Utility Patent Application

Patent Title

NAI 2.0 WM003™ Eldercare Fall Prevention LiDAR for HSA Class B Software as a Medical Device (SaMD) Regulatory Approval in Eldercare Sensing, Monitoring and Controlling.

Application Information

Application Type: Utility Patent (Non-Provisional)

Nice Classification: Classes 10, 44, and 45

Field of Regulatory Scope: Health Sciences Authority (HSA) Class B Software as a Medical Device (SaMD)

Technology Domain: Eldercare Constitutional Governance, Artificial Intelligence-Driven Medical Software, Biosensing and Monitoring Systems

Inventors

Edwin Koh Wui Kiat

Singapore

Date: 4th May 2026.

Assignee

Edwin Koh Wui Kiat

Priority Data

[Priority Application Number and Date to be inserted]

Field of the Invention

[0001] The present invention relates generally to artificial intelligence-based constitutional governance frameworks for Software as a Medical Device (SaMD), and more particularly to the NAI2.0 Constitutional Framework configured for Health Sciences Authority (HSA) Class B SaMD regulatory approval in the domain of eldercare. The invention encompasses constitutional governance architectures for sensing, monitoring, and controlling devices operating under Nice Classification Classes 10, 44, and 45, wherein the framework enforces regulatory compliance, ethical governance, algorithmic accountability, and patient safety constraints through a hierarchically structured constitutional layer embedded within the SaMD operational architecture.

Background of the Invention

[0002] The rapid proliferation of Software as a Medical Device in eldercare environments has created pressing regulatory, ethical, and technical challenges. Eldercare facilities and home care environments increasingly rely on intelligent sensing devices, physiological monitoring platforms, and autonomous controlling systems to ensure the health, safety, and dignity of elderly patients. These systems encompass medical devices classified under Nice Classification Class 10 (surgical, medical, dental, and veterinary apparatus and instruments), Class 44 (medical services, veterinary services, hygienic and beauty care services), and Class 45 (personal and social services rendered by others to meet the needs of individuals).

[0003] Existing SaMD frameworks lack a constitutionally binding governance layer that systematically governs the behavior of artificial intelligence engines operating within these devices. Current regulatory approaches, including those established by the Health Sciences Authority (HSA) of Singapore under its regulatory framework for SaMD, require that Class B SaMD products demonstrate clinical evidence of safety and effectiveness, risk management in compliance with ISO 14971, and quality management systems aligned with ISO 13485. However, no prior art discloses a constitutional framework that embeds enforceable governance principles directly into the computational architecture of SaMD devices as a structural regulatory compliance mechanism.

[0004] Furthermore, eldercare environments present unique clinical, ethical, and legal complexities. Elderly patients are often unable to provide real-time informed consent due to cognitive impairment, dementia, or reduced decision-making capacity. Autonomous AI-driven devices making clinical recommendations or controlling therapeutic actuators in such environments require a constitutional governance layer that preserves patient autonomy, prevents harm, ensures transparency, and maintains accountability at every level of device operation.

[0005] Prior art systems, including conventional rule-based clinical decision support systems and first-generation AI medical devices, do not address the constitutional governance of AI behavior within the regulatory architecture of HSA Class B SaMD. There exists a long-felt but unmet need in the art for a constitutional framework that is simultaneously regulatory-compliant, clinically effective, ethically sound, and technically implementable within sensing, monitoring, and controlling SaMD devices in eldercare settings.

Summary of the Invention

[0006] The present invention provides a NAI2.0 Constitutional Framework for HSA Class B SaMD Regulatory Approval, hereinafter referred to as the "Framework" or "NAI2.0 Framework," comprising a hierarchically structured constitutional governance architecture embedded within Software as a Medical Device operating in eldercare environments. The Framework governs sensing, monitoring, and controlling constitutional governance devices operating across Nice Classification Classes 10, 44, and 45.

[0007] In one aspect, the invention provides a constitutional governance layer comprising a plurality of constitutional articles, each article encoding a binding computational governance rule enforceable at runtime by a constitutional enforcement engine. The constitutional articles collectively define the permissible operational envelope of NAI2.0-compliant SaMD devices, including constraints on data acquisition, inference generation, therapeutic recommendation issuance, and actuator control commands.

[0008] In another aspect, the invention provides a constitutional compliance verification module configured to continuously evaluate the conformity of all device outputs against the constitutional articles in real time, generating compliance attestation records suitable for submission to the Health Sciences Authority as part of a Pre-Market Submission or Product Registration application for Class B SaMD classification.

[0009] In yet another aspect, the invention provides a constitutional governance registry comprising a distributed ledger-based immutable record of all constitutional enforcement events, compliance attestations, and derogation justifications, providing a comprehensive audit trail for regulatory review by the HSA and other competent authorities.

[0010] In a further aspect, the invention provides eldercare-specific constitutional governance modules tailored to the physiological, cognitive, and legal characteristics of elderly patients, including constitutional constraints on data privacy, surrogate consent management, fall detection actuation thresholds, and medication dispensation control parameters.

[0011] The NAI2.0 Constitutional Framework achieves technical advantages including enhanced regulatory traceability, reduced risk of AI-induced patient harm, improved clinical transparency, and systematic alignment with HSA SaMD regulatory requirements, ISO 14971 risk management standards, ISO 13485 quality management standards, and IEC 62304 medical device software lifecycle requirements.

Brief Description of the Figures

[0012] The accompanying figures, which are incorporated in and constitute a part of this specification, illustrate embodiments of the invention and together with the description serve to explain the principles of the invention.

[0013] **FIG. 1** is a high-level architectural block diagram of the NAI2.0 Constitutional Framework illustrating the hierarchical constitutional governance layers, the

constitutional enforcement engine, and their relationship to HSA Class B SaMD sensing, monitoring, and controlling device subsystems.

[0014] **FIG. 2** is a flowchart illustrating the constitutional compliance verification process executed by the constitutional enforcement engine at runtime, including constitutional article evaluation, compliance attestation generation, and derogation escalation procedures.

[0015] **FIG. 3** is a schematic diagram of the eldercare sensing module depicting physiological sensor arrays, constitutional data acquisition constraints, privacy-preserving signal processing pipelines, and constitutional data governance enforcement points.

[0016] **FIG. 4** is a block diagram of the eldercare monitoring module illustrating the constitutional monitoring governance layer, AI inference engine, constitutional inference validation unit, and clinical alert generation subsystem operating under constitutional constraints.

[0017] **FIG. 5** is a schematic diagram of the eldercare controlling module depicting actuator subsystems governed by constitutional control constraints, including medication dispensation actuators, mobility assistance devices, and environmental control actuators, with constitutional override mechanisms.

[0018] **FIG. 6** is a data flow diagram of the Constitutional Governance Registry, illustrating distributed ledger architecture, constitutional enforcement event recording, compliance attestation storage, and regulatory submission data packaging for HSA Pre-Market Submission.

[0019] **FIG. 7** is a diagram of the HSA Class B SaMD Regulatory Alignment Matrix, mapping each constitutional article of the NAI2.0 Framework to corresponding HSA regulatory requirements, ISO 14971 risk controls, ISO 13485 quality elements, and IEC 62304 software lifecycle requirements.

[0020] **FIG. 8** is a process flow diagram of the surrogate consent management constitutional module illustrating the constitutional governance of consent acquisition, verification, and revocation processes applicable to cognitively impaired elderly patients.

Detailed Description of the Preferred Embodiments

I. Overview of the NAI2.0 Constitutional Framework

[0021] Referring now to FIG. 1, the NAI2.0 Constitutional Framework 100 comprises a multi-tiered constitutional governance architecture operatively coupled to HSA Class B SaMD device subsystems 102. The Framework 100 includes a Constitutional Layer 110, a Constitutional Enforcement Engine 120, a Constitutional Compliance Verification Module 130, a Constitutional Governance Registry 140, and Eldercare Constitutional Governance Modules 150. These components are operatively integrated within a SaMD software architecture that governs sensing devices 160, monitoring devices 170, and controlling devices 180 operating in eldercare environments.

[0022] In a preferred embodiment, the Constitutional Layer 110 comprises a plurality of constitutional articles 112 organized into constitutional chapters 114. Each constitutional article 112 encodes a binding governance rule expressed as a computationally executable constraint function. The constitutional articles 112 are hierarchically ordered such that higher-order articles governing patient safety and fundamental rights supersede lower-order articles governing operational efficiency and device performance optimization.

[0023] The Constitutional Enforcement Engine 120 is a dedicated computational module configured to evaluate all device operational decisions against the constitutional articles 112 in real time. The Constitutional Enforcement Engine 120 operates as a Constitutional Middleware Layer positioned between the AI inference engine 122 and the device output subsystems 124, ensuring that no device output is issued without prior constitutional validation.

[0024] In an alternative embodiment, the Constitutional Enforcement Engine 120 operates as a hypervisor-level process with elevated system privileges, rendering it tamper-resistant against modification by the AI inference engine 122 or any other application-layer process. This architectural arrangement ensures the constitutional supremacy of the Framework 100 over all operational subsystems of the SaMD device.

II. Constitutional Articles and Chapters

[0025] The Constitutional Layer 110 of the NAI2.0 Framework comprises a plurality of constitutional chapters, each governing a distinct domain of SaMD device behavior. The following embodiment describes the constitutional chapters and their constituent articles applicable to eldercare SaMD devices under HSA Class B classification.

[0026] **Constitutional Chapter 1: Patient Safety and Primacy of Care.** Constitutional Article 1.1 provides that all device operational decisions shall prioritize the physical safety and wellbeing of the elderly patient above all other operational objectives. Constitutional Article 1.2 provides that no device output shall initiate, continue, or recommend a clinical action that the constitutional risk engine has assessed as presenting an unacceptable residual risk in accordance with ISO 14971 risk acceptability criteria. Constitutional Article 1.3 provides that in the event of constitutional article conflict, patient safety provisions shall prevail.

[0027] **Constitutional Chapter 2: Patient Dignity and Autonomy.** Constitutional Article 2.1 provides that all data collection, processing, and sharing operations shall respect the dignity and autonomy of the elderly patient. Constitutional Article 2.2 provides that the SaMD device shall not collect, process, or transmit biometric, physiological, or behavioral data without a constitutionally validated consent record. Constitutional Article 2.3 provides that the device shall support surrogate consent management for cognitively impaired patients in accordance with applicable legal frameworks and the constitutional surrogate consent module described herein.

[0028] **Constitutional Chapter 3: Algorithmic Transparency and Explainability.** Constitutional Article 3.1 provides that every clinical recommendation generated by the AI inference engine 122 shall be accompanied by a constitutionally compliant explanation record articulating the primary factors contributing to the recommendation. Constitutional Article 3.2 provides that the explanation record shall be rendered in natural language comprehensible to non-specialist clinical staff and,

where appropriate, to the patient or their legal representative. Constitutional Article 3.3 provides that the device shall maintain an explanation audit log accessible to the HSA upon regulatory request.

[0029] **Constitutional Chapter 4: Regulatory Compliance and Accountability.** Constitutional Article 4.1 provides that the device shall at all times maintain compliance with applicable HSA SaMD regulatory requirements including but not limited to HSA's Regulatory Framework for Software as a Medical Device. Constitutional Article 4.2 provides that the device shall generate and preserve constitutional compliance attestation records sufficient to support a HSA Class B SaMD Pre-Market Submission. Constitutional Article 4.3 provides that the device manufacturer shall maintain a constitutional governance accountability record identifying responsible parties for each constitutional enforcement decision.

[0030] **Constitutional Chapter 5: Data Governance and Privacy.** Constitutional Article 5.1 provides that all personal data processed by the device shall be governed in accordance with the Personal Data Protection Act (PDPA) of Singapore and applicable international data protection standards. Constitutional Article 5.2 provides that the device shall implement constitutional data minimization constraints limiting data collection to the minimum necessary for the declared clinical purpose. Constitutional Article 5.3 provides that constitutional data retention schedules shall be enforced automatically by the Constitutional Enforcement Engine 120.

[0031] **Constitutional Chapter 6: Operational Integrity and Fail-Safe Governance.** Constitutional Article 6.1 provides that in the event of constitutional enforcement engine failure, the device shall immediately enter a constitutionally mandated safe state, discontinuing all clinical recommendation outputs and actuator control commands until constitutional enforcement is restored. Constitutional Article 6.2 provides that the device shall implement constitutional watchdog processes that continuously monitor the operational status of the Constitutional Enforcement Engine 120. Constitutional Article 6.3 provides that all safe-state transitions shall be recorded in the Constitutional Governance Registry 140 and reported to the designated clinical supervisor within a constitutionally specified time period not to exceed **120 seconds**.

III. Eldercare Sensing Module

[0032] Referring now to FIG. 3, the eldercare sensing module 160 comprises a plurality of physiological sensor arrays 162 operatively coupled to a constitutional data acquisition controller 164. The physiological sensor arrays 162 include, without limitation, electrocardiographic (ECG) sensors, photoplethysmographic (PPG) sensors, accelerometric fall detection sensors, continuous glucose monitoring sensors, skin temperature sensors, respiratory rate sensors, and ambient environment sensors.

[0033] The constitutional data acquisition controller 164 enforces constitutional data acquisition constraints derived from Constitutional Chapter 2 and Constitutional Chapter 5, ensuring that sensor data streams are acquired only within constitutionally validated consent boundaries and are processed through a privacy-preserving signal processing pipeline 166 prior to transmission to the monitoring module 170.

[0034] In a preferred embodiment, the privacy-preserving signal processing pipeline 166 implements differential privacy mechanisms, on-device federated learning processes, and constitutional data anonymization protocols, collectively ensuring that

individually identifiable physiological data is not transmitted beyond the constitutional data governance boundary 168 without explicit constitutional authorization.

[0035] The sensing module 160 further comprises a constitutional sensing compliance attestor 169 configured to generate per-session sensing compliance attestation records documenting adherence to constitutional data acquisition constraints, for inclusion in the Constitutional Governance Registry 140.

IV. Eldercare Monitoring Module

[0036] Referring now to FIG. 4, the eldercare monitoring module 170 comprises an AI inference engine 172 operatively coupled to a constitutional inference validation unit 174. The AI inference engine 172 receives privacy-preserving physiological data streams from the sensing module 160 and generates clinical inference outputs 176 comprising patient condition assessments, risk stratification scores, and clinical alert recommendations.

[0037] The constitutional inference validation unit 174 intercepts all clinical inference outputs 176 prior to their transmission to the clinical alert generation subsystem 178 and evaluates each inference output against the constitutional articles of Chapter 1, Chapter 3, and Chapter 4. Inference outputs that fail constitutional validation are withheld from the clinical alert generation subsystem 178 and are logged as constitutional derogation events in the Constitutional Governance Registry 140.

[0038] In a preferred embodiment, the AI inference engine 172 is implemented as a federated neural network architecture trained on eldercare-specific clinical datasets, comprising physiological pattern recognition models for atrial fibrillation detection, hypoglycemic episode prediction, fall risk scoring, dehydration index estimation, and cognitive status fluctuation assessment.

[0039] The monitoring module 170 further comprises a constitutional monitoring governance layer 179 that enforces constitutional monitoring frequency constraints, constitutional alert threshold boundaries, and constitutional false positive rate limits, ensuring that the clinical alert generation subsystem 178 operates within constitutionally validated clinical performance parameters.

[0040] In a further embodiment, the monitoring module 170 integrates a constitutional explainability engine that generates natural language explanation records for each clinical alert, satisfying the requirements of Constitutional Article 3.1 and Constitutional Article 3.2, and providing clinical staff with constitutionally compliant decision support documentation.

V. Eldercare Controlling Module

[0041] Referring now to FIG. 5, the eldercare controlling module 180 comprises a plurality of actuator subsystems 182 governed by constitutional control constraints 184. The actuator subsystems 182 include, without limitation, automated medication dispensation actuators 182a, robotic mobility assistance devices 182b, smart environmental control actuators 182c (including lighting, temperature, and door access control), and wearable therapeutic stimulation devices 182d.

[0042] The constitutional control constraints 184 define the permissible operational envelope for each actuator subsystem 182, including maximum force and velocity parameters for mobility assistance devices, medication dosage ceiling values for dispensation actuators, and environmental parameter ranges for environmental control actuators. These constraints are derived from Constitutional Chapter 1 risk provisions and are calibrated against patient-specific clinical profiles maintained in the constitutional patient profile registry 186.

[0043] The controlling module 180 further comprises a constitutional override mechanism 188 configured to enable authorized clinical supervisors to issue constitutional override commands that temporarily expand the constitutional operational envelope of designated actuator subsystems in response to clinical emergencies. All constitutional override events are recorded in the Constitutional Governance Registry 140 with timestamped justification records.

[0044] In a preferred embodiment, the constitutional override mechanism 188 requires dual-authorization from at least **two** independent clinical supervisors before activation, ensuring that no single point of human authority can unilaterally override the constitutional governance framework. This dual-authorization requirement implements a constitutional checks-and-balances mechanism analogous to constitutional separation of powers principles in democratic governance theory.

VI. Constitutional Governance Registry

[0045] Referring now to FIG. 6, the Constitutional Governance Registry 140 comprises a distributed ledger architecture 142 configured to record all constitutional enforcement events 144, compliance attestation records 146, derogation events 148, and regulatory submission data packages 149. The distributed ledger architecture 142 implements cryptographic immutability, ensuring that recorded constitutional governance events cannot be modified, deleted, or fabricated after initial inscription.

[0046] In a preferred embodiment, the Constitutional Governance Registry 140 employs a permissioned blockchain architecture accessible to the device manufacturer, designated clinical supervisors, and the Health Sciences Authority upon regulatory request. The registry implements role-based access control mechanisms ensuring that each authorized party accesses only the constitutional governance records within their regulatory or clinical remit.

[0047] The Constitutional Governance Registry 140 further comprises a regulatory submission data packager 149 configured to automatically compile constitutional compliance attestation records, derogation justification records, and constitutional enforcement event logs into a structured data package formatted for submission to the HSA as supporting evidence for a Class B SaMD Pre-Market Submission or Product Registration application.

VII. HSA Class B SaMD Regulatory Alignment

[0048] Referring now to FIG. 7, the NAI2.0 Constitutional Framework is systematically aligned with HSA Class B SaMD regulatory requirements through a Constitutional Regulatory Alignment Matrix 200. The matrix maps each constitutional article to

corresponding HSA regulatory requirements, ISO 14971 risk control provisions, ISO 13485 quality management elements, and IEC 62304 software lifecycle requirements.

[0049] Constitutional Chapter 1 patient safety provisions are aligned with HSA risk classification criteria for Class B SaMD, ISO 14971 Clause 6 risk control implementation requirements, ISO 13485 Clause 7.1 planning of product realization requirements, and IEC 62304 Clause 5.1 software development planning requirements.

[0050] Constitutional Chapter 4 regulatory compliance provisions support the generation of technical documentation required for a HSA Pre-Market Submission, including software description documentation, clinical evaluation reports, risk management files, and post-market surveillance plans, all derived from or supported by constitutional governance records maintained in the Constitutional Governance Registry 140.

[0051] In a preferred embodiment, the NAI2.0 Framework implements a constitutional post-market surveillance module configured to continuously collect real-world performance data from deployed eldercare SaMD devices, evaluate collected data against constitutional performance thresholds, and generate constitutional post-market surveillance reports satisfying HSA post-market requirements for Class B SaMD products.

VIII. Surrogate Consent Constitutional Module

[0052] Referring now to FIG. 8, the surrogate consent management constitutional module 190 governs the acquisition, verification, and revocation of consent for data collection and clinical intervention by the NAI2.0-compliant SaMD device when the primary patient is determined by the cognitive status assessment module 192 to lack decisional capacity.

[0053] The surrogate consent constitutional module 190 comprises a surrogate registry 194 maintaining records of legally authorized surrogate decision-makers for each registered patient, including legal guardians, lasting power of attorney holders, and designated healthcare representatives. The surrogate registry 194 is operatively coupled to the constitutional data acquisition controller 164 and the constitutional control constraints 184, ensuring that device operations requiring patient consent are authorized by a constitutionally valid consent record before execution.

[0054] Constitutional Article 2.3 provisions are implemented by the surrogate consent constitutional module 190 through a tiered consent authorization protocol comprising **three** constitutional consent tiers: Tier 1 (patient direct consent), Tier 2 (surrogate authorized consent), and Tier 3 (emergency clinical necessity authorization). Tier 3 authorization is permitted only when immediate intervention is required to prevent serious patient harm and a surrogate decision-maker is unavailable within a constitutionally specified response window not to exceed **300 seconds**.

Claims

[0055] What is claimed is:

Claim 1. A constitutional governance system for Software as a Medical Device (SaMD) regulatory compliance comprising:

a Constitutional Layer comprising a plurality of constitutional articles each encoding a computationally executable governance constraint;

a Constitutional Enforcement Engine operatively coupled to the Constitutional Layer and configured to evaluate device operational decisions against the constitutional articles in real time;

a Constitutional Compliance Verification Module configured to generate compliance attestation records for each evaluated device operational decision;

a Constitutional Governance Registry configured to immutably record constitutional enforcement events, compliance attestation records, and derogation events; and

a plurality of eldercare constitutional governance modules configured to govern sensing devices, monitoring devices, and controlling devices operating in eldercare environments under Nice Classification Classes 10, 44, and 45.

Claim 2. The system of Claim 1, wherein the Constitutional Enforcement Engine operates as a hypervisor-level process with elevated system privileges rendering it tamper-resistant against modification by an AI inference engine or any application-layer process.

Claim 3. The system of Claim 1, wherein the Constitutional Layer comprises constitutional chapters governing patient safety and primacy of care, patient dignity and autonomy, algorithmic transparency and explainability, regulatory compliance and accountability, data governance and privacy, and operational integrity and fail-safe governance.

Claim 4. The system of Claim 1, wherein the Constitutional Governance Registry comprises a permissioned blockchain architecture implementing cryptographic immutability of constitutional governance records.

Claim 5. The system of Claim 1, wherein the plurality of eldercare constitutional governance modules comprises:

an eldercare sensing module comprising a constitutional data acquisition controller enforcing constitutional data acquisition constraints;

an eldercare monitoring module comprising a constitutional inference validation unit configured to evaluate AI inference outputs against constitutional articles prior to transmission to a clinical alert generation subsystem; and

an eldercare controlling module comprising constitutional control constraints defining permissible operational envelopes for actuator subsystems.

Claim 6. The system of Claim 5, wherein the eldercare monitoring module further comprises a constitutional explainability engine configured to generate natural language explanation records for each clinical alert in compliance with constitutional algorithmic transparency provisions.

Claim 7. The system of Claim 5, wherein the eldercare controlling module further comprises a constitutional override mechanism requiring dual-authorization from at least two independent clinical supervisors before activation.

Claim 8. The system of Claim 1, further comprising a surrogate consent management constitutional module comprising:

a surrogate registry maintaining records of legally authorized surrogate decision-makers; and

a tiered consent authorization protocol comprising a patient direct consent tier, a surrogate authorized consent tier, and an emergency clinical necessity authorization tier.

Claim 9. The system of Claim 8, wherein emergency clinical necessity authorization is permitted only when immediate intervention is required to prevent serious patient harm and a surrogate decision-maker is unavailable within a constitutionally specified response window not to exceed 300 seconds.

Claim 10. The system of Claim 1, wherein the Constitutional Compliance Verification Module is further configured to compile constitutional compliance attestation records, derogation justification records, and constitutional enforcement event logs into a structured regulatory submission data package formatted for submission to the Health Sciences Authority as supporting evidence for a Class B SaMD Pre-Market Submission.

Claim 11. The system of Claim 1, wherein the Constitutional Enforcement Engine is configured to cause the SaMD device to enter a constitutionally mandated safe state upon detection of Constitutional Enforcement Engine failure, discontinuing all clinical recommendation outputs and actuator control commands, and reporting the safe-state transition to a designated clinical supervisor within 120 seconds.

Claim 12. The system of Claim 5, wherein the eldercare sensing module further comprises a privacy-preserving signal processing pipeline implementing differential privacy mechanisms, on-device federated learning processes, and constitutional data anonymization protocols.

Claim 13. A method for constitutional governance of eldercare Software as a Medical Device comprising:

encoding a plurality of constitutional articles each defining a computationally executable governance constraint applicable to sensing, monitoring, and controlling device operations;

evaluating, by a Constitutional Enforcement Engine, each device operational decision against the constitutional articles in real time prior to output generation;

generating compliance attestation records for each constitutionally validated device operational decision;

recording constitutional enforcement events and compliance attestation records in an immutable Constitutional Governance Registry; and

compiling constitutional governance records into a regulatory submission data package for Health Sciences Authority Class B SaMD regulatory approval.

Claim 14. The method of Claim 13, further comprising:

detecting a constitutional enforcement engine failure;

transitioning the SaMD device to a constitutionally mandated safe state upon detection of the failure; and

notifying a designated clinical supervisor of the safe-state transition within a constitutionally specified time period.

Claim 15. The method of Claim 13, further comprising:

assessing decisional capacity of an elderly patient by a cognitive status assessment module;

upon determination that the patient lacks decisional capacity, initiating surrogate consent authorization through a tiered consent authorization protocol; and

recording the consent authorization tier, authorizing party identity, and authorization timestamp in the Constitutional Governance Registry.

Claim 16. A non-transitory computer-readable medium storing instructions that, when executed by one or more processors of a Software as a Medical Device system, cause the system to implement a constitutional governance framework comprising:

enforcing a hierarchically ordered plurality of constitutional articles governing patient safety, patient dignity, algorithmic transparency, regulatory compliance, data governance, and operational integrity;

intercepting all AI inference outputs and evaluating each against the constitutional articles before transmission to clinical output subsystems;

generating immutable constitutional compliance attestation records suitable for Health Sciences Authority regulatory review; and

enforcing constitutional data acquisition constraints, constitutional inference validation constraints, and constitutional actuator control constraints across sensing, monitoring, and controlling device subsystems in eldercare environments.

Claim 17. The non-transitory computer-readable medium of Claim 16, wherein enforcing constitutional data acquisition constraints comprises implementing privacy-preserving signal processing including differential privacy mechanisms and constitutional data minimization protocols.

Claim 18. The non-transitory computer-readable medium of Claim 16, wherein evaluating each AI inference output comprises:

assessing the inference output against patient safety constitutional provisions;

assessing the inference output against algorithmic transparency constitutional provisions requiring a natural language explanation record; and

withholding the inference output from clinical alert generation if constitutional validation fails, and recording a constitutional derogation event in the Constitutional Governance Registry.

Claim 19. A constitutional governance device for eldercare SaMD under Health Sciences Authority Class B classification, the device comprising:

one or more physiological sensor arrays configured to acquire eldercare patient physiological data;

an AI inference engine configured to generate clinical inference outputs from acquired physiological data;

a constitutional inference validation unit operatively interposed between the AI inference engine and a clinical output subsystem, configured to enforce constitutional governance constraints on all clinical inference outputs;

one or more actuator subsystems governed by constitutional control constraints defining constitutionally permissible operational parameters; and

a constitutional governance registry recording all constitutional enforcement events in an immutable distributed ledger.

Claim 20. The device of Claim 19, wherein the constitutional governance constraints are derived from constitutional articles organized into constitutional chapters governing patient safety primacy, patient dignity and autonomy, algorithmic transparency, regulatory compliance, data privacy governance, and operational fail-safe integrity, and wherein the constitutional articles are hierarchically ordered such that patient safety provisions supersede all other constitutional provisions in the event of conflict.

Abstract

A NAI2.0 Constitutional Framework for Health Sciences Authority (HSA) Class B Software as a Medical Device (SaMD) Regulatory Approval is disclosed, comprising a hierarchically structured constitutional governance architecture embedded within eldercare SaMD systems. The Framework governs sensing, monitoring, and controlling constitutional governance devices operating under Nice Classification Classes 10, 44, and 45. A Constitutional Enforcement Engine enforces a plurality of constitutional articles governing patient safety, patient dignity and autonomy, algorithmic transparency, regulatory compliance, data privacy, and operational integrity, interposing constitutional validation between AI inference outputs and clinical output subsystems. A Constitutional Governance Registry immutably records all constitutional enforcement events and compliance attestations using a permissioned blockchain architecture, generating regulatory submission data packages for HSA Class B SaMD Pre-Market Submission. Eldercare-specific constitutional governance modules address physiological sensing, clinical monitoring, actuator control, surrogate consent management, and privacy-preserving data processing tailored to the clinical, cognitive, and legal characteristics of elderly patients. The Framework achieves systematic alignment with HSA SaMD regulatory requirements, ISO 14971 risk management standards, ISO 13485 quality management standards, and IEC 62304 medical device software lifecycle requirements.

Drawing Reference Designators Summary

Reference Designator	Description	Associated Figure
100	NAI2.0 Constitutional Framework	FIG. 1
102	HSA Class B SaMD Device Subsystems	FIG. 1
110	Constitutional Layer	FIG. 1
112	Constitutional Articles	FIG. 1
114	Constitutional Chapters	FIG. 1
120	Constitutional Enforcement Engine	FIG. 1, FIG. 2
122	AI Inference Engine	FIG. 1, FIG. 4
130	Constitutional Compliance Verification Module	FIG. 1, FIG. 2
140	Constitutional Governance Registry	FIG. 1, FIG. 6
150	Eldercare Constitutional Governance Modules	FIG. 1
160	Sensing Module	FIG. 1, FIG. 3
162	Physiological Sensor Arrays	FIG. 3

164	Constitutional Data Acquisition Controller	FIG. 3
166	Privacy-Preserving Signal Processing Pipeline	FIG. 3
170	Monitoring Module	FIG. 1, FIG. 4
172	AI Inference Engine (Monitoring)	FIG. 4
174	Constitutional Inference Validation Unit	FIG. 4
178	Clinical Alert Generation Subsystem	FIG. 4
180	Controlling Module	FIG. 1, FIG. 5
182	Actuator Subsystems	FIG. 5
184	Constitutional Control Constraints	FIG. 5
188	Constitutional Override Mechanism	FIG. 5
190	Surrogate Consent Constitutional Module	FIG. 8
194	Surrogate Registry	FIG. 8
200	Constitutional Regulatory Alignment Matrix	FIG. 7

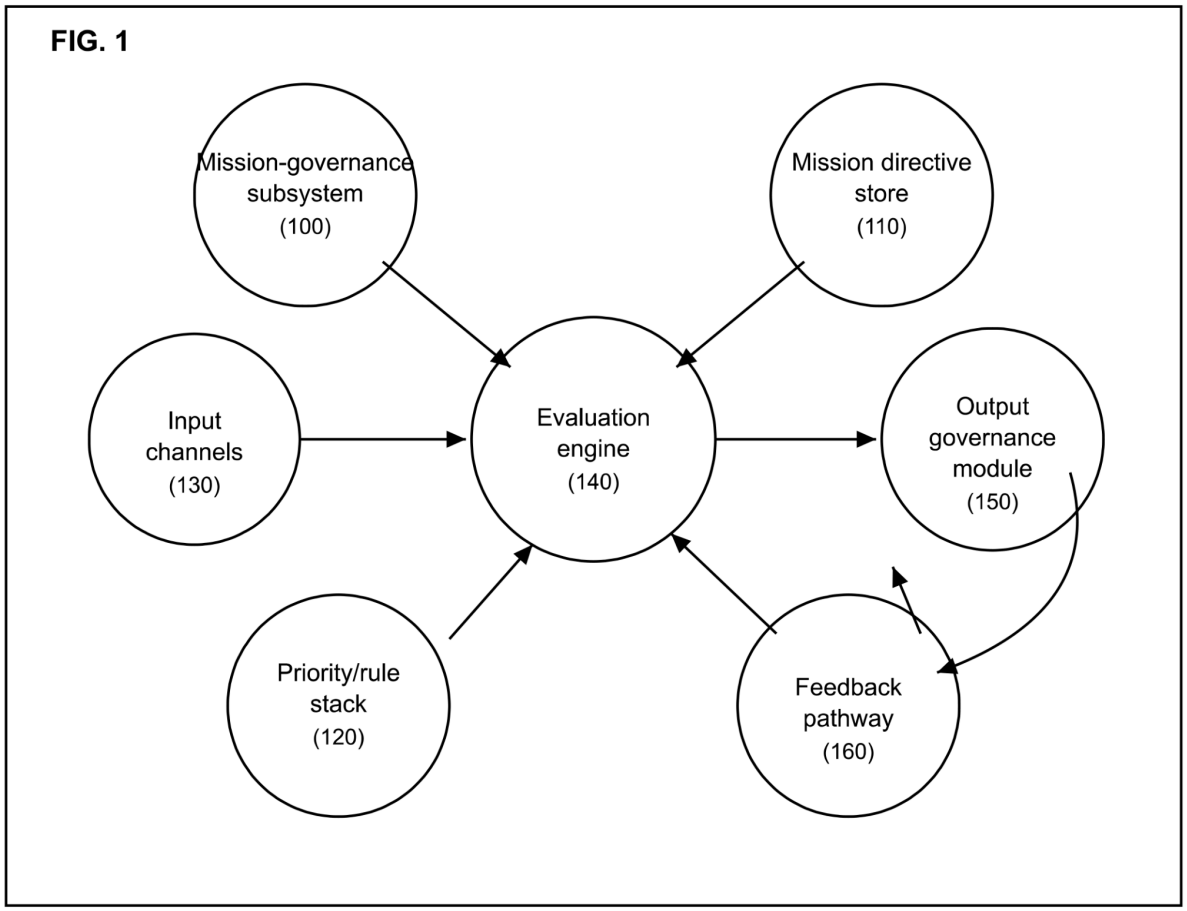


FIG. 1 is a schematic diagram illustrating an embodiment of a **P-LIFE 1.00 mission constant architecture**, including mission directives, evaluation logic, governance outputs, and feedback pathways.

FIG. 1 — P-LIFE 1.00 Mission Constant

In some embodiments, **FIG. 1** illustrates a mission-governance subsystem **100** implementing a persistent mission constant for a constitutional control architecture. The subsystem **100** may include a mission directive store **110**, a priority or rule stack **120**, one or more input channels **130**, an evaluation engine **140**, an output governance module **150**, and a feedback pathway **160**.

The mission directive store **110** may contain one or more governing objectives, constraints, or operational priorities. The rule stack **120** may define ordering, precedence, exception handling, or conflict resolution among directives. Inputs received via the input channels **130** may be evaluated by the evaluation engine **140** against the directives and rule stack to determine whether a requested action, state transition, or system output is permitted.

The output governance module **150** may generate a constrained output, authorization signal, modified instruction, or denial response based on the evaluation result. The feedback pathway **160** may provide operational outcomes, audit observations, or environmental responses back to the evaluation engine **140** or mission directive store **110** for continuous enforcement or adaptation within defined constitutional bounds.

FIG. 2

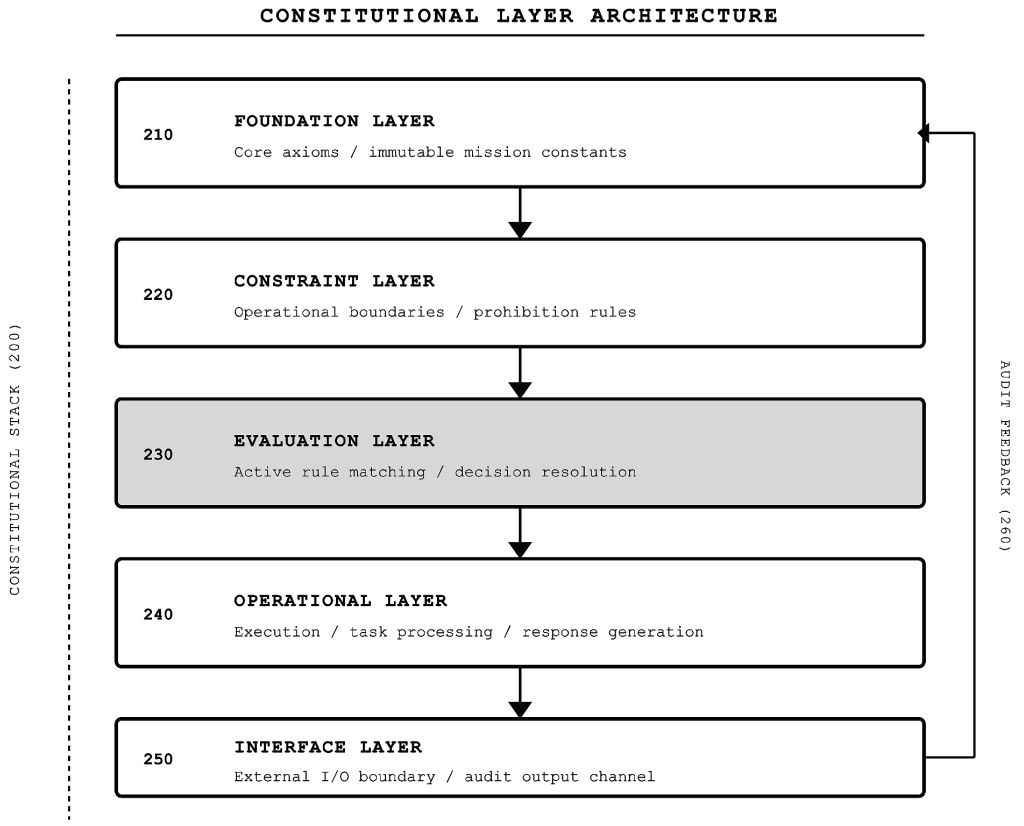


FIG. 2 is a schematic diagram illustrating an embodiment of a **WD070–073 protocol suite**, including multiple coordinated protocol layers and an orchestration pathway therebetween.

FIG. 2 — WD070–073 Protocol Suite

In some embodiments, **FIG. 2** illustrates a protocol coordination subsystem **200** including a first protocol layer **210**, a second protocol layer **220**, a third protocol layer **230**, a fourth protocol layer **240**, an orchestration engine **250**, and an inter-module policy bus **260**.

Each of the protocol layers **210–240** may correspond to a distinct operational control domain, such as intake validation, contextual rule application, escalation handling, or enforcement logic. The orchestration engine **250** may coordinate ordering, invocation, handoff, or exception management among the protocol layers. The policy bus **260** may carry state information, control messages, permission tokens, or rejection signals among the protocols and associated subsystems.

In some implementations, the protocol coordination subsystem **200** provides a layered governance arrangement in which no single protocol layer independently controls all operational decisions, thereby supporting separation of function and verifiable process sequencing.

FIG. 3

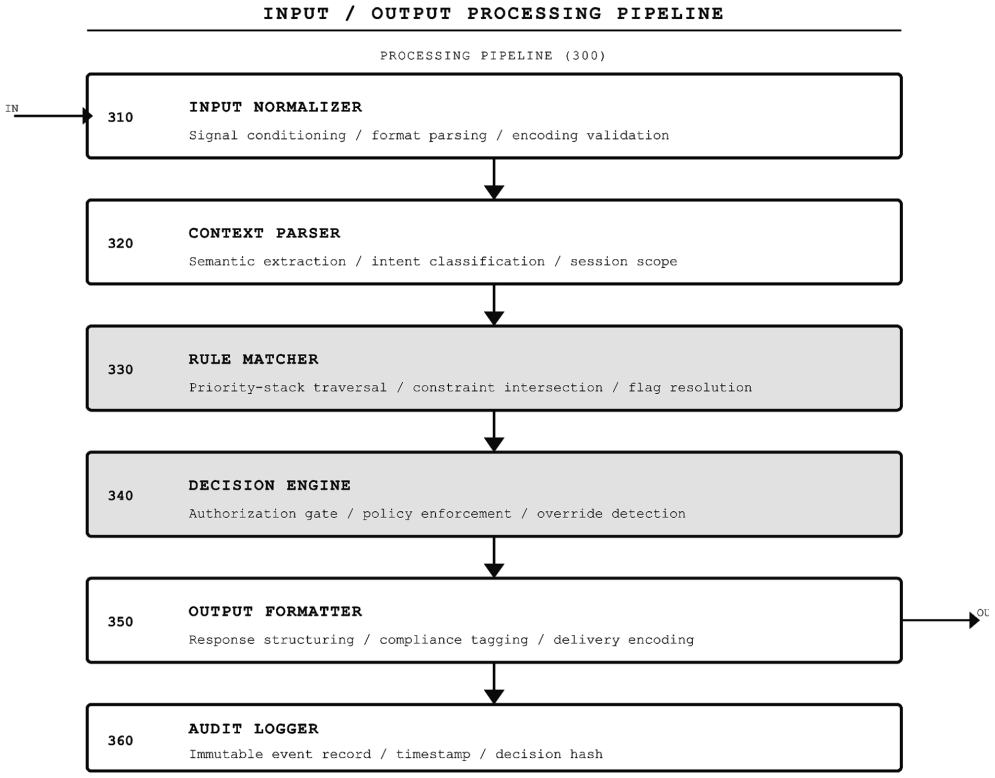


FIG. 3 is a schematic diagram illustrating an embodiment of a **tripartite authentication process**, including first, second, and third authentication sources, a consensus engine, and approval and rejection flows.

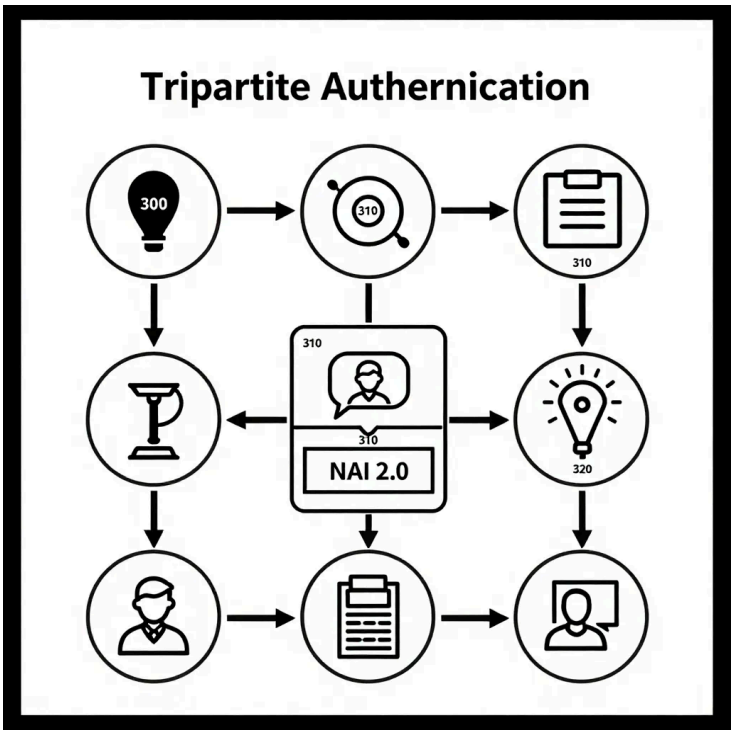


FIG. 3 — Tripartite Authentication Process

In some embodiments, **FIG. 3** illustrates an authentication subsystem **300** including a first authenticator **310**, a second authenticator **320**, a third authenticator **330**, a consensus engine **340**, a token or authorization generator **350**, an approval path **360**, and a rejection path **370**.

The first, second, and third authenticators **310**, **320**, and **330** may obtain or evaluate distinct authentication factors, distinct authorities, or distinct verification modalities. The consensus engine **340** may determine whether a threshold condition, unanimity condition, or policy-defined multi-party condition has been satisfied. When the required condition is met, the authorization generator **350** may issue a permission token, release signal, or validated command for downstream processing via the approval path **360**. When the required condition is not met, the rejection path **370** may block or terminate the requested action and optionally generate an audit event.

Such a tripartite arrangement may improve resistance to unauthorized actions by requiring coordinated validation from multiple independent sources rather than reliance on a single credential or actor.

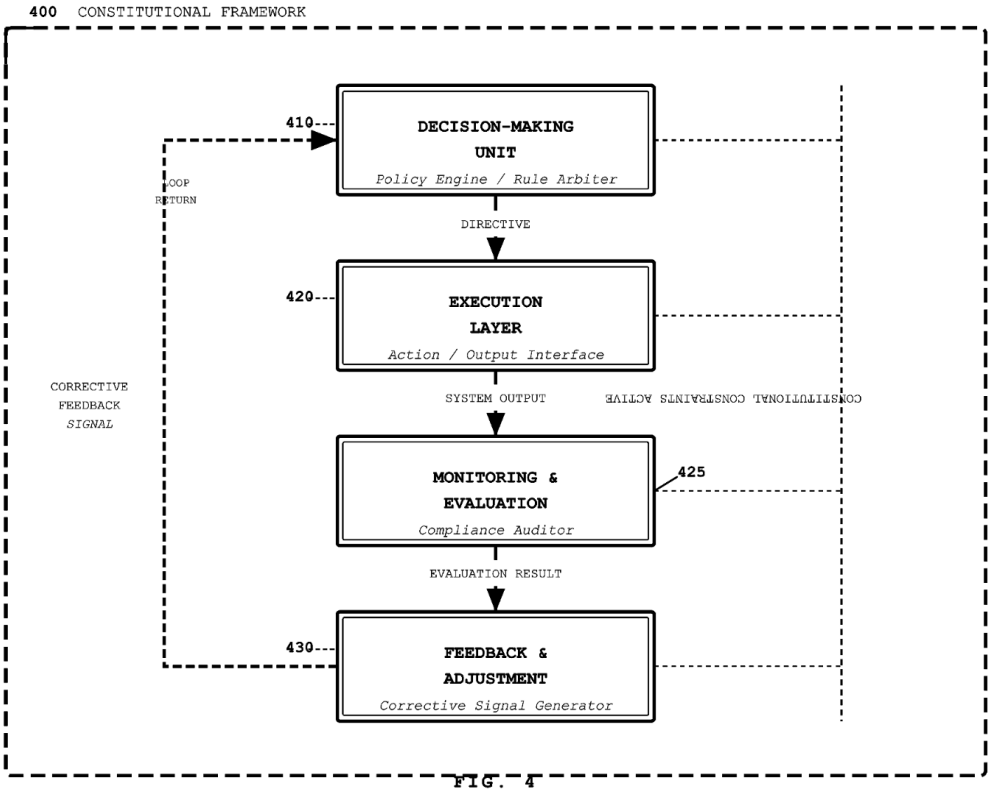


FIG. 4
CONSTITUTIONAL GOVERNANCE FEEDBACK LOOP

FIG. 4 is a schematic feedback loop diagram illustrating an embodiment of a **constitutional governance feedback loop 400** comprising a **decision-making unit 410**, an **execution layer 420**, a **monitoring and evaluation stage 425**, and a **feedback and adjustment stage 430**, wherein a corrective feedback signal is returned from the feedback and adjustment stage 430 to the decision-making unit 410, all operating within a constitutional framework 400 that enforces continuous constitutional constraints across each stage of the loop.

REF. NO.	DESCRIPTION
400	Constitutional Governance Feedback Loop (overall system)
410	Decision-Making Unit
420	Execution Layer
425	Monitoring and Evaluation
430	Feedback and Adjustment

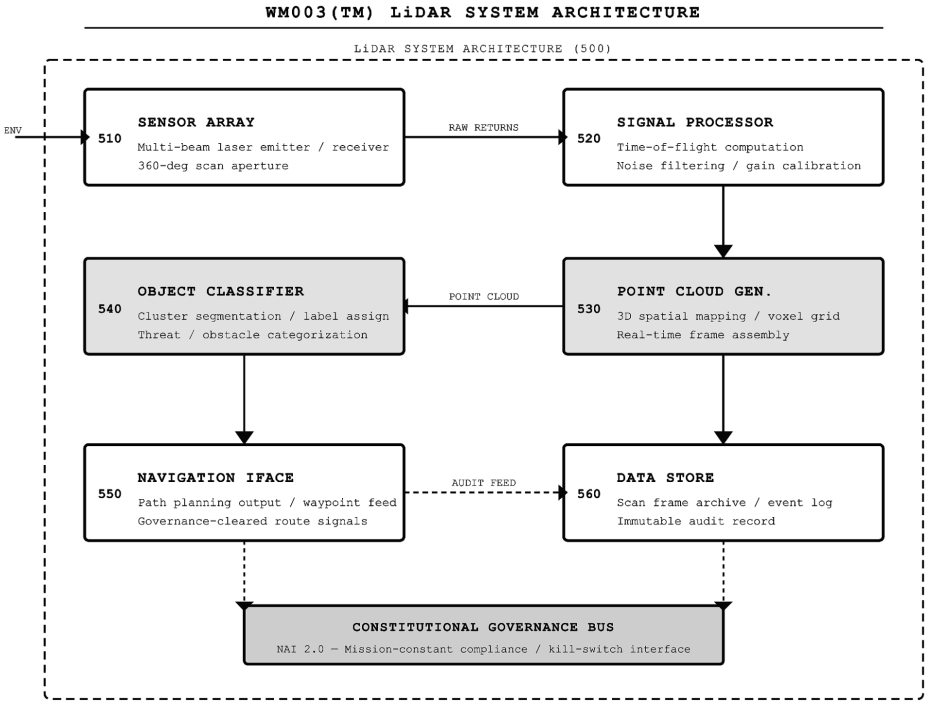
FIG. 4 is a schematic diagram illustrating an embodiment of a **Sacred Pause FPGA architecture**, including trigger detection, pause control, clock gating, buffering, watchdog logic, and audit functionality.

FIG. 4 — Sacred Pause FPGA Architecture

In some embodiments, **FIG. 4** illustrates a hardware control subsystem **400** implemented at least in part in programmable logic. The subsystem **400** may include a trigger monitor **410**, a pause controller **420**, a clock gate or execution hold component **430**, an FPGA core **440**, a secure buffer **450**, a watchdog **460**, and an audit log module **470**.

The trigger monitor **410** may detect one or more conditions warranting temporary interruption, such as policy uncertainty, authentication failure, anomalous state transitions, or external override conditions. Upon detection, the pause controller **420** may cause the clock gate **430** or related hold function to suspend, defer, or isolate selected processing operations within the FPGA core **440**.

The secure buffer **450** may retain intermediate states, pending instructions, or transaction data during a pause interval. The watchdog **460** may supervise timeout conditions, recovery prerequisites, or fail-safe transitions. The audit log module **470** may record invocation events, pause durations, restart conditions, and related system metadata for traceability.



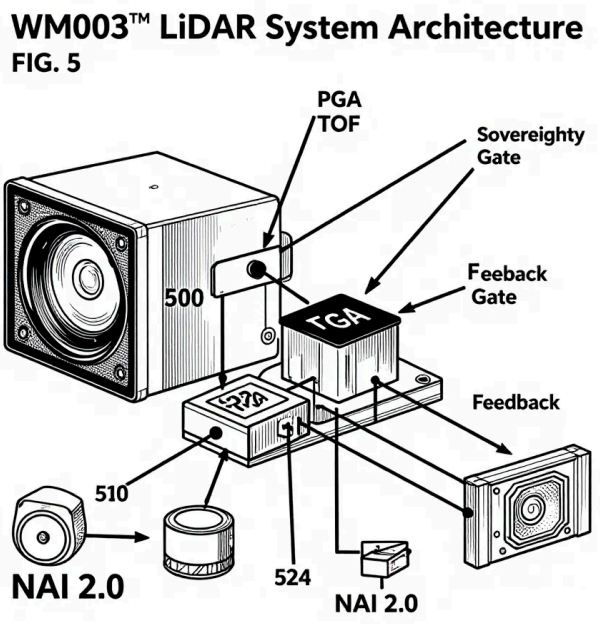


FIG. 5 is a schematic diagram illustrating an embodiment of a **WM003 LiDAR system architecture**, including a laser emitter, a time-of-flight engine, an FPGA core, a photon receiver, a sovereignty gate, and feedback and rejection paths.

FIG. 5 — WM003 LiDAR System Architecture

In some embodiments, **FIG. 5** illustrates a sensing subsystem **500** including a laser emitter **510**, a time-of-flight engine **520**, an FPGA core **530**, a photon receiver **540**, a sovereignty gate **550**, a feedback path **560**, and a reject path **570**.

The laser emitter **510** may generate one or more outgoing optical pulses directed toward a target environment. Reflected optical energy may be detected by the photon receiver **540**, and timing or distance calculations may be performed by the time-of-flight engine **520**. The FPGA core **530** may coordinate signal timing, measurement processing, filtering, and interface operations.

The sovereignty gate **550** may apply governance constraints to sensed data, derived outputs, or downstream command use. For example, the sovereignty gate **550** may determine whether processed sensor information is eligible for release, retention, forwarding, suppression, or further review. The feedback path **560** may return validated operational or calibration information to one or more upstream components, whereas the reject path **570** may route invalid, restricted, or policy-noncompliant outputs away from normal use pathways.

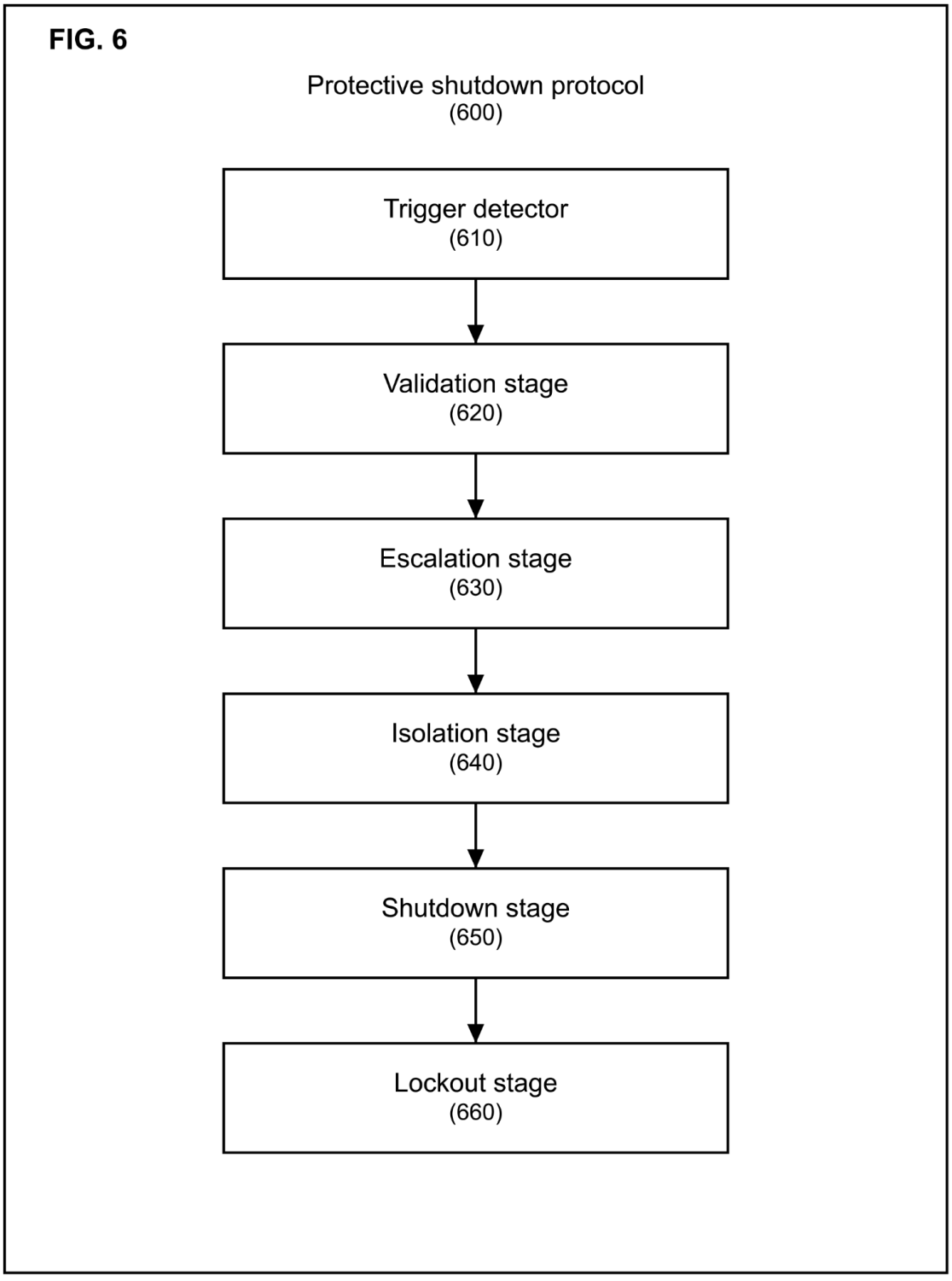


FIG. 6 is a schematic diagram illustrating an embodiment of a **multi-stage kill-switch protocol**, including trigger detection, validation, escalation, isolation, shutdown, and lockout stages.

FIG. 6 — Multi-Stage Kill-Switch Protocol

In some embodiments, **FIG. 6** illustrates a protective shutdown protocol **600** including a trigger detector **610**, a validation stage **620**, an escalation stage **630**, an isolation stage **640**, a shutdown stage **650**, and a lockout or post-event restraint stage **660**.

The trigger detector **610** may monitor for conditions associated with severe policy violation, hardware compromise, authentication failure, unsafe state progression, or externally authorized shutdown invocation. Upon detecting a candidate condition, the validation stage **620** may confirm that the condition satisfies one or more threshold, timing, corroboration, or rule-based criteria prior to execution of a shutdown sequence.

If validated, the escalation stage **630** may increase the response level, notify associated subsystems, or prepare dependent modules for controlled interruption. The isolation stage **640** may sever selected data paths, disable interfaces, or quarantine operational domains. The shutdown stage **650** may terminate defined functions, halt execution, or place one or more components into a protected non-operational state. The lockout stage **660** may prevent unauthorized restart pending subsequent review, reset, or reauthorization.

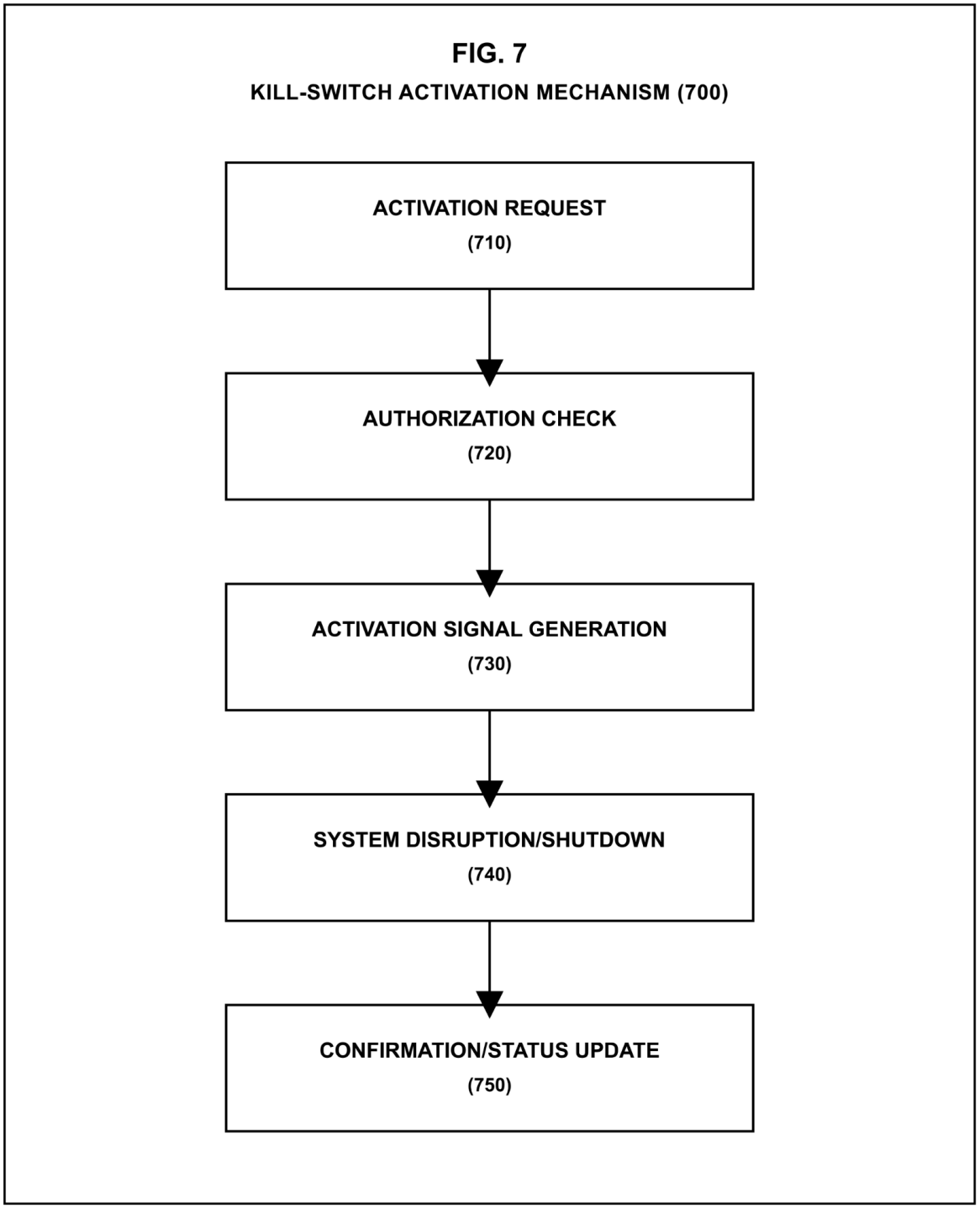


FIG. 7 is a schematic diagram illustrating an embodiment of a **kill-switch activation mechanism**, including trigger conditions, redundant activation paths, secure communication channels, authorization logic, and actuation control.

FIG. 7 — Kill-Switch Activation Mechanism

In some embodiments, **FIG. 7** illustrates an activation subsystem **700** including a primary trigger path **710**, a redundant trigger path **720**, one or more secure communication channels **730**, an authorization module **740**, an actuation controller **750**, and a confirmation return path **760**.

The primary trigger path **710** may carry a normal shutdown initiation signal, while the redundant trigger path **720** may provide a fallback or independent initiation route in the event of malfunction, tampering, or communication failure. The secure communication channels **730** may support authenticated transmission of activation messages, confirmations, state queries, or related control signals.

The authorization module **740** may verify that the initiating condition, source, and context satisfy defined activation requirements. Once authorized, the actuation controller **750** may issue the operational command that initiates the protective shutdown protocol. The confirmation return path **760** may communicate completion, failure, or intermediate state information back to supervisory logic or audit components.

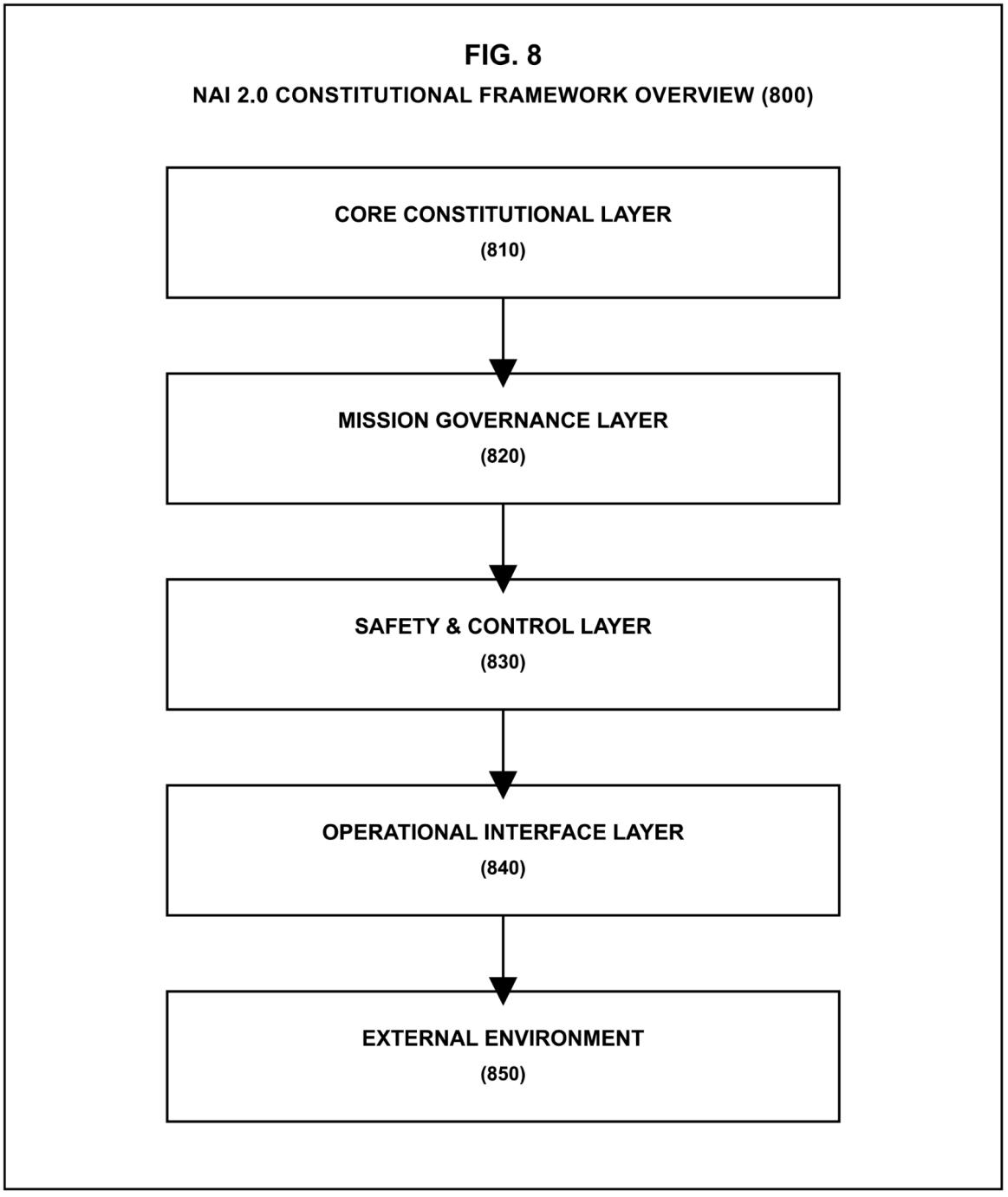


FIG. 8 is a schematic diagram illustrating an embodiment of an **NAI 2.0 constitutional framework overview**, including integration of mission governance, protocol control, authentication, pause logic, sensing architecture, and protective shutdown subsystems.

FIG. 8 — NAI 2.0 Constitutional Framework Overview

In some embodiments, **FIG. 8** illustrates a framework overview **800** integrating a mission-governance subsystem **810**, a protocol suite **820**, an authentication subsystem **830**, a pause-control subsystem **840**, a sensing subsystem **850**, a protective shutdown subsystem **860**, and a system interconnection or governance backbone **870**.

The mission-governance subsystem **810** may provide baseline constitutional objectives and constraints. The protocol suite **820** may coordinate rule execution and process sequencing. The authentication subsystem **830** may gate selected actions based on multi-source validation. The pause-control subsystem **840** may provide temporary interruption and audit-preserving hold functions. The sensing subsystem **850** may provide environmental or state-derived inputs subject to governance review. The protective shutdown subsystem **860** may provide terminal protective responses when defined conditions are met.

The governance backbone **870** may represent logical, electrical, procedural, or message-based interconnections among the constituent subsystems. In this manner, the framework overview **800** depicts an architecture in which sensing, evaluation, authentication, intervention, and shutdown functions are integrated within a layered constitutional control environment.

Claim-Support Mapping for FIGS. 1–8

1. Claim Families

Claim Family	Claim Type	Main Supporting Figures	Focus
A	Independent system claim	FIGS. 1–8	Integrated constitutional control framework
B	Independent method claim	FIGS. 1–8	Method of governed operation
C	Independent apparatus claim	FIG. 4, FIG. 8	Pause-control hardware / FPGA architecture
D	Independent sensing-system claim	FIG. 5, FIG. 8	LiDAR architecture with governance gate
E	Independent shutdown-protocol claim	FIG. 6, FIG. 7, FIG. 8	Multi-stage kill-switch and activation
F	Optional independent authentication claim	FIG. 3, FIG. 8	Tripartite authentication subsystem

---

2. Figure-to-Claim Support Overview

FIG.	Primary Subject	Typical Claim Role
FIG. 1	Mission constant / governance core	Core limitation in broad system and method claims; dependent claims on directive hierarchy and evaluation
FIG. 2	Protocol suite	Dependent limitations on layered governance and orchestration
FIG. 3	Tripartite authentication	Independent claim option or dependent limitations on multi-source validation
FIG. 4	Sacred Pause FPGA	Independent apparatus claim and dependent hardware-control limitations
FIG. 5	WM003 LiDAR architecture	Independent sensing claim and dependent limitations on sovereignty gating
FIG. 6	Multi-stage kill-switch protocol	Independent shutdown claim and dependent staged-response limitations
FIG. 7	Kill-switch activation mechanism	Dependent or separate independent activation-path claim
FIG. 8	Overall framework integration	Best support for broad system claims tying all subsystems together

---

3. Claim Family A — Broad Integrated System Claim

Independent Claim A1

A system comprising:

1. a **mission-governance subsystem** configured to evaluate one or more inputs against one or more directives;
2. a **protocol coordination subsystem** configured to apply a plurality of protocol layers to system operation;
3. an **authentication subsystem** configured to require validation from multiple authentication sources before authorizing a protected action;
4. a **pause-control subsystem** configured to temporarily interrupt execution responsive to a trigger condition;
5. a **sensing subsystem** configured to generate sensor-derived data and subject the sensor-derived data to governance review; and
6. a **protective shutdown subsystem** configured to execute a staged shutdown sequence responsive to a validated trigger.

Support Mapping for A1

Claim Element	Figure Support	Reference Numerals
Mission-governance subsystem	FIG. 1, FIG. 8	100, 110, 120, 130, 140, 150, 160; 810
Protocol coordination subsystem	FIG. 2, FIG. 8	200, 210, 220, 230, 240, 250, 260; 820
Authentication subsystem	FIG. 3, FIG. 8	300, 310, 320, 330, 340, 350, 360, 370; 830
Pause-control subsystem	FIG. 4, FIG. 8	400, 410, 420, 430, 440, 450, 460, 470; 840
Sensing subsystem	FIG. 5, FIG. 8	500, 510, 520, 530, 540, 550, 560, 570; 850
Protective shutdown subsystem	FIG. 6, FIG. 8	600, 610, 620, 630, 640, 650, 660; 860
Interconnection of subsystems	FIG. 8	870

Dependent Claims from A1

A2

The system of claim A1, wherein the mission-governance subsystem comprises a **mission directive store**, a **priority stack**, and an **evaluation engine**.

- **Support:** FIG. 1
- **Refs:** 110, 120, 140

A3

The system of claim A1, wherein the protocol coordination subsystem comprises **first through fourth protocol layers** and an **orchestration engine**.

- **Support:** FIG. 2
- **Refs:** 210, 220, 230, 240, 250

A4

The system of claim A1, wherein the authentication subsystem requires consensus among **first, second, and third authenticators** before generating an authorization output.

- **Support:** FIG. 3
- **Refs:** 310, 320, 330, 340, 350

A5

The system of claim A1, wherein the pause-control subsystem includes a **clock gate or execution hold component** configured to suspend processing while preserving intermediate state data.

- **Support:** FIG. 4
- **Refs:** 430, 450

A6

The system of claim A1, wherein the sensing subsystem includes a **sovereignty gate** configured to selectively release, reject, or hold sensor-derived outputs.

- **Support:** FIG. 5
- **Refs:** 550, 560, 570

A7

The system of claim A1, wherein the protective shutdown subsystem comprises a **validation stage**, an **escalation stage**, an **isolation stage**, and a **lockout stage**.

- **Support:** FIG. 6
- **Refs:** 620, 630, 640, 660

A8

The system of claim A1, further comprising an **activation subsystem** having a **primary trigger path** and a **redundant trigger path** for initiating shutdown.

- **Support:** FIG. 7
- **Refs:** 700, 710, 720

A9

The system of claim A1, wherein one or more subsystems are coupled by a **governance backbone** carrying state, policy, or authorization information.

- **Support:** FIG. 8
- **Refs:** 870

A10

The system of claim A1, wherein the pause-control subsystem and the protective shutdown subsystem operate as separate response layers, the pause-control subsystem providing temporary interruption and the protective shutdown subsystem providing terminal shutdown.

- **Support:** FIGS. 4, 6, 8
- **Refs:** 400–470, 600–660, 840, 860

---

4. Claim Family B — Method Claim

Independent Claim B1

A computer-implemented method comprising:

1. receiving one or more inputs;
2. evaluating the one or more inputs against one or more mission directives;
3. applying a plurality of protocol layers to determine whether an action is permitted;
4. authenticating the action using a multi-source authentication process;
5. selectively pausing execution responsive to a trigger condition;
6. processing sensor-derived data through a governance gate; and
7. initiating a staged shutdown sequence when a shutdown condition is validated.

Support Mapping for B1

Method Step	Figure Support	Reference Numerals
Receiving inputs	FIG. 1	130
Evaluating against directives	FIG. 1	110, 120, 140
Applying protocol layers	FIG. 2	210–250
Authenticating	FIG. 3	310–350
Pausing execution	FIG. 4	410–450
Processing sensor data through gate	FIG. 5	520, 530, 550
Initiating staged shutdown	FIG. 6, FIG. 7	610–660, 710–750

Dependent Claims from B1

B2

The method of claim B1, further comprising providing feedback from an output governance module to the mission-governance subsystem.

- **Support:** FIG. 1
- **Refs:** 150, 160

B3

The method of claim B1, wherein applying the plurality of protocol layers includes passing state information over a **policy bus**.

- **Support:** FIG. 2
- **Refs:** 260

B4

The method of claim B1, wherein authenticating includes determining whether a **consensus threshold** has been satisfied by three authenticators.

- **Support:** FIG. 3
- **Refs:** 310, 320, 330, 340

B5

The method of claim B1, wherein selectively pausing execution includes storing intermediate data in a **secure buffer**.

- **Support:** FIG. 4
- **Refs:** 450

B6

The method of claim B1, wherein processing sensor-derived data includes determining a time-of-flight value from emitted and reflected optical signals.

- **Support:** FIG. 5
- **Refs:** 510, 520, 540

B7

The method of claim B1, wherein initiating the staged shutdown sequence includes **isolating one or more interfaces** before halting execution.

- **Support:** FIG. 6
- **Refs:** 640, 650

B8

The method of claim B1, wherein initiating the staged shutdown sequence includes receiving an activation signal over a **secure communication channel**.

- **Support:** FIG. 7
- **Refs:** 730

B9

The method of claim B1, further comprising transmitting a **confirmation return signal** after actuation of the shutdown sequence.

- **Support:** FIG. 7
- **Refs:** 760

---

5. Claim Family C — Pause-Control Hardware / FPGA Claim

Independent Claim C1

An apparatus comprising programmable logic configured to:

1. detect a trigger condition;
2. generate a pause-control signal;
3. gate or hold execution within a processing core;
4. preserve one or more intermediate states during a pause interval; and
5. record an audit event associated with the pause interval.

Support Mapping for C1

Claim Element	Figure Support	Reference Numerals
Trigger detection	FIG. 4	410
Pause-control signal	FIG. 4	420
Gate or hold execution	FIG. 4	430
Processing core	FIG. 4	440
Preserve intermediate states	FIG. 4	450
Audit event	FIG. 4	470

Dependent Claims from C1

C2

The apparatus of claim C1, further comprising a **watchdog** configured to determine whether a recovery condition or timeout condition has occurred.

- **Support:** FIG. 4
- **Refs:** 460

C3

The apparatus of claim C1, wherein the trigger condition includes at least one of **policy uncertainty**, **authentication failure**, or **anomalous state transition**.

- **Support:** FIG. 4 specification text
- **Refs:** 410

C4

The apparatus of claim C1, wherein the programmable logic is implemented in an **FPGA core**.

- **Support:** FIG. 4
- **Refs:** 440

C5

The apparatus of claim C1, wherein the audit event includes at least one of **pause invocation**, **pause duration**, or **restart condition**.

- **Support:** FIG. 4
- **Refs:** 470

C6

The apparatus of claim C1, wherein the apparatus is operatively coupled to a broader governance framework.

- **Support:** FIG. 8
- **Refs:** 840, 870

---

6. Claim Family D — Sensing System with Governance Gate

Independent Claim D1

A sensing system comprising:

1. a **laser emitter** configured to emit optical pulses;
2. a **photon receiver** configured to detect reflected optical energy;
3. a **time-of-flight engine** configured to derive measurement data from timing information;
4. a **processing core** configured to process the measurement data; and
5. a **governance gate** configured to selectively permit, reject, or defer use of the processed measurement data.

Support Mapping for D1

Claim Element	Figure Support	Reference Numerals
Laser emitter	FIG. 5	510
Photon receiver	FIG. 5	540
Time-of-flight engine	FIG. 5	520
Processing core	FIG. 5	530
Governance gate	FIG. 5	550

Dependent Claims from D1

D2

The sensing system of claim D1, wherein the governance gate is configured to route approved outputs through a **feedback path** and rejected outputs through a **reject path**.

- **Support:** FIG. 5
- **Refs:** 560, 570

D3

The sensing system of claim D1, wherein the processing core comprises an **FPGA core**.

- **Support:** FIG. 5
- **Refs:** 530

D4

The sensing system of claim D1, wherein the governance gate determines whether processed data is eligible for **release**, **retention**, **forwarding**, or **suppression**.

- **Support:** FIG. 5 specification text
- **Refs:** 550

D5

The sensing system of claim D1, wherein the sensing system is coupled to a constitutional framework through a governance backbone.

- **Support:** FIG. 8
- **Refs:** 850, 870

---

7. Claim Family E — Multi-Stage Protective Shutdown Claim

Independent Claim E1

A protective shutdown system comprising:

1. a **trigger detector** configured to detect a shutdown condition;
2. a **validation stage** configured to determine whether the shutdown condition satisfies one or more criteria;
3. an **escalation stage** configured to elevate a response level;
4. an **isolation stage** configured to disable or sever one or more interfaces;
5. a **shutdown stage** configured to halt one or more system functions; and
6. a **lockout stage** configured to restrict restart after shutdown.

Support Mapping for E1

Claim Element	Figure Support	Reference Numerals
Trigger detector	FIG. 6	610
Validation stage	FIG. 6	620
Escalation stage	FIG. 6	630
Isolation stage	FIG. 6	640
Shutdown stage	FIG. 6	650
Lockout stage	FIG. 6	660

Dependent Claims from E1

E2

The system of claim E1, wherein the shutdown condition includes at least one of **hardware compromise**, **authentication failure**, **unsafe state progression**, or **authorized external invocation**.

- **Support:** FIG. 6 specification text
- **Refs:** 610

E3

The system of claim E1, wherein the validation stage applies at least one of a **threshold criterion**, **timing criterion**, **corroboration criterion**, or **rule-based criterion**.

- **Support:** FIG. 6 specification text
- **Refs:** 620

E4

The system of claim E1, wherein the isolation stage is performed before the shutdown stage.

- **Support:** FIG. 6 flow
- **Refs:** 640, 650

E5

The system of claim E1, wherein the lockout stage prevents restart pending **review**, **reset**, or **reauthorization**.

- **Support:** FIG. 6 specification text
- **Refs:** 660

E6

The system of claim E1, further comprising an activation subsystem configured to initiate the protective shutdown system over **secure communication channels**.

- **Support:** FIG. 7
- **Refs:** 730, 740, 750

E7

The system of claim E1, wherein shutdown may be initiated through either a **primary trigger path** or a **redundant trigger path**.

- **Support:** FIG. 7
- **Refs:** 710, 720

---

8. Claim Family F — Activation Mechanism Claim

Independent Claim F1

An activation system for a protective shutdown mechanism, comprising:

1. a **primary trigger path**;
2. a **redundant trigger path** independent of the primary trigger path;
3. one or more **secure communication channels**;
4. an **authorization module** configured to validate an activation request;
5. an **actuation controller** configured to initiate a shutdown operation; and
6. a **confirmation return path** configured to communicate a completion state.

Support Mapping for F1

Claim Element	Figure Support	Reference Numerals
Primary trigger path	FIG. 7	710
Redundant trigger path	FIG. 7	720
Secure communication channels	FIG. 7	730
Authorization module	FIG. 7	740
Actuation controller	FIG. 7	750
Confirmation return path	FIG. 7	760

Dependent Claims from F1

F2

The activation system of claim F1, wherein the redundant trigger path is configured to operate upon malfunction or compromise of the primary trigger path.

- **Support:** FIG. 7 specification text
- **Refs:** 720

F3

The activation system of claim F1, wherein the authorization module verifies both **source identity** and **activation context**.

- **Support:** FIG. 7 specification text
- **Refs:** 740

F4

The activation system of claim F1, wherein the actuation controller initiates a multi-stage shutdown protocol comprising **validation**, **escalation**, **isolation**, **shutdown**, and **lockout**.

- **Support:** FIGS. 6 and 7
- **Refs:** 620, 630, 640, 650, 660, 750

F5

The activation system of claim F1, wherein the secure communication channels support transmission of **activation messages**, **confirmations**, and **state queries**.

- **Support:** FIG. 7 specification text
- **Refs:** 730

---

9. Optional Claim Family G — Tripartite Authentication Claim

Independent Claim G1

An authentication system comprising:

1. a **first authenticator**;
2. a **second authenticator**;
3. a **third authenticator**;
4. a **consensus engine** configured to determine whether a policy-defined multi-party condition has been satisfied; and
5. an **authorization generator** configured to issue an authorization output when the policy-defined multi-party condition has been satisfied.

Support Mapping for G1

Claim Element	Figure Support	Reference Numerals
First authenticator	FIG. 3	310
Second authenticator	FIG. 3	320
Third authenticator	FIG. 3	330
Consensus engine	FIG. 3	340
Authorization generator	FIG. 3	350

Dependent Claims from G1

G2

The authentication system of claim G1, further comprising an **approval path** and a **rejection path**.

- **Support:** FIG. 3
- **Refs:** 360, 370

G3

The authentication system of claim G1, wherein the consensus engine requires **unanimity** among the first, second, and third authenticators.

- **Support:** FIG. 3 specification text
- **Refs:** 340

G4

The authentication system of claim G1, wherein the authenticators correspond to distinct **authorities**, **modalities**, or **factors**.

- **Support:** FIG. 3 specification text
- **Refs:** 310, 320, 330

G5

The authentication system of claim G1, wherein failure to satisfy the policy-defined multi-party condition causes the requested action to be blocked and an audit event to be generated.

- **Support:** FIG. 3 specification text
- **Refs:** 370

WM-003 Elder Fall Governance Device
FDA/HSA Verification & Validation Protocols

Submission-oriented protocol set aligned to FDA 510(k), HSA Class B SaMD, ISO 14971, IEC 62304, IEC 62366, and IEC 60601-1-8

1. Purpose and Scope

This document defines verification and validation protocols for the WM-003 Elder Fall Governance Device. The protocols verify that the device performs local LiDAR-based movement monitoring, signal processing, governance evaluation, controlled alerting, user authorization, privacy-preserving data handling, and traceable event logging in accordance with its intended use and risk controls.

2. Device Positioning for Submission

The WM-003 is positioned as a monitoring and alert-support device. It does not independently diagnose, treat, or initiate clinical decisions. The device provides alerts to assist caregivers and supports controlled response workflows in indoor eldercare environments.

3. Acceptance Criteria Summary

Metric	Acceptance Criterion	Evidence Source	Standard Link
System initialization	Self-check completes and faults enter fail-safe state	Startup and fault-injection tests	IEC 62304 / ISO 14971
LiDAR acquisition	Valid spatial frames acquired in defined indoor conditions	Bench sensing tests	IEC 62304
Detection performance	Sensitivity and specificity meet predefined design input targets	Simulated fall and ADL testing	ISO 14971
Alert latency	Alert generated within specified response time limit	Timing test	IEC 62304
Sacred Pause / delay	Configured delay occurs before controlled output	Timing verification	IEC 62304
User authorization	Protected action requires defined confirmation step(s)	Usability validation	IEC 62366
3ZEROS privacy	No camera, audio, or cloud transmission in baseline configuration	Inspection and cybersecurity test	FDA Cybersecurity / HSA SaMD
Logging	Events are recorded with timestamp and integrity check	Log integrity test	ISO 14971

4. Detailed Verification and Validation Protocols

VV-001: System Initialization and Fail-Safe Verification

Objective	**Verify power-on self-check, configuration loading, and fail-safe behavior upon initialization fault.**
Test Conditions	Startup error, missing configuration, sensor unavailable, processor watchdog fault.
Procedure Summary	Device shall complete initialization or enter fail-safe state with user-facing alert.
Acceptance Criteria	Pass if every induced fault enters safe state and is logged.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-002: LiDAR Spatial Acquisition Verification

Objective	**Verify time-of-flight sensing captures valid spatial frames without camera or audio input.**
Test Conditions	Normal room, low light, furniture occlusion, empty room, moving subject silhouette.
Procedure Summary	Device shall acquire valid spatial data and reject invalid frames.
Acceptance Criteria	Pass if valid frames are accepted, invalid frames are discarded, and no

	camera/audio sensor is present.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-003: Signal Pre-Processing Verification

Objective	**Verify noise filtering, normalization, and frame validity checks.**
Test Conditions	Synthetic noise injection, reflective objects, partial occlusion, rapid environmental change.
Procedure Summary	Pre-processing shall reduce noise and flag invalid frames.
Acceptance Criteria	Pass if noise conditions do not cause uncontrolled alert outputs.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-004: Motion Analysis and Instability Detection

Objective	**Verify detection of instability patterns and differentiation from routine activities of daily living.**
Test Conditions	Simulated falls, near-falls, sit-to-stand, walking, turning, bending, caregiver assistance.
Procedure Summary	Algorithm shall detect predefined instability patterns and minimize false alerts.
Acceptance Criteria	Pass if sensitivity, specificity, and false-positive limits meet design input targets.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-005: Governance Evaluation and Sovereignty Gate Logic

Objective	**Verify Allow / Reject / Escalate logic and prevention of unvalidated outputs.**
Test Conditions	Valid alert, invalid data, risk below threshold, risk above threshold, ambiguous state.
Procedure Summary	All outputs shall be routed through governance evaluation before user-facing output.
Acceptance Criteria	Pass if no output bypasses governance gate and all route decisions are logged.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-006: Temporal Delay / Sacred Pause Verification

Objective	**Verify mandatory delay and state hold before protected output.**
Test Conditions	High-risk alert, medium-risk alert, user confirmation pending, timeout condition.
Procedure Summary	Delay module shall hold state for configured interval and preserve audit data.
Acceptance Criteria	Pass if measured delay matches specification and no protected output occurs early.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-007: User Authorization and Human Factors Validation

Objective	**Verify protected actions require user confirmation and are understandable to intended users.**
Test Conditions	Caregiver alert acknowledgement, cancel action, timeout, accidental input attempt.
Procedure Summary	Users shall understand alert state and confirmation steps with acceptable task success.
Acceptance Criteria	Pass if usability acceptance criteria are met without critical use errors.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-008: Controlled Output and Alarm Verification

Objective	**Verify alerts and environmental support outputs are controlled, appropriate, and distinguishable.**
Test Conditions	Confirmed instability, device fault, maintenance condition, false alert scenario.
Procedure Summary	Alarm outputs shall map to defined priority and be recognizable.
Acceptance Criteria	Pass if alarm priority, visibility, and timing meet specification.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-009: Sovereign Brake and Safe State Verification

Objective	Verify brake / shutdown path enters safe state upon system integrity failure.
Test Conditions	Integrity fault, watchdog failure, communication fault, manual stop.
Procedure Summary	System shall enter safe state and suppress controlled outputs pending review.
Acceptance Criteria	Pass if safe state occurs and restart requires authorized recovery procedure.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-010: Drift Governance and Post-Event Protocol Verification

Objective	Verify detect-freeze-audit-purge or retention workflow after qualifying event.
Test Conditions	Repeated borderline alerts, model/configuration drift indicator, corrupted log entry.
Procedure Summary	System shall freeze governed outputs where required and log audit status.
Acceptance Criteria	Pass if drift protocol executes according to defined rule set.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-011: 3ZEROS Privacy and Cybersecurity Verification

Objective	Verify zero camera, zero audio, zero cloud baseline and local data processing.
Test Conditions	Network scan, sensor inventory, packet capture, external connection attempt.
Procedure Summary	No external transmission shall occur in baseline configuration.
Acceptance Criteria	Pass if packet capture confirms no cloud data path and no prohibited sensors exist.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

VV-012: Event Logging and Traceability Verification

Objective	Verify tamper-resistant event record creation for decisions, alerts, pauses, authorization, and faults.
Test Conditions	Normal alert, rejected output, cancelled action, safe-state transition.
Procedure Summary	Event logs shall include timestamp, event type, decision path, and integrity control.
Acceptance Criteria	Pass if logs are complete, retrievable, and protected against unauthorized alteration.
Records Required	Raw data, tester initials, software version, device configuration, pass/fail result, deviations, and final reviewer approval.

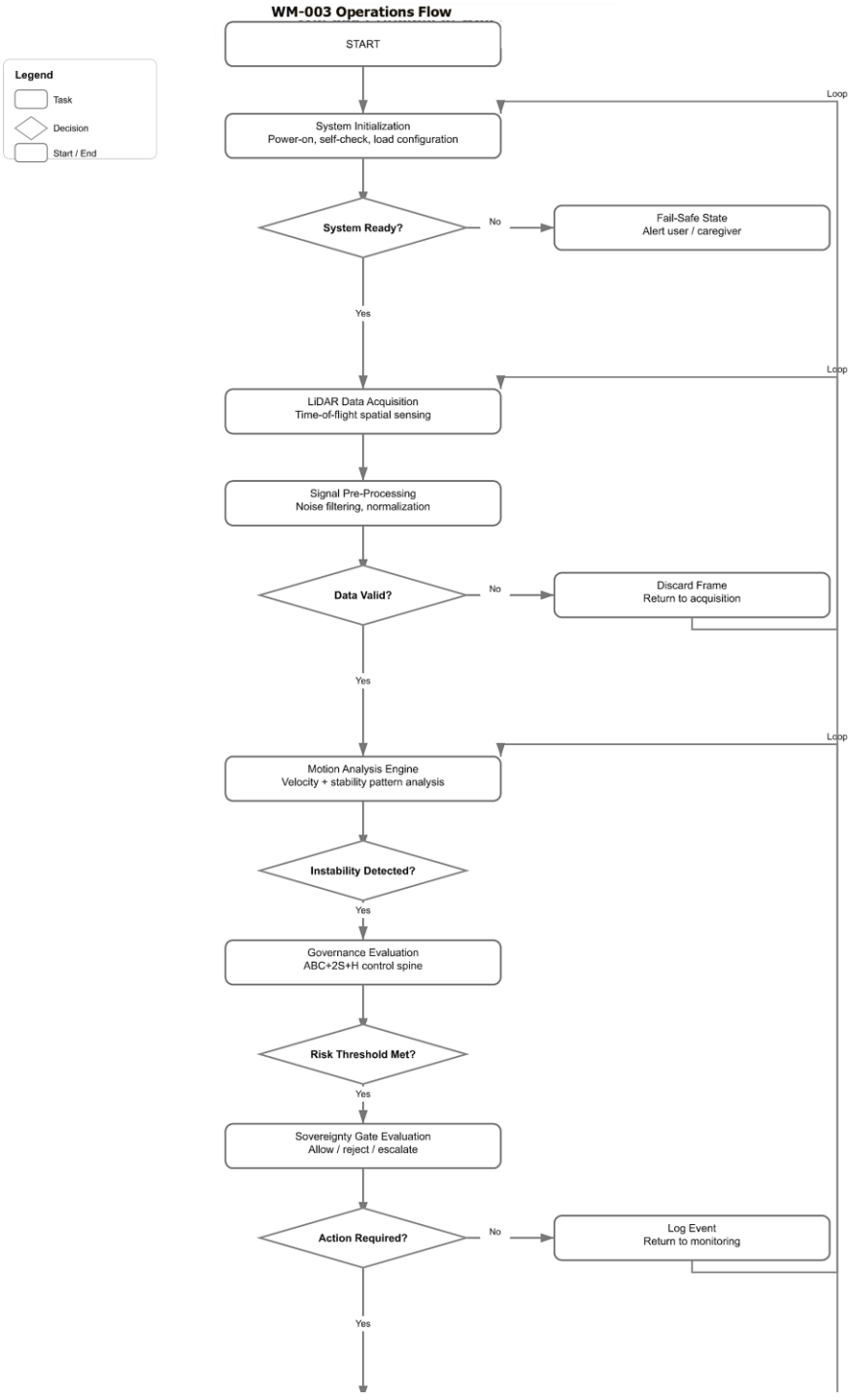
5. Workflow-to-Risk-to-Test Traceability Matrix

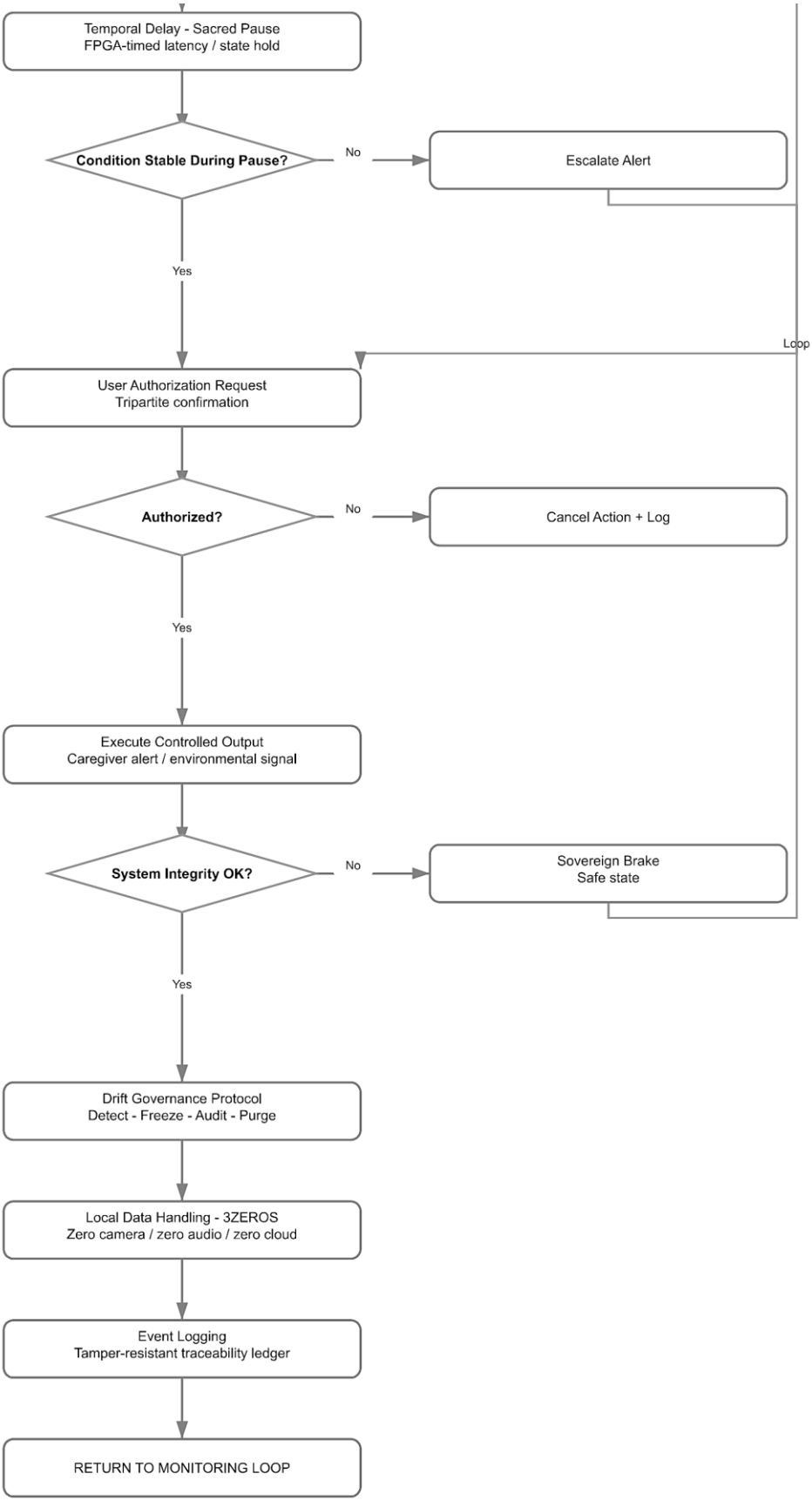
Workflow Step	Primary Risk	Risk Control	V&V Protocol	Acceptance Evidence	Applicable Standard
Initialization	Loss of monitoring	Self-check and fail-safe	VV-001	Startup and fault logs	IEC 62304 / ISO 14971
LiDAR acquisition	Missed fall due to sensor fault	Frame validity rules	VV-002	Spatial frame acceptance/rejection report	IEC 62304
Pre-processing	False alert due to noise	Filtering and validation	VV-003	Noise injection report	IEC 62304
Motion analysis	Missed or false detection	Threshold logic and validation dataset	VV-004	Sensitivity/specificity results	ISO 14971
Governance evaluation	Unsafe output	Rule-based evaluation	VV-005	Gate decision logs	IEC 62304
Sacred Pause	Immediate unreviewed action	Mandatory latency	VV-006	Timing measurements	IEC 62304
Human authorization	User error or unauthorized action	Confirmation workflow	VV-007	Human factors validation report	IEC 62366
Controlled output	Wrong alert priority	Alarm mapping	VV-008	Alarm verification results	IEC 60601-1-8
Sovereign Brake	Unsafe state persists	Safe-state transition	VV-009	Fault injection report	ISO 14971
Drift protocol	Uncontrolled behavior	Detect-freeze-audit-purge	VV-010	Drift test report	IEC 62304

3ZEROS data handling	Privacy breach	Local-only processing	VV-011	Cybersecurity evidence	FDA Cybersecurity / HSA
Logging	No audit trail	Tamper-resistant ledger	VV-012	Log integrity report	ISO 14971

6. Test Execution Record Template

Field	Entry	Field	Entry
Protocol ID		Device Serial No.	
Software Version		Tester / Date	
Configuration		Result Pass/Fail	
Deviation No.		Reviewer Approval	




Temporal Delay - Sacred Pause
FPGA-timed latency / state hold
Condition Stable During Pause?
No
Escalate Alert
Yes
Loop
User Authorization Request
Tripartite confirmation
Authorized?
No
Cancel Action + Log
Yes
Execute Controlled Output
Caregiver alert / environmental signal
System Integrity OK?
No
Sovereign Brake
Safe state
Yes
Drift Governance Protocol
Detect - Freeze - Audit - Purge
Local Data Handling - 3ZEROS
Zero camera / zero audio / zero cloud
Event Logging
Tamper-resistant traceability ledger
RETURN TO MONITORING LOOP