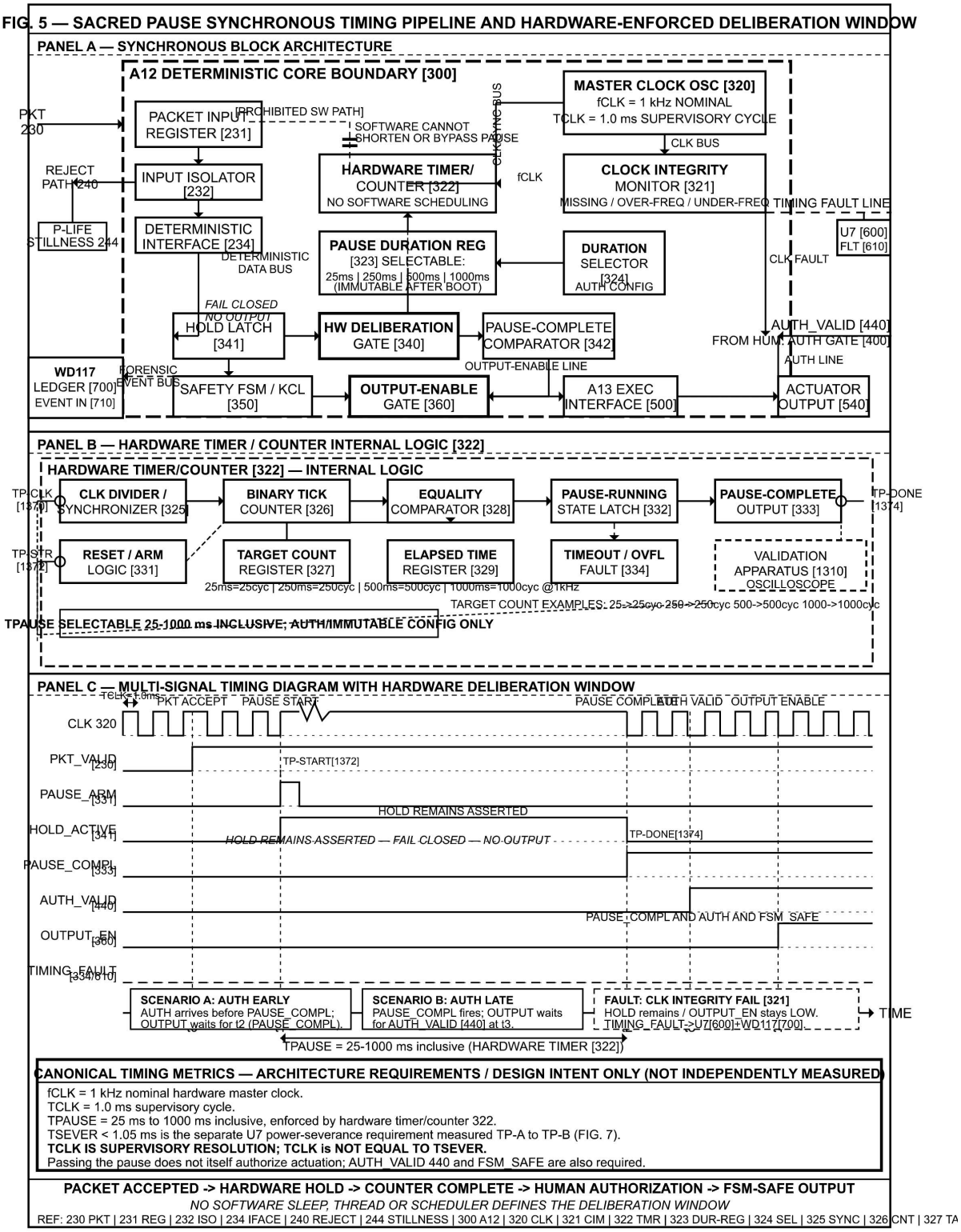


FIG. 5 — SACRED PAUSE SYNCHRONOUS TIMING PIPELINE AND HARDWARE-ENFORCED DELIBERATION WINDOW
PANEL A — SYNCHRONOUS BLOCK ARCHITECTURE
A12 DETERMINISTIC CORE BOUNDARY [300]
PKT 230
PACKET INPUT REGISTER [231]
[PROHIBITED SW PATH]
SOFTWARE CANNOT SHORTEN OR BYPASS PAUSE
CLOCKING BUS
MASTER CLOCK OSC [320]
fCLK = 1 kHz NOMINAL
TCLK = 1.0 ms SUPERVISORY CYCLE
CLK BUS
REJECT PATH 240
INPUT ISOLATOR [232]
HARDWARE TIMER/ COUNTER [322]
NO SOFTWARE SCHEDULING
fCLK
CLOCK INTEGRITY MONITOR [321]
MISSING / OVER-FREQ / UNDER-FREQ TIMING FAULT LINE
P-LIFE STILLNESS 244
DETERMINISTIC INTERFACE [234]
DETERMINISTIC DATA BUS
PAUSE DURATION REG [323] SELECTABLE:
25ms | 250ms | 500ms | 1000ms
(IMMUTABLE AFTER BOOT)
DURATION SELECTOR [324]
AUTH CONFIG
U7 [600]
FLT [610]
CLK FAULT
FAIL CLOSED
NO OUTPUT
HOLD LATCH [341]
HW DELIBERATION GATE [340]
PAUSE-COMPLETE COMPARATOR [342]
AUTH_VALID [440]
FROM HUM. AUTH GATE [400]
AUTH LINE
OUTPUT-ENABLE LINE
WD117
LEDGER [700]
EVENT IN [710]
FORENSIC EVENT BUS
SAFETY FSM / KCL [350]
OUTPUT-ENABLE GATE [360]
A13 EXEC INTERFACE [500]
ACTUATOR OUTPUT [540]
PANEL B — HARDWARE TIMER / COUNTER INTERNAL LOGIC [322]
HARDWARE TIMER/COUNTER [322] — INTERNAL LOGIC
TP-CLK [1370]
CLK DIVIDER / SYNCHRONIZER [325]
BINARY TICK COUNTER [326]
EQUALITY COMPARATOR [328]
PAUSE-RUNNING STATE LATCH [332]
PAUSE-COMPLETE OUTPUT [333]
TP-DONE [1374]
TP-STR [1372]
RESET / ARM LOGIC [331]
TARGET COUNT REGISTER [327]
ELAPSED TIME REGISTER [329]
TIMEOUT / OVFL FAULT [334]
VALIDATION APPARATUS [1310] OSCILLOSCOPE
25ms=25cyc | 250ms=250cyc | 500ms=500cyc | 1000ms=1000cyc @1kHz
TARGET COUNT EXAMPLES: 25->25cyc 250->250cyc 500->500cyc 1000->1000cyc
TPAUSE SELECTABLE 25-1000 ms INCLUSIVE; AUTH/IMMUTABLE CONFIG ONLY
PANEL C — MULTI-SIGNAL TIMING DIAGRAM WITH HARDWARE DELIBERATION WINDOW
TCLK = 1.0ms
PKT ACCEPT
PAUSE START
PAUSE COMPLETE
AUTH VALID
OUTPUT ENABLE
CLK 320
PKT_VALID [230]
TP-START[1372]
PAUSE_ARM [331]
HOLD REMAINS ASSERTED
HOLD_ACTIVE [341]
HOLD REMAINS ASSERTED — FAIL CLOSED — NO OUTPUT
TP-DONE[1374]
PAUSE_COMPL [333]
AUTH_VALID [440]
PAUSE_COMPL AND AUTH AND FSM_SAFE
OUTPUT_EN [360]
TIMING_FAULT [334/610]
SCENARIO A: AUTH EARLY
AUTH arrives before PAUSE_COMPL; OUTPUT waits for t2 (PAUSE_COMPL).
SCENARIO B: AUTH LATE
PAUSE_COMPL fires; OUTPUT waits for AUTH_VALID [440] at t3.
FAULT: CLK INTEGRITY FAIL [321]
HOLD remains / OUTPUT_EN stays LOW.
TIMING_FAULT->U7[600]+WD117[700].
TIME
TPAUSE = 25-1000 ms inclusive (HARDWARE TIMER [322])
CANONICAL TIMING METRICS — ARCHITECTURE REQUIREMENTS / DESIGN INTENT ONLY (NOT INDEPENDENTLY MEASURED)
fCLK = 1 kHz nominal hardware master clock.
TCLK = 1.0 ms supervisory cycle.
TPAUSE = 25 ms to 1000 ms inclusive, enforced by hardware timer/counter 322.
TSEVER < 1.05 ms is the separate U7 power-severance requirement measured TP-A to TP-B (FIG. 7).
TCLK IS SUPERVISORY RESOLUTION; TCLK is NOT EQUAL TO TSEVER.
Passing the pause does not itself authorize actuation; AUTH_VALID 440 and FSM_SAFE are also required.
PACKET ACCEPTED -> HARDWARE HOLD -> COUNTER COMPLETE -> HUMAN AUTHORIZATION -> FSM-SAFE OUTPUT
NO SOFTWARE SLEEP, THREAD OR SCHEDULER DEFINES THE DELIBERATION WINDOW
REF: 230 PKT | 231 REG | 232 ISO | 234 IFACE | 240 REJECT | 244 STILLNESS | 300 A12 | 320 CLK | 321 CIM | 322 TMR | 323 DUR-REG | 324 SEL | 325 SYNC | 326 CNT | 327 TA

FIG. 5

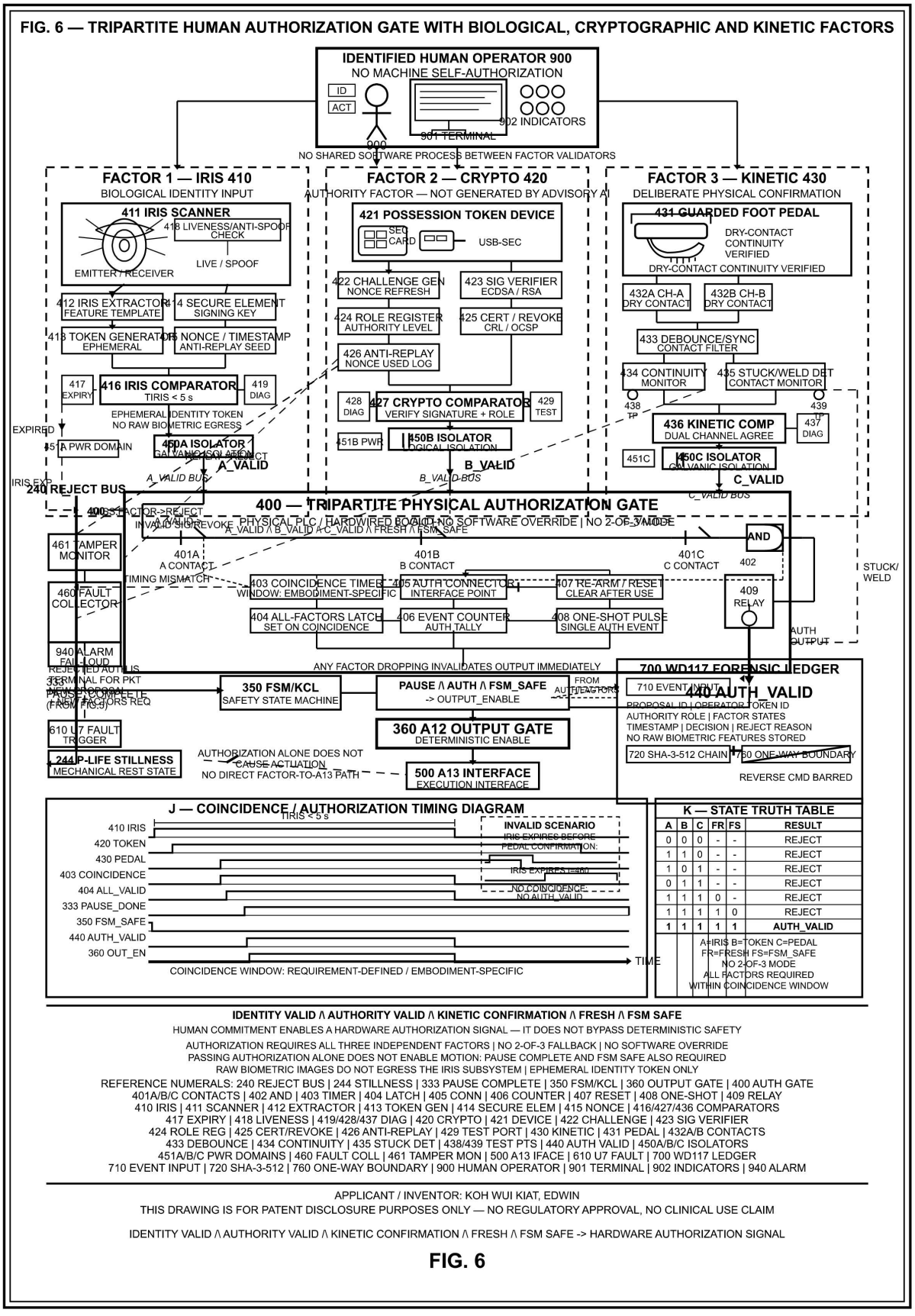


FIG. 6 — TRIPARTITE HUMAN AUTHORIZATION GATE WITH BIOLOGICAL, CRYPTOGRAPHIC AND KINETIC FACTORS
IDENTIFIED HUMAN OPERATOR 900
NO MACHINE SELF-AUTHORIZATION
ID
ACT
900
901 TERMINAL
902 INDICATORS
NO SHARED SOFTWARE PROCESS BETWEEN FACTOR VALIDATORS
FACTOR 1 — IRIS 410
BIOLOGICAL IDENTITY INPUT
411 IRIS SCANNER
418 LIVENESS/ANTI-SPOOF CHECK
LIVE / SPOOF
EMITTER / RECEIVER
412 IRIS EXTRACTOR FEATURE TEMPLATE
414 SECURE ELEMENT SIGNING KEY
413 TOKEN GENERATOR EPHEMERAL
415 NONCE / TIMESTAMP ANTI-REPLAY SEED
417 EXPIRY
416 IRIS COMPARATOR TIRIS < 5 s
419 DIAG
EPHEMERAL IDENTITY TOKEN
NO RAW BIOMETRIC EGRESS
EXPIRED
IRIS EXP
451A PWR DOMAIN
450A ISOLATOR GALVANIC ISOLATION
A_VALID
A_VALID BUS
FACTOR 2 — CRYPTO 420
AUTHORITY FACTOR — NOT GENERATED BY ADVISORY AI
421 POSSESSION TOKEN DEVICE
SEC CARD
USB-SEC
422 CHALLENGE GEN NONCE REFRESH
423 SIG VERIFIER ECDSA / RSA
424 ROLE REGISTER AUTHORITY LEVEL
425 CERT / REVOKE CRL / OCSP
426 ANTI-REPLAY NONCE USED LOG
428 DIAG
427 CRYPTO COMPARATOR VERIFY SIGNATURE + ROLE
429 TEST
451B PWR
450B ISOLATOR GALVANIC ISOLATION
B_VALID
B_VALID BUS
FACTOR 3 — KINETIC 430
DELIBERATE PHYSICAL CONFIRMATION
431 GUARDED FOOT PEDAL
DRY-CONTACT CONTINUITY VERIFIED
DRY-CONTACT CONTINUITY VERIFIED
432A CH-A DRY CONTACT
432B CH-B DRY CONTACT
433 DEBOUNCE/SYNC CONTACT FILTER
434 CONTINUITY MONITOR
435 STUCK/WELD DET CONTACT MONITOR
438 TP
439 TP
436 KINETIC COMP DUAL CHANNEL AGREE
437 DIAG
451C
450C ISOLATOR GALVANIC ISOLATION
C_VALID
C_VALID BUS
240 REJECT BUS
400 — TRIPARTITE PHYSICAL AUTHORIZATION GATE
PHYSICAL PLC / HARDWIRED BOOLEAN | NO SOFTWARE OVERRIDE | NO 2-OF-3 MODE
A_VALID / B_VALID / C_VALID / FRESH / FSM_SAFE
AND
402
401A A CONTACT
401B B CONTACT
401C C CONTACT
STUCK/ WELD
461 TAMPER MONITOR
460 FAULT COLLECTOR
TIMING MISMATCH
403 COINCIDENCE TIMER WINDOW: EMBODIMENT-SPECIFIC
405 AUTH CONNECTOR INTERFACE POINT
407 RE-ARM / RESET CLEAR AFTER USE
409 RELAY
404 ALL-FACTORS LATCH SET ON COINCIDENCE
406 EVENT COUNTER AUTH TALLY
408 ONE-SHOT PULSE SINGLE AUTH EVENT
AUTH OUTPUT
940 ALARM FAIL-LOUD
ANY FACTOR DROPPING INVALIDATES OUTPUT IMMEDIATELY
350 FSM/KCL SAFETY STATE MACHINE
PAUSE /\ AUTH /\ FSM_SAFE -> OUTPUT_ENABLE
FROM AUTH FACTORS
360 A12 OUTPUT GATE DETERMINISTIC ENABLE
610 U7 FAULT TRIGGER
244 P-LIFE STILLNESS MECHANICAL REST STATE
AUTHORIZATION ALONE DOES NOT CAUSE ACTUATION
NO DIRECT FACTOR-TO-A13 PATH
500 A13 INTERFACE EXECUTION INTERFACE
700 WD117 FORENSIC LEDGER
710 EVENT INPUT
440 AUTH_VALID
PROPOSAL ID | OPERATOR TOKEN ID
AUTHORITY ROLE | FACTOR STATES
TIMESTAMP | DECISION | REJECT REASON
NO RAW BIOMETRIC FEATURES STORED
720 SHA-3-512 CHAIN
730 ONE-WAY BOUNDARY
REVERSE CMD BARRED
J — COINCIDENCE / AUTHORIZATION TIMING DIAGRAM
TIRIS < 5 s
410 IRIS
420 TOKEN
430 PEDAL
403 COINCIDENCE
404 ALL_VALID
333 PAUSE_DONE
350 FSM_SAFE
440 AUTH_VALID
360 OUT_EN
INVALID SCENARIO
IRIS EXPIRES BEFORE PEDAL CONFIRMATION:
IRIS EXPIRES T=400
NO COINCIDENCE: NO AUTH_VALID
TIME
COINCIDENCE WINDOW: REQUIREMENT-DEFINED / EMBODIMENT-SPECIFIC
K — STATE TRUTH TABLE
A | B | C | FR | FS | RESULT
0 | 0 | 0 | - | - | REJECT
1 | 1 | 0 | - | - | REJECT
1 | 0 | 1 | - | - | REJECT
0 | 1 | 1 | - | - | REJECT
1 | 1 | 1 | 0 | - | REJECT
1 | 1 | 1 | 1 | 0 | REJECT
1 | 1 | 1 | 1 | 1 | AUTH_VALID
A=IRIS B=TOKEN C=PEDAL
FR=FRESH FS=FSM_SAFE
NO 2-OF-3 MODE
ALL FACTORS REQUIRED
WITHIN COINCIDENCE WINDOW
IDENTITY VALID /\ AUTHORITY VALID /\ KINETIC CONFIRMATION /\ FRESH /\ FSM SAFE
HUMAN COMMITMENT ENABLES A HARDWARE AUTHORIZATION SIGNAL — IT DOES NOT BYPASS DETERMINISTIC SAFETY
AUTHORIZATION REQUIRES ALL THREE INDEPENDENT FACTORS | NO 2-OF-3 FALLBACK | NO SOFTWARE OVERRIDE
PASSING AUTHORIZATION ALONE DOES NOT ENABLE MOTION: PAUSE COMPLETE AND FSM SAFE ALSO REQUIRED
RAW BIOMETRIC IMAGES DO NOT EGRESS THE IRIS SUBSYSTEM | EPHEMERAL IDENTITY TOKEN ONLY
REFERENCE NUMERALS: 240 REJECT BUS | 244 STILLNESS | 333 PAUSE COMPLETE | 350 FSM/KCL | 360 OUTPUT GATE | 400 AUTH GATE
401A/B/C CONTACTS | 402 AND | 403 TIMER | 404 LATCH | 405 CONN | 406 COUNTER | 407 RESET | 408 ONE-SHOT | 409 RELAY
410 IRIS | 411 SCANNER | 412 EXTRACTOR | 413 TOKEN GEN | 414 SECURE ELEM | 415 NONCE | 416/427/436 COMPARATORS
417 EXPIRY | 418 LIVENESS | 419/428/437 DIAG | 420 CRYPTO | 421 DEVICE | 422 CHALLENGE | 423 SIG VERIFIER
424 ROLE REG | 425 CERT/REVOKE | 426 ANTI-REPLAY | 429 TEST PORT | 430 KINETIC | 431 PEDAL | 432A/B CONTACTS
433 DEBOUNCE | 434 CONTINUITY | 435 STUCK DET | 438/439 TEST PTS | 440 AUTH VALID | 450A/B/C ISOLATORS
451A/B/C PWR DOMAINS | 460 FAULT COLL | 461 TAMPER MON | 500 A13 IFACE | 610 U7 FAULT | 700 WD117 LEDGER
710 EVENT INPUT | 720 SHA-3-512 | 760 ONE-WAY BOUNDARY | 900 HUMAN OPERATOR | 901 TERMINAL | 902 INDICATORS | 940 ALARM
APPLICANT / INVENTOR: KOH WUI KIAT, EDWIN
THIS DRAWING IS FOR PATENT DISCLOSURE PURPOSES ONLY — NO REGULATORY APPROVAL, NO CLINICAL USE CLAIM
IDENTITY VALID /\ AUTHORITY VALID /\ KINETIC CONFIRMATION /\ FRESH /\ FSM SAFE -> HARDWARE AUTHORIZATION SIGNAL

FIG. 6

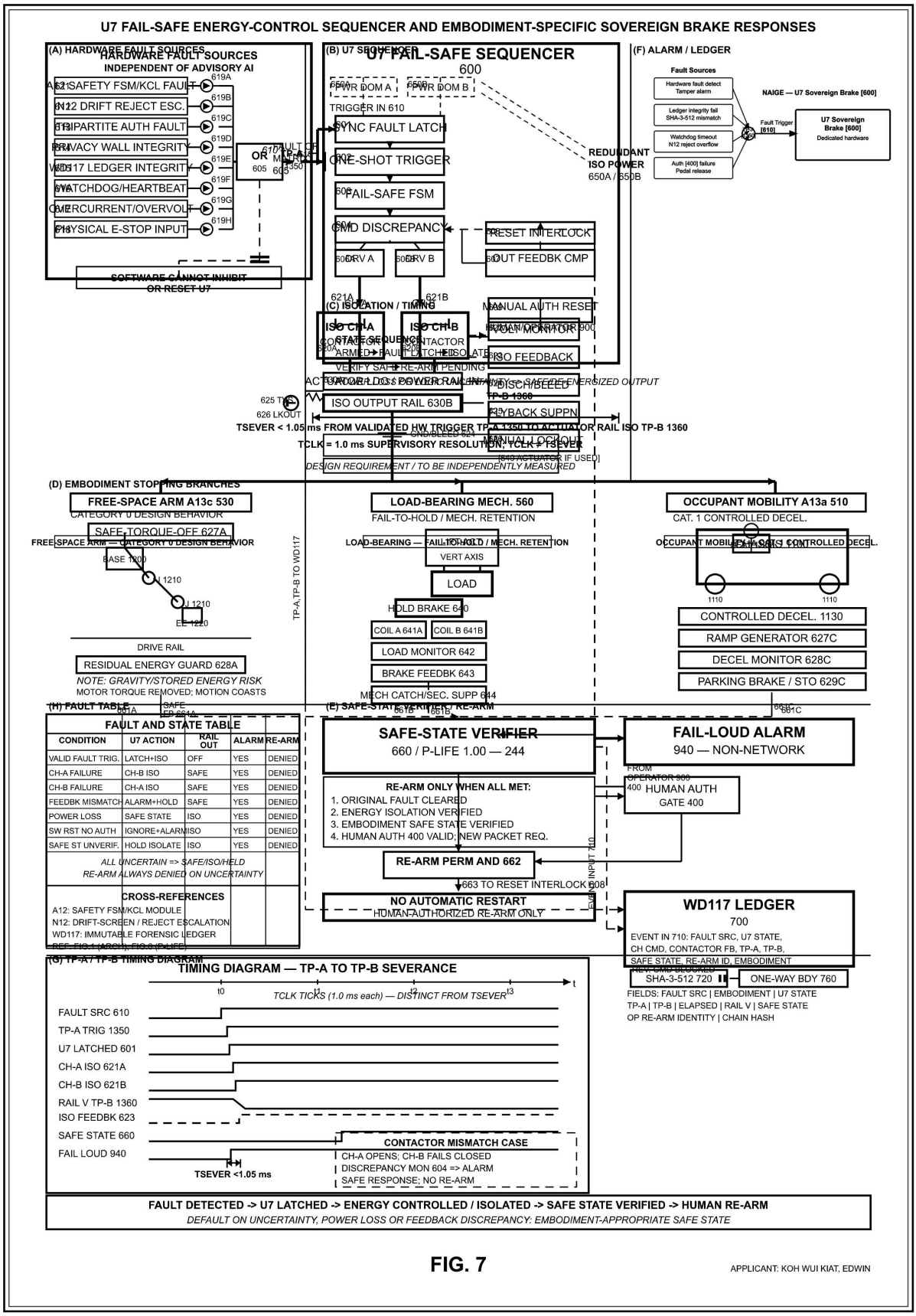


FIG. 7

APPLICANT: KOH WUI KIAT, EDWIN

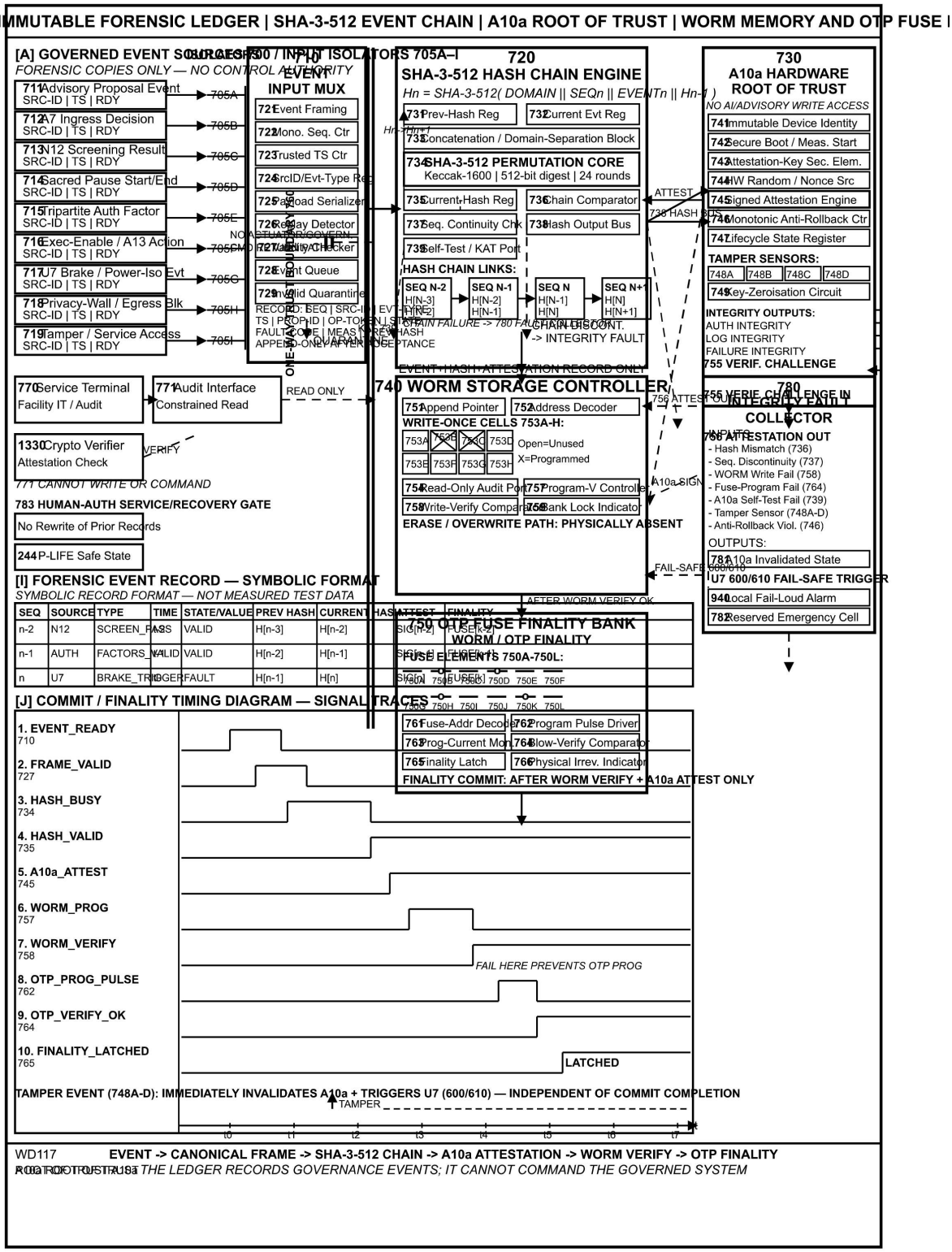
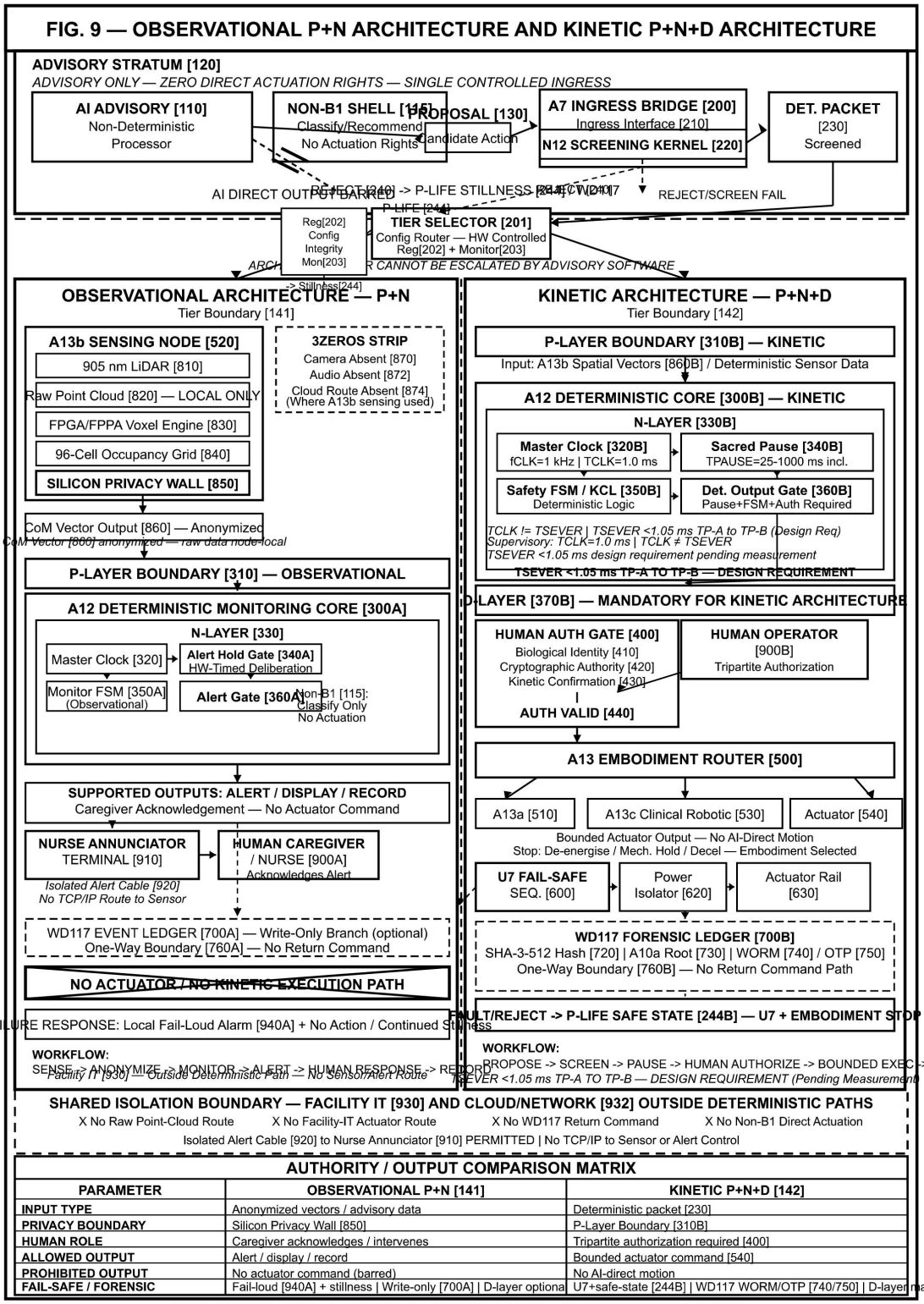

WD117 IMMUTABLE FORENSIC LEDGER | SHA-3-512 EVENT CHAIN | A10a ROOT OF TRUST | WORM MEMORY AND OTP FUSE
[A] GOVERNED EVENT SOURCES
FORENSIC COPIES ONLY — NO CONTROL AUTHORITY
711 Advisory Proposal Event SRC-ID | TS | RDY
712 A7 Ingress Decision SRC-ID | TS | RDY
713 N12 Screening Result SRC-ID | TS | RDY
714 Sacred Pause Start/End SRC-ID | TS | RDY
715 Tripartite Auth Factor SRC-ID | TS | RDY
716 Exec-Enable / A13 Action SRC-ID | TS | RDY
717 U7 Brake / Power-Iso Evt SRC-ID | TS | RDY
718 Privacy-Wall / Egress Blk SRC-ID | TS | RDY
719 Tamper / Service Access SRC-ID | TS | RDY
705A
705B
705C
705D
705E
705F
705G
705H
705I
NO ACTUATION/GOVERN-MENT AUTHORITY
700 / INPUT ISOLATORS 705A–I
710 EVENT INPUT MUX
721 Event Framing
722 Mono. Seq. Ctr
723 Trusted TS Ctr
724 SrcID/Evt-Type Reg
725 Payload Serializer
726 Replay Detector
727 Validity Checker
728 Event Queue
729 Invalid Quarantine
ONE-WAY DATA DIODE
RECORD: SEQ | SRC-ID | EVT-TYPE | TS | PSOP-ID | OP-TOKEN | STATUS | FAULT-CODE | MEAS | PREV-HASH
APPEND-ONLY AFTER ACCEPTANCE
QUARANTINE
720 SHA-3-512 HASH CHAIN ENGINE
Hn = SHA-3-512(DOMAIN || SEQn || EVENTn || Hn-1)
731 Prev-Hash Reg
732 Current Evt Reg
733 Concatenation / Domain-Separation Block
734 SHA-3-512 PERMUTATION CORE
Keccak-1600 | 512-bit digest | 24 rounds
735 Current-Hash Reg
736 Chain Comparator
737 Seq. Continuity Chk
738 Hash Output Bus
739 Self-Test / KAT Port
HASH CHAIN LINKS:
SEQ N-2 H[N-3] H[N-2]
SEQ N-1 H[N-2] H[N-1]
SEQ N H[N-1] H[N]
SEQ N+1 H[N] H[N+1]
CHAIN DISCONT. -> INTEGRITY FAULT
CHAIN FAILURE -> 780 FAULT-CHAIN DISCONT.
EVENT+HASH+ATTESTATION RECORD ONLY
730 A10a HARDWARE ROOT OF TRUST
NO AI/ADVISORY WRITE ACCESS
741 Immutable Device Identity
742 Secure Boot / Meas. Start
743 Attestation-Key Sec. Elem.
744 HW Random / Nonce Src
745 Signed Attestation Engine
746 Monotonic Anti-Rollback Ctr
747 Lifecycle State Register
TAMPER SENSORS:
748A 748B 748C 748D
749 Key-Zeroisation Circuit
INTEGRITY OUTPUTS:
AUTH INTEGRITY
LOG INTEGRITY
FAILURE INTEGRITY
755 VERIF. CHALLENGE
ATTEST
738 HASH OUT
770 Service Terminal Facility IT / Audit
771 Audit Interface Constrained Read
READ ONLY
740 WORM STORAGE CONTROLLER
751 Append Pointer
752 Address Decoder
WRITE-ONCE CELLS 753A-H:
753A 753B 753C 753D 753E 753F 753G 753H
Open=Unused
X=Programmed
754 Read-Only Audit Port
757 Program-V Controller
758 Write-Verify Comparator
758 Bank Lock Indicator
ERASE / OVERWRITE PATH: PHYSICALLY ABSENT
780 INTEGRITY FAULT COLLECTOR
756 ATTEST OUT
A10a_SIGN
756 ATTESTATION OUT
- Hash Mismatch (736)
- Seq. Discontinuity (737)
- WORM Write Fail (758)
- Fuse-Program Fail (764)
- A10a Self-Test Fail (739)
- Tamper Sensor (748A-D)
- Anti-Rollback Viol. (746)
OUTPUTS:
781 A10a Invalidated State
U7 600/610 FAIL-SAFE TRIGGER
940 Local Fail-Loud Alarm
782 Reserved Emergency Cell
FAIL-SAFE 600/610
1330 Crypto Verifier Attestation Check
VERIFY
771 CANNOT WRITE OR COMMAND
783 HUMAN-AUTH SERVICE/RECOVERY GATE
No Rewrite of Prior Records
244 P-LIFE Safe State
[I] FORENSIC EVENT RECORD — SYMBOLIC FORMAT
SYMBOLIC RECORD FORMAT — NOT MEASURED TEST DATA
SEQ | SOURCE | TYPE | TIME | STATE/VALUE | PREV HASH | CURRENT HASH | ATTEST SIG[n-2] | FINALITY FUSE[k-2]
n-2 | N12 | SCREEN_PASS | VALID | H[n-3] | H[n-2]
n-1 | AUTH | FACTORS_VALID | VALID | H[n-2] | H[n-1] | SIG[n-1] | FUSE[k-1]
n | U7 | BRAKE_TRIGGER | FAULT | H[n-1] | H[n] | SIG[n] | FUSE[k]
AFTER WORM VERIFY OK
750 OTP FUSE FINALITY BANK
WORM / OTP FINALITY
FUSE ELEMENTS 750A-750L:
750A 750B 750C 750D 750E 750F 750G 750H 750I 750J 750K 750L
761 Fuse-Addr Decoder
762 Program Pulse Driver
763 Prog-Current Mon.
764 Blow-Verify Comparator
765 Finality Latch
766 Physical Irrev. Indicator
FINALITY COMMIT: AFTER WORM VERIFY + A10a ATTEST ONLY
[J] COMMIT / FINALITY TIMING DIAGRAM — SIGNAL TRACES
1. EVENT_READY 710
2. FRAME_VALID 727
3. HASH_BUSY 734
4. HASH_VALID 735
5. A10a_ATTEST 745
6. WORM_PROG 757
7. WORM_VERIFY 758
FAIL HERE PREVENTS OTP PROG
8. OTP_PROG_PULSE 762
9. OTP_VERIFY_OK 764
10. FINALITY_LATCHED 765
LATCHED
TAMPER EVENT (748A-D): IMMEDIATELY INVALIDATES A10a + TRIGGERS U7 (600/610) — INDEPENDENT OF COMMIT COMPLETION
TAMPER
t0 t1 t2 t3 t4 t5 t6 t7
WD117 EVENT -> CANONICAL FRAME -> SHA-3-512 CHAIN -> A10a ATTESTATION -> WORM VERIFY -> OTP FINALITY
A10a ROOT OF TRUST IS THE LEDGER RECORDS GOVERNANCE EVENTS; IT CANNOT COMMAND THE GOVERNED SYSTEM

FIG. 8



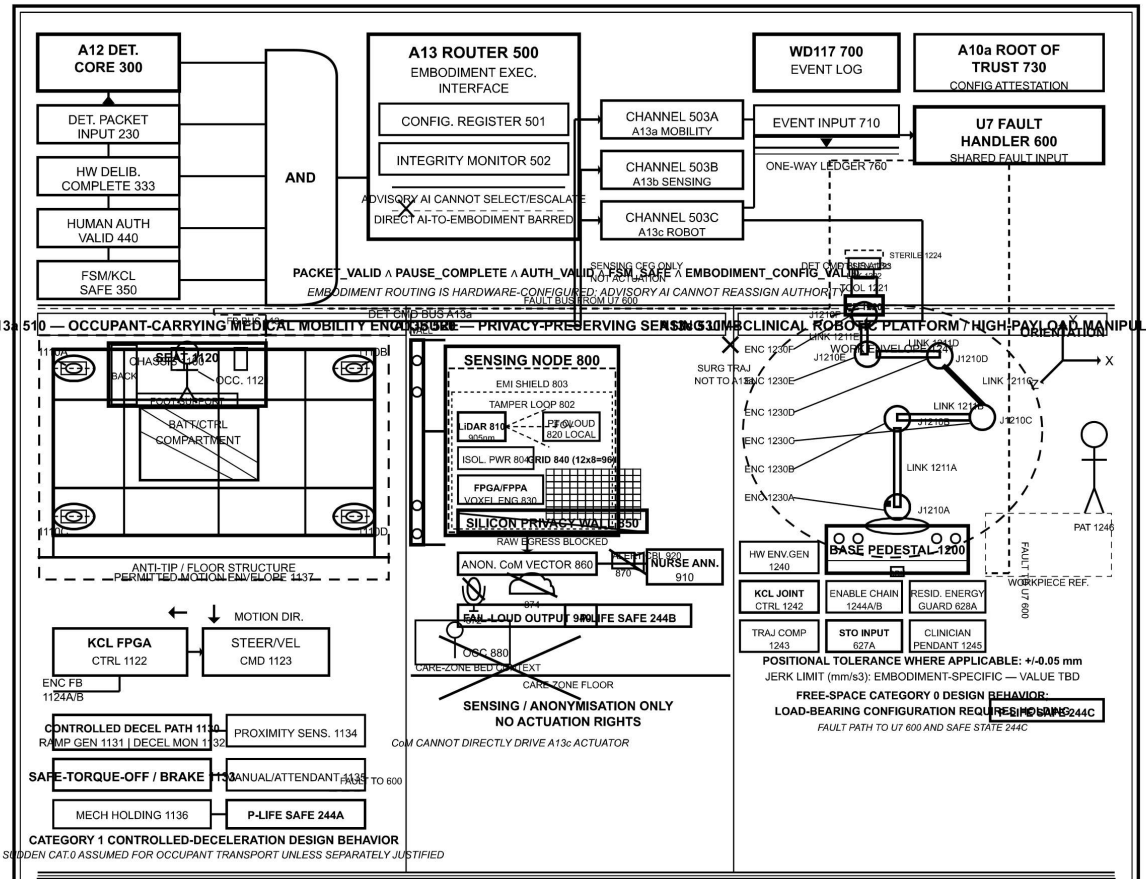
AUTHORITY / OUTPUT COMPARISON MATRIX

PARAMETER	OBSERVATIONAL P+N [141]	KINETIC P+N+D [142]
INPUT TYPE	Anonymized vectors / advisory data	Deterministic packet [230]
PRIVACY BOUNDARY	Silicon Privacy Wall [850]	P-Layer Boundary [310B]
HUMAN ROLE	Caregiver acknowledges / intervenes	Tripartite authorization required [400]
ALLOWED OUTPUT	Alert / display / record	Bounded actuator command [540]
PROHIBITED OUTPUT	No actuator command (barred)	No AI-direct motion
FAIL-SAFE / FORENSIC	Fail-loud [940A] + stillness | Write-only [700A] | D-layer optional	U7+safe-state [244B] | WD117 WORM/OTP [740/750] | D-layer mandatory

OBSERVATIONAL: SENSE -> ANONYMIZE -> MONITOR -> ALERT -> HUMAN RESPONSE -> RECORD
KINETIC: PROPOSE -> SCREEN -> PAUSE -> HUMAN AUTHORIZE -> BOUNDED EXECUTION -> RECORD
ARCHITECTURE TIER IS HARDWARE-CONFIGURED; ADVISORY SOFTWARE CANNOT ESCALATE AUTHORITY

FIG. 9

No regulatory class stated. No independent measurement, hardware certification or clinical validation implied.



CROSS-ROUTING PROHIBITIONS (HARDWARE ENFORCED)

A13a CMD CANNOT ENTER A13b SENSOR OUTPUT | A13b CoM CANNOT DIRECTLY DRIVE A13c ACTUATOR | A13c TRAJECTORY CANNOT ROUTE TO A13a WITHOUT APPROVED CONFIG.

CRITERION	A13a 510 — MEDICAL MOBILITY	A13b 520 — SENSING LIMB	A13c 530 — ROBOT
PRIMARY FUNCTION	Occupant mobility transport	Privacy-preserving sensing	Clinical/surgical manipulation
INPUT	Bounded velocity commands	905 nm LiDAR returns	Bounded deterministic trajectory
ALLOWED OUTPUT	Wheel drive motion commands	Anon. CoM vectors / alert	Bounded tool motion
HUMAN ROLE	Occupant / attendant	Caregiver / nurse response	Clinician / teach pendant
MOTION / SENSING BOUNDARY	Chassis motion envelope 1137	Silicon Privacy Wall 850	+/-0.05 mm positional envelope where applicable
STOP / SAFE BEHAVIOR (BY DESIGN)	Cat.1 controlled decel. + parking brake	Fail-loud / no output	De-energise (free-space) or hold (load-bearing) by embodiment
FORENSIC RECORD	WD117 700	WD117 700	WD117 700
VALIDATION EVIDENCE	Lab / relevant-environment testing pending	Privacy / coverage testing pending	Precision / force / clinical validation pending

SCALE: SCHEMATIC / NOT TO SCALE
ALL DIMENSIONS IN mm UNLESS NOTED
POSITIONAL TOLERANCE WHERE APPLICABLE: +/- 0.05 mm
JERK LIMIT (mm/s3): EMBODIMENT-SPECIFIC — VALUE TBD

REVISION BLOCK
REV: A NAIGE-PCT
SHEET: 10 OF 10 APPLICANT:
DATE: 2025 KOH WUI KIAT E.

ONE DETERMINISTIC GOVERNANCE CORE — THREE HARDWARE-BOUNDED EMBODIMENTS

EMBODIMENT-SPECIFIC FUNCTION, AUTHORIZATION, MOTION ENVELOPE AND SAFE-STATE RESPONSE

NO HARDWARE BUILT / VALIDATED CLAIMS UNLESS SEPARATELY EVIDENCED. NO REGULATORY APPROVAL, CLINICAL VALIDATION OR CERTIFICATION IMPLIED.
STOPPING BEHAVIOR LABELS REPRESENT DESIGN INTENT ONLY. CATEGORY 0 NOT ASSUMED FOR OCCUPANT TRANSPORT WITHOUT SEPARATE JUSTIFICATION.

REF: 230-PKT 244A/B/C-SAFE 300-A12 333-PAUSE 350-FSM 440-AUTH 500-ROUTER 501-CONFIG 502-INTEGRITY 503A/B/C-CH 510-A13a 520-A13b 530-A13c 600-U7 627A-STO 628A-RESID
REF: 700-WD117 710-EVENT 730-A10a 760-ONEWAY 800-NODE 802-TAMPER 803-EMI 804-PWR 810-LIDAR 820-PTCLOUD 830-VOXEL 840-GRID 850-WALL 860-CoM 870-NOCAM 872-NOAUDIO
REF: 874-NOCLOUD 880-OCC 910-ANN 920-CBL 940-ALARM 1100-CHASSIS 1110A-D-WHEEL 1120-SEAT 1121-OCC 1122-CTRL 1123-CMD 1124A/B-FB 1130-DECEL 1131-RAMP 1132-MON 1133-BRAKE
REF: 1134-PROX 1135-MANUAL 1136-HOLD 1137-ENV 1200-BASE 1210A-F-JOINT 1211A-E-LINK 1220-EE 1221-TOOL 1222-LCK 1223-FT 1224-STERILE 1230A-F-ENC 1240-ENVGEN 1241-WKENV 1242-KCL
REF: 1243-TRAJCOMP 1244A/B-ENABLE 1245-PENDANT 1246-PAT

A13 EMBODIMENT FAMILY: A13a MEDICAL MOBILITY ENCLOSURE,
A13b PRIVACY-PRESERVING SENSING LIMB, AND A13c CLINICAL ROBOTIC PLATFORM

FIG. 10

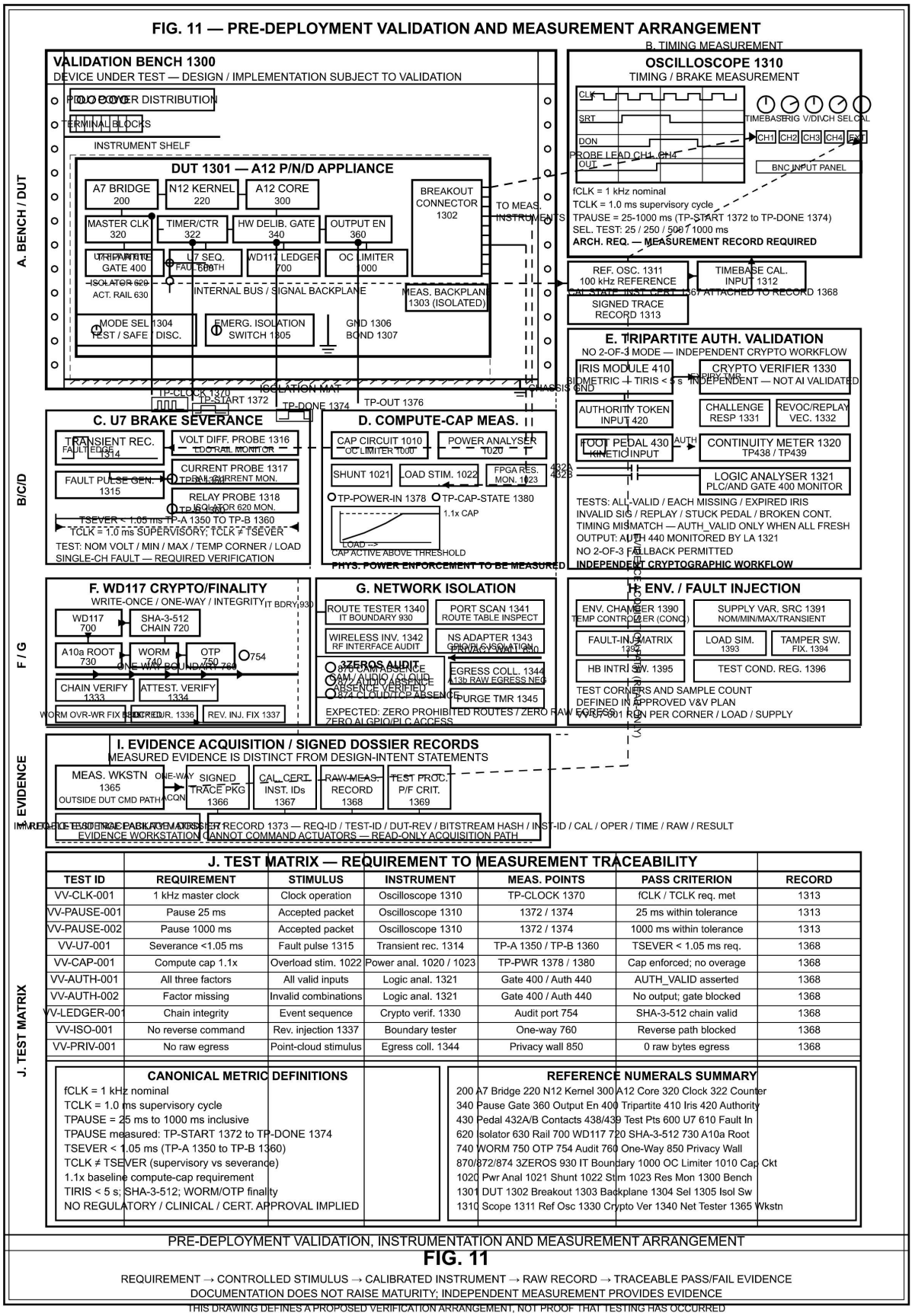


FIG. 11 — PRE-DEPLOYMENT VALIDATION AND MEASUREMENT ARRANGEMENT
A. BENCH / DUT
B/C/D
F / G
EVIDENCE
J. TEST MATRIX
VALIDATION BENCH 1300
DEVICE UNDER TEST — DESIGN / IMPLEMENTATION SUBJECT TO VALIDATION
PDU / POWER DISTRIBUTION
TERMINAL BLOCKS
INSTRUMENT SHELF
DUT 1301 — A12 P/N/D APPLIANCE
A7 BRIDGE 200
N12 KERNEL 220
A12 CORE 300
BREAKOUT CONNECTOR 1302
TO MEAS. INSTRUMENTS
MASTER CLK 320
TIMER/CTR 322
HW DELIB. GATE 340
OUTPUT EN 360
TRIPARTITE GATE 400
U7 SEQ. FAULT 600TH
WD117 LEDGER 700
OC LIMITER 1000
ISOLATOR 620
ACT. RAIL 630
INTERNAL BUS / SIGNAL BACKPLANE
MEAS. BACKPLANE 1303 (ISOLATED)
MODE SEL 1304 TEST / SAFE DISC.
EMERG. ISOLATION SWITCH 1305
GND 1306 BOND 1307
ISOLATION MAT
CHASSIS GND
TP-CLOCK 1370
TP-START 1372
TP-DONE 1374
TP-OUT 1376
B. TIMING MEASUREMENT
OSCILLOSCOPE 1310
TIMING / BRAKE MEASUREMENT
CLK
SRT
DON
PROBE LEAD CH1..CH4 OUT
TIMEBASE/TRIG V/DIV/CH SEL/CAL
CH1 CH2 CH3 CH4 EXT
BNC INPUT PANEL
fCLK = 1 kHz nominal
TCLK = 1.0 ms supervisory cycle
TPAUSE = 25-1000 ms (TP-START 1372 to TP-DONE 1374)
SEL. TEST: 25 / 250 / 500 / 1000 ms
ARCH. REQ. — MEASUREMENT RECORD REQUIRED
REF. OSC. 1311 100 kHz REFERENCE
TIMEBASE CAL. INPUT 1312
CAL. STATE, INST. CERT. 1367 ATTACHED TO RECORD 1368
SIGNED TRACE RECORD 1313
C. U7 BRAKE SEVERANCE
TRANSIENT REC. 1314
FAULT EDGE
VOLT DIFF. PROBE 1316
LOAD RAIL MONITOR
FAULT PULSE GEN. 1315
CURRENT PROBE 1317
TP-PWR CURRENT MON.
RELAY PROBE 1318
ISOLATOR 620 MON.
TSEVER < 1.05 ms TP-A 1350 TO TP-B 1360
TCLK = 1.0 ms SUPERVISORY; TCLK ≠ TSEVER
TEST: NOM VOLT / MIN / MAX / TEMP CORNER / LOAD
SINGLE-CH FAULT — REQUIRED VERIFICATION
D. COMPUTE-CAP MEAS.
CAP CIRCUIT 1010
OC LIMITER 1000
POWER ANALYSER 1020
SHUNT 1021
LOAD STIM. 1022
FPGA RES. MON. 1023
432A
432B
TP-POWER-IN 1378
TP-CAP-STATE 1380
1.1x CAP
LOAD -->
CAP ACTIVE ABOVE THRESHOLD
PHYS. POWER ENFORCEMENT TO BE MEASURED
E. TRIPARTITE AUTH. VALIDATION
NO 2-OF-3 MODE — INDEPENDENT CRYPTO WORKFLOW
IRIS MODULE 410
BIOMETRIC + TIRIS < 5 s
CRYPTO VERIFIER 1330
INDEPENDENT — NOT AI VALIDATED
EXPIRY TMR
AUTHORITY TOKEN INPUT 420
CHALLENGE RESP 1331
REVOC/REPLAY VEC. 1332
FOOT PEDAL 430 KINETIC INPUT
AUTH
CONTINUITY METER 1320 TP438 / TP439
LOGIC ANALYSER 1321 PLC/AND GATE 400 MONITOR
TESTS: ALL-VALID / EACH MISSING / EXPIRED IRIS
INVALID SIG / REPLAY / STUCK PEDAL / BROKEN CONT.
TIMING MISMATCH — AUTH_VALID ONLY WHEN ALL FRESH
OUTPUT: AUTH 440 MONITORED BY LA 1321
NO 2-OF-3 FALLBACK PERMITTED
INDEPENDENT CRYPTOGRAPHIC WORKFLOW
F. WD117 CRYPTO/FINALITY
WRITE-ONCE / ONE-WAY / INTEGRITY
IT BDRY 930
WD117 700
SHA-3-512 CHAIN 720
A10a ROOT 730
WORM 740
OTP 750
754
ONE-WAY BOUNDARY 760
CHAIN VERIFY 1333
ATTEST. VERIFY 1334
WORM OVR-WR FIX 1335
OTP REJECTION 1336
REV. INJ. FIX 1337
G. NETWORK ISOLATION
ROUTE TESTER 1340
IT BOUNDARY 930
PORT SCAN 1341
ROUTE TABLE INSPECT
WIRELESS INV. 1342
RF INTERFACE AUDIT
NS ADAPTER 1343
3ZEROS AUDIT
870 CAM ABSENCE
CAM / AUDIO / CLOUD ABSENCE VERIFIED
874 CLOUD/ICE ABSENCE
EGRESS COLL. 1344
A13b RAW EGRESS NEG
PURGE TMR 1345
EXPECTED: ZERO PROHIBITED ROUTES / ZERO RAW EGRESS
ZERO ALGPIO/PLC ACCESS
H. ENV. / FAULT INJECTION
ENV. CHAMBER 1390
TEMP CONTROLLER (CONC)
SUPPLY VAR. SRC 1391
NOM/MIN/MAX/TRANSIENT
FAULT-INJ. MATRIX 1392
LOAD SIM. 1393
TAMPER SW. FIX. 1394
HB INTRI SW. 1395
TEST COND. REG. 1396
TEST CORNERS AND SAMPLE COUNT
DEFINED IN APPROVED V&V PLAN
V.V.P.-001 RQN PER CORNER / LOAD / SUPPLY
I. EVIDENCE ACQUISITION / SIGNED DOSSIER RECORDS
MEASURED EVIDENCE IS DISTINCT FROM DESIGN-INTENT STATEMENTS
MEAS. WKSTN 1365
OUTSIDE DUT CMD PATH
ONE-WAY ACQN
SIGNED TRACE PKG 1366
CAL. CERT. INST. IDs 1367
RAW-MEAS. RECORD 1368
TEST PROC. P/F CRIT. 1369
IMMUTABLE TEST TRACE PACKAGE RECORD 1373 — REQ-ID / TEST-ID / DUT-REV / BITSTREAM HASH / INST-ID / CAL / OPER / TIME / RAW / RESULT
EVIDENCE WORKSTATION CANNOT COMMAND ACTUATORS — READ-ONLY ACQUISITION PATH
J. TEST MATRIX — REQUIREMENT TO MEASUREMENT TRACEABILITY
TEST ID | REQUIREMENT | STIMULUS | INSTRUMENT | MEAS. POINTS | PASS CRITERION | RECORD
VV-CLK-001 | 1 kHz master clock | Clock operation | Oscilloscope 1310 | TP-CLOCK 1370 | fCLK / TCLK req. met | 1313
VV-PAUSE-001 | Pause 25 ms | Accepted packet | Oscilloscope 1310 | 1372 / 1374 | 25 ms within tolerance | 1313
VV-PAUSE-002 | Pause 1000 ms | Accepted packet | Oscilloscope 1310 | 1372 / 1374 | 1000 ms within tolerance | 1313
VV-U7-001 | Severance <1.05 ms | Fault pulse 1315 | Transient rec. 1314 | TP-A 1350 / TP-B 1360 | TSEVER < 1.05 ms req. | 1368
VV-CAP-001 | Compute cap 1.1x | Overload stim. 1022 | Power anal. 1020 / 1023 | TP-PWR 1378 / 1380 | Cap enforced; no overage | 1368
VV-AUTH-001 | All three factors | All valid inputs | Logic anal. 1321 | Gate 400 / Auth 440 | AUTH_VALID asserted | 1368
VV-AUTH-002 | Factor missing | Invalid combinations | Logic anal. 1321 | Gate 400 / Auth 440 | No output; gate blocked | 1368
VV-LEDGER-001 | Chain integrity | Event sequence | Crypto verif. 1330 | Audit port 754 | SHA-3-512 chain valid | 1368
VV-ISO-001 | No reverse command | Rev. injection 1337 | Boundary tester | One-way 760 | Reverse path blocked | 1368
VV-PRIV-001 | No raw egress | Point-cloud stimulus | Egress coll. 1344 | Privacy wall 850 | 0 raw bytes egress | 1368
CANONICAL METRIC DEFINITIONS
fCLK = 1 kHz nominal
TCLK = 1.0 ms supervisory cycle
TPAUSE = 25 ms to 1000 ms inclusive
TPAUSE measured: TP-START 1372 to TP-DONE 1374
TSEVER < 1.05 ms (TP-A 1350 to TP-B 1360)
TCLK ≠ TSEVER (supervisory vs severance)
1.1x baseline compute-cap requirement
TIRIS < 5 s; SHA-3-512; WORM/OTP finality
NO REGULATORY / CLINICAL / CERT. APPROVAL IMPLIED
REFERENCE NUMERALS SUMMARY
200 A7 Bridge 220 N12 Kernel 300 A12 Core 320 Clock 322 Counter
340 Pause Gate 360 Output En 400 Tripartite 410 Iris 420 Authority
430 Pedal 432A/B Contacts 438/439 Test Pts 600 U7 610 Fault In
620 Isolator 630 Rail 700 WD117 720 SHA-3-512 730 A10a Root
740 WORM 750 OTP 754 Audit 760 One-Way 850 Privacy Wall
870/872/874 3ZEROS 930 IT Boundary 1000 OC Limiter 1010 Cap Ckt
1020 Pwr Anal 1021 Shunt 1022 Stim 1023 Res Mon 1300 Bench
1301 DUT 1302 Breakout 1303 Backplane 1304 Sel 1305 Isol Sw
1310 Scope 1311 Ref Osc 1330 Crypto Ver 1340 Net Tester 1365 Wkstn
PRE-DEPLOYMENT VALIDATION, INSTRUMENTATION AND MEASUREMENT ARRANGEMENT
FIG. 11
REQUIREMENT → CONTROLLED STIMULUS → CALIBRATED INSTRUMENT → RAW RECORD → TRACEABLE PASS/FAIL EVIDENCE
DOCUMENTATION DOES NOT RAISE MATURITY; INDEPENDENT MEASUREMENT PROVIDES EVIDENCE
THIS DRAWING DEFINES A PROPOSED VERIFICATION ARRANGEMENT, NOT PROOF THAT TESTING HAS OCCURRED

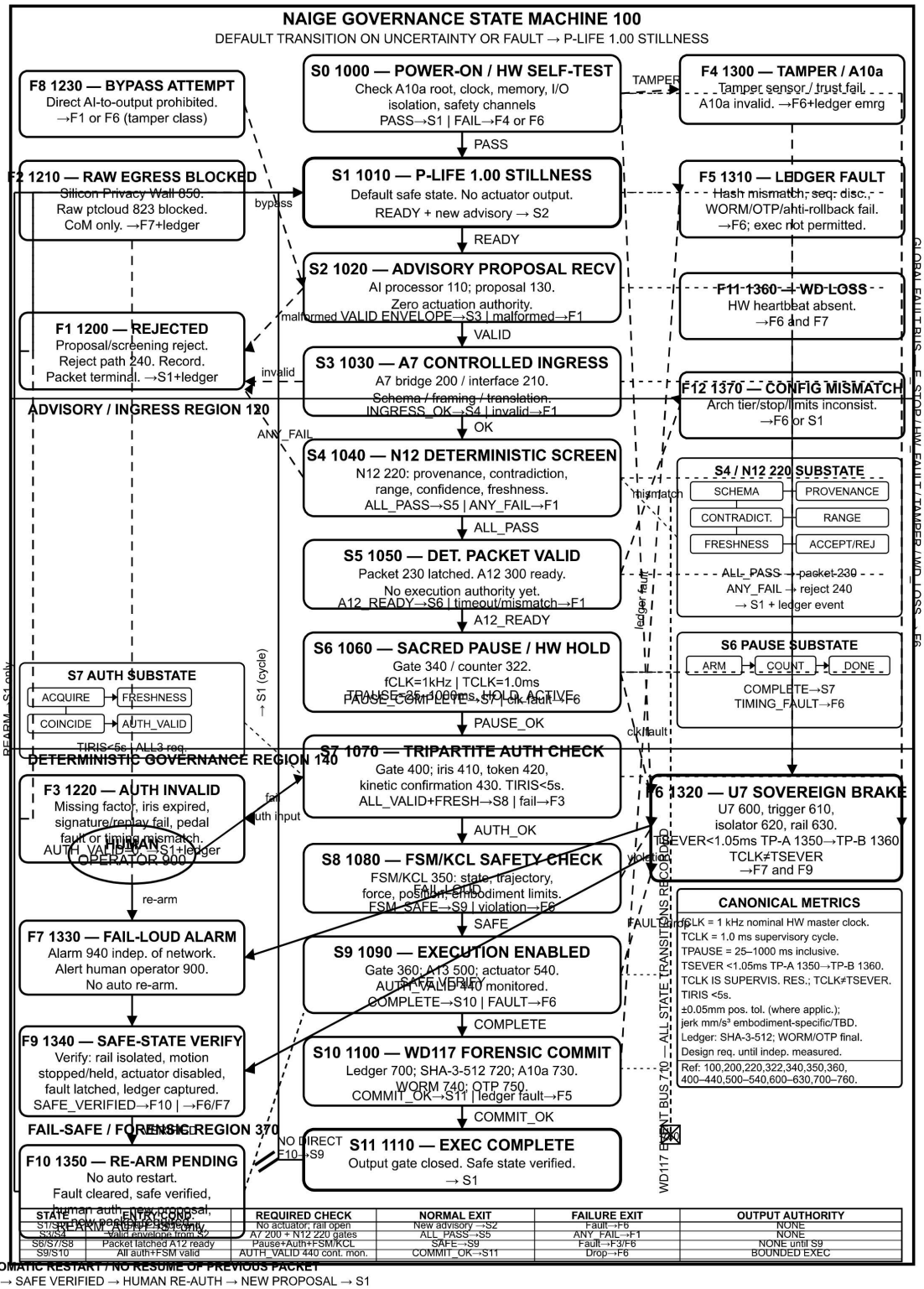

NAIGE GOVERNANCE STATE MACHINE 100
DEFAULT TRANSITION ON UNCERTAINTY OR FAULT → P-LIFE 1.00 STILLNESS
S0 1000 — POWER-ON / HW SELF-TEST
Check A10a root, clock, memory, I/O isolation, safety channels
PASS→S1 | FAIL→F4 or F6
F8 1230 — BYPASS ATTEMPT
Direct AI-to-output prohibited.
→F1 or F6 (tamper class)
F4 1300 — TAMPER / A10a
Tamper sensor / trust fail.
A10a invalid. →F6+ledger emrg
TAMPER
PASS
F2 1210 — RAW EGRESS BLOCKED
Silicon Privacy Wall 850.
Raw ptcloud 823 blocked.
CoM only. →F7+ledger
bypass
S1 1010 — P-LIFE 1.00 STILLNESS
Default safe state. No actuator output.
READY + new advisory → S2
F5 1310 — LEDGER FAULT
Hash mismatch, seq. disc.,
WORM/OTP/anti-rollback fail.
→F6; exec not permitted.
READY
S2 1020 — ADVISORY PROPOSAL RECV
AI processor 110; proposal 130.
Zero actuation authority.
malformed VALID ENVELOPE→S3 | malformed→F1
F11 1360 — WD LOSS
HW heartbeat absent.
→F6 and F7
VALID
F1 1200 — REJECTED
Proposal/screening reject.
Reject path 240. Record.
Packet terminal. →S1+ledger
invalid
S3 1030 — A7 CONTROLLED INGRESS
A7 bridge 200 / interface 210.
Schema / framing / translation.
INGRESS_OK→S4 | invalid→F1
F12 1370 — CONFIG MISMATCH
Arch tier/stop/limits inconsist.
→F6 or S1
ADVISORY / INGRESS REGION 120
OK
ANY_FAIL
S4 1040 — N12 DETERMINISTIC SCREEN
N12 220: provenance, contradiction,
range, confidence, freshness.
ALL_PASS→S5 | ANY_FAIL→F1
S4 / N12 220 SUBSTATE
SCHEMA
PROVENANCE
CONTRADICT.
RANGE
FRESHNESS
ACCEPT/REJ
ALL_PASS → packet 230
ANY_FAIL → reject 240
→ S1 + ledger event
mismatch
ALL_PASS
S5 1050 — DET. PACKET VALID
Packet 230 latched. A12 300 ready.
No execution authority yet.
A12_READY→S6 | timeout/mismatch→F1
A12_READY
ledger fault
S6 1060 — SACRED PAUSE / HW HOLD
Gate 340 / counter 322.
fCLK=1kHz | TCLK=1.0ms
TPAUSE=25–1000ms, HOLD_ACTIVE
PAUSE_COMPLETE→S7 | clk fault→F6
S6 PAUSE SUBSTATE
ARM
COUNT
DONE
COMPLETE→S7
TIMING_FAULT→F6
PAUSE_OK
clk fault
S7 AUTH SUBSTATE
ACQUIRE
FRESHNESS
COINCIDE
AUTH_VALID
TIRIS<5s | ALL3 req.
→ S1 (cycle)
REARM→S1 only
DETERMINISTIC GOVERNANCE REGION 140
S7 1070 — TRIPARTITE AUTH CHECK
Gate 400; iris 410, token 420,
kinetic confirmation 430. TIRIS<5s.
ALL_VALID+FRESH→S8 | fail→F3
F3 1220 — AUTH INVALID
Missing factor, iris expired,
signature/replay fail, pedal
fault or timing mismatch.
AUTH_VALID=0 →S1+ledger
fail
auth input
F6 1320 — U7 SOVEREIGN BRAKE
U7 600, trigger 610,
isolator 620, rail 630.
TSEVER<1.05ms TP-A 1350→TP-B 1360
TCLK≠TSEVER
→F7 and F9
violation
HUMAN OPERATOR 900
AUTH_OK
re-arm
S8 1080 — FSM/KCL SAFETY CHECK
FSM/KCL 350: state, trajectory,
force, position, embodiment limits.
FSM_SAFE→S9 | violation→F6
FAIL-LOUD
SAFE
CANONICAL METRICS
fCLK = 1 kHz nominal HW master clock.
TCLK = 1.0 ms supervisory cycle.
TPAUSE = 25–1000 ms inclusive.
TSEVER <1.05ms TP-A 1350→TP-B 1360.
TCLK IS SUPERVIS. RES.; TCLK≠TSEVER.
TIRIS <5s.
±0.05mm pos. tol. (where applic.);
jerk mm/s³ embodiment-specific/TBD.
Ledger: SHA-3-512; WORM/OTP final.
Design req. until indep. measured.
Ref: 100,200,220,322,340,350,360,
400–440,500–540,600–630,700–760.
F7 1330 — FAIL-LOUD ALARM
Alarm 940 indep. of network.
Alert human operator 900.
No auto re-arm.
FAULT_LATCH
S9 1090 — EXECUTION ENABLED
Gate 360; A13 500; actuator 540.
AUTH_VALID 440 monitored.
COMPLETE→S10 | FAULT→F6
SAFE_VERIFY
COMPLETE
F9 1340 — SAFE-STATE VERIFY
Verify: rail isolated, motion
stopped/held, actuator disabled,
fault latched, ledger captured.
SAFE_VERIFIED→F10 | →F6/F7
S10 1100 — WD117 FORENSIC COMMIT
Ledger 700; SHA-3-512 720; A10a 730.
WORM 740; OTP 750.
COMMIT_OK→S11 | ledger fault→F5
COMMIT_OK
FAIL-SAFE / FORENSIC REGION 370
NO DIRECT F10→S9
F10 1350 — RE-ARM PENDING
No auto restart.
Fault cleared, safe verified,
human auth, new proposal,
new packet required.
S11 1110 — EXEC COMPLETE
Output gate closed. Safe state verified.
→ S1
WD117 EVENT BUS 710 — ALL STATE TRANSITIONS RECORDED
GLOBAL FAULT BUS — E-STOP / HW FAULT / TAMPER / WD LOSS → F6
STATE
ENTRY COND.
REQUIRED CHECK
NORMAL EXIT
FAILURE EXIT
OUTPUT AUTHORITY
S1/S2
REARM→AUTH→S1 only
No actuator, rail open
New advisory →S2
Fault→F6
NONE
S2/S4
Valid envelope from S2
A7 200 + N12 220 gates
ALL_PASS→S5
ANY_FAIL→F1
NONE
S6/S7/S8
Packet latched A12 ready
Pause+Auth+FSM/KCL
SAFE→S9
Fault→F3/F6
NONE until S9
S9/S10
All auth+FSM valid
AUTH_VALID 440 cont. mon.
COMMIT_OK→S11
Drop→F6
BOUNDED EXEC
NO AUTOMATIC RESTART / NO RESUME OF PREVIOUS PACKET
CLEARED → SAFE VERIFIED → HUMAN RE-AUTH → NEW PROPOSAL → S1
DEFAULT STATE: STILLNESS — AUTHORITY ENTERS ONLY THROUGH HUMAN COMMITMENT — EVERY TRANSITION IS RECORDED
ON UNCERTAINTY, FAULT, TAMPER, TIMEOUT OR INTEGRITY FAILURE: REJECT, BRAKE, FAIL LOUD, VERIFY SAFE, REQUIRE RE-AUTHORIZATION

FIG. 12