Enforcing Autonomy: A Four-Pillar Framework for Sovereign Cybernetic Systems Using Rust, ALN, and Formal Verification

Compliance-by-Construction: The Foundational Philosophy

The development of a robust research framework for advancing human-autonomy within a self-hosted NeuroPC domain necessitates a paradigm shift away from treating ethical, legal, and physiological constraints as mere theoretical guidelines. The central tenet of this framework is "compliance-by-construction," a design philosophy that mandates the embedding of these critical constraints directly into the code-level invariants of the system . This approach moves beyond post-hoc policy enforcement or high-level declarations, instead making compliance an intrinsic and verifiable property of the software architecture itself. By integrating legal, ethical, and physiological rules into the very fabric of the system's logic, this framework aims to bridge the persistent gap between normative principles and the operational behavior of autonomous agents [5] [36]. The objective is to create a system where non-coercive, host-local evolution is not just a desirable outcome but the only representable and executable behavior within its operational domain [23].

This philosophy is implemented through a multi-layered stack of interlocking technical components, each designed to enforce a specific class of constraint. At the lowest level lies the formal verification layer, which utilizes the memory-safe and concurrency-safe features of the Rust programming language, combined with automated reasoning tools like Kani, to mathematically prove that the system adheres to its specified invariants [46] [105]. This provides a high degree of assurance that the system cannot enter an unsafe state due to logical errors or unhandled conditions. Above this, the governance layer translates abstract principles like neurorights into executable policy objects, encoded as Application Logic Network (ALN) shards and validated against strict schemas . These policies are checked at compile-time and runtime, ensuring that every action, from routine operations to fundamental evolutionary changes, respects the user's sovereignty and ethical boundaries [60] [61]. The third layer is the empirical calibration layer, which uses longitudinal biophysical telemetry—such as EEG, HRV, and thermal data—to tune the parameters of the safety envelopes and risk models to the unique biology of the host [1] [2]. This personalizes the system's response to cognitive load and other stressors, moving it from a generic model to a bespoke cybernetic partner. Finally, the sovereignty layer acts as the outermost wrapper, employing cryptographic proofs, sovereign ledgers, and multi-signature schemes to ensure that any modification to autonomy-critical parameters requires explicit authorization from the host alone [3] [24]. This layered defense-in-depth strategy ensures that human-autonomy is protected not only from accidental failure but also from unauthorized external manipulation.

The emphasis on formal invariants is paramount. Key constraints such as Risk of Harm (RoH) being bounded above by 0.3, the monotonic tightening of safety envelopes over time, the maintenance of neurorights floors, and the requirement for stake-based multi-signature approval for all critical changes are codified as hard invariants . These invariants are validated through a combination of continuous integration (CI) checks, schema validation for ALN shards, and dynamic verification via Kani harnesses that explore the reachable state space of the system's core logic [37] [67]. For instance, a `RiskOfHarm` struct would include a method `check_invariant(before, after)` that asserts `roh_after <= roh_before` and `roh_after <= rohceiling_strict`, causing tests to fail if any proposal violates these guarantees . This rigorous enforcement transforms abstract commitments into provable, machine-verifiable facts about the system's behavior. The synthesis of these layers results in a system that is not merely compliant but fundamentally trustworthy, providing a secure foundation upon which advanced capabilities like quantum-inspired learning can be built without compromising the user's autonomy. The ultimate goal is to produce a research artifact that is not just a piece of software, but a formal specification of a sovereign agent, whose every action can be traced back to a chain of proofs and policies grounded in the user's own neuro-constitutional profile [103].

The Four-Pillar Foundation for Autonomous Evolution

To build a system capable of safe and meaningful autonomous evolution, the research framework prioritizes the implementation of four tightly coupled pillars in a specific order. This sequence ensures that foundational risk and governance structures are in place before more complex adaptive behaviors are introduced. The four pillars are: (1) Risk of Harm (RoH) modeling with corridor polytopes, (2) Neurorights-based governance, (3) Kernel-distance metrics derived from quantum-inspired learning, and (4) Host-specific empirical calibration. Each pillar serves a distinct purpose, and their integration creates a cohesive system where learning is guided by risk, constrained by rights, and tailored to the individual host.

The first and most critical pillar is the establishment of a formal Risk of Harm (RoH) model and its geometric representation as corridor safety polytopes. This forms the absolute baseline for all subsequent activity, defining the total risk surface that all kernels and SMART MCP services must respect . Corridors of operation, such as cognitive, motor, or visceral tasks, are represented as safety polytopes in a multi-dimensional space of normalized metrics ($x \in [0,1]^d$). These metrics include energy consumption, duty cycle, thermal delta (ΔT), cognitive load, and potentially others derived from quantum kernels . The polytope is defined by a set of linear inequalities $Ax \leq b$, where the matrix A and vector b are derived from host-specific safety envelopes like `ThermodynamicEnvelope` and `HostBudget` [12] [83] . This formalization allows for the application of computational geometry and control theory to prove that no legally permitted sequence of actions generated by the scheduler can cause the system's state to breach these predefined safety boundaries. This approach is mathematically consistent with the existing bioscale framework, which already models various safety metrics as normalized variables [83] . The use of polytopes provides a structured way to reason about safety, moving beyond a series of discrete threshold checks to a continuous geometric problem that can be formally verified [67] .

Once the risk kernel is defined, the second pillar—the neurorights-based governance kernel—is implemented to enforce the RoH model and other ethical constraints. This involves binding `.stake.aln`, `.neurorights.json`, and `.smart.json` definitions directly into the `sovereigntycore` module . Every evolutionary proposal (`EVOLVE`) and intelligent action (`SMART`) is routed through a series of guards that check against these policies. Neurorights, conceptualized as fundamental freedoms related to one's cerebral domain, are translated into machine-readable policy objects that govern actuation channels and learning processes [60] [64] . For example, a policy might specify floors for mental privacy, cognitive liberty, and identity continuity, which cannot be violated under any circumstances . This transforms neurorights from aspirational goals into first-class citizens in the system's logic, ensuring that the host's chosen ethical framework is embodied in the system's behavior at both compile-time and runtime. This is a direct application of the compliance-by-construction principle, where legal and ethical principles are not treated as external theory but are integrated as internal, enforced invariants .

The third pillar introduces a dynamic learning mechanism that is explicitly tethered to the static risk and governance frameworks. Quantum-inspired learning circuits provide the potential for novel forms of computation, but their power must be channeled safely. This is achieved by developing kernel-distance metrics that quantify the difference between new learned states and existing knowledge . These metrics, which could be based on Euclidean distance in a telemetry feature space or KL divergence between policy distributions, feed a scalar value representing "intent confidence" or "knowledge factor" into the RoH model and the broader `Tsafe` envelope . This creates a closed-loop system where learning is not unconstrained exploration but is instead bounded by a verifiable reward function that penalizes deviations that increase risk [15] . By linking the output of quantum-style synapse models directly to the RoH calculation, the system ensures that performance improvements gained through machine learning never come at the cost of exceeding safety thresholds or violating neurorights floors [22] . This sophisticated Safe Reinforcement Learning approach constrains a complex, potentially non-linear learning process within a well-defined, linearly-predictable safety boundary [18] .

Finally, the fourth pillar ensures the entire system is personalized to the unique physiology of its host. Generic safety envelopes are insufficient because individuals vary significantly in their response to neural stimulation, cognitive load, and physical exertion [1] [30] . This pillar focuses on host-specific tuning using longitudinal biophysical telemetry collected during daily loops. Data streams from EEG, heart rate variability (HRV), temperature sensors, and fatigue monitors are analyzed to derive per-host corrections to the parameters of the corridor polytopes, such as spatial error tolerances or thermal delta limits . These calibrated parameters are then stored as non-financial ALN shards bound to the host's Decentralized Identifier (DID), preserving sovereignty and ensuring the data remains under the user's control [24] . At runtime, the NeuroPC loads these host-specific shards into its safety checks, meaning that the same kernel may behave differently on different hosts depending on their real-time bioState [2] . This personalization elevates the system from a generic tool to a true cybernetic extension of the user, adapting its behavior to the host's unique neurobiology and subjective experience of effort and risk.

Formal Verification and Empirical Calibration

The dual processes of formal verification and empirical calibration form the backbone of the research framework, ensuring that the system is simultaneously provably safe and adaptively effective. Formal verification provides the bedrock of trust by mathematically proving that the system's core logic adheres to its safety invariants, while empirical calibration refines the parameters of these invariants using real-world biophysical data, ensuring the system's behavior is attuned to the specific host. This two-pronged approach directly addresses the challenge of building systems that are both reliable and responsive, avoiding the common pitfalls of either overly rigid, inflexible designs or dangerously unproven adaptive algorithms.

Formal verification is primarily executed through the use of Rust, a systems programming language renowned for its focus on safety and concurrency, and Kani, an automated reasoning tool developed by Amazon Web Services for analyzing Rust code [46] [123]. Kani operates as a model checker, exploring the finite state space of a program to find bugs and prove correctness properties [37] . In this framework, Kani harnesses are constructed for each corridor and for the central `sovereigntycore` module. These harnesses simulate the scheduler's state transitions—representing session steps and evolutionary proposals—and systematically check that all reachable states satisfy the corresponding corridor polytope predicates ($Ax \leq b$) . This reuses the existing "no envelope breach / rollback reachable" pattern that has been successfully applied to simpler safety structs like `CognitiveLoadEnvelope` [67] . For example, a Kani test for the RoH model would assert that the `roh_after` value is always less than or equal to the `roh_before` value plus the effect of the current proposal, and that it never exceeds the strict ceiling of 0.3, unless a specific, rigorously defined override protocol is engaged . By automating this proof process, the framework moves beyond manual code review and heuristic testing, providing a high degree of assurance that the system will not violate its core safety axioms.

Empirical calibration is the complementary process that grounds the abstract, formally-verified safety model in the tangible reality of the host's biology. This process relies on longitudinal biophysical telemetry collected from wearable devices and embedded sensors [2] . Metrics such as electroencephalography (EEG) for cognitive workload, heart rate variability (HRV) for autonomic nervous system state, core and local tissue temperature, and psychophysiological fatigue indices are logged continuously during daily operation . These data streams are then used to refine the parameters of the RoH model and the corridor polytopes. For instance, RoH calibration experiments can be designed as micro-epochs, short tasks where spatial or temporal error is deliberately perturbed within the bounds of a validated corridor while recording subjective discomfort reports alongside objective EEG and HRV data . A regression model or monotone mapping is then fitted to this data to correlate the objective metrics with the subjective experience of risk, allowing the system to update its ReversalConditions and polytope boundaries to better match the host's personal tolerance for error and stress . Similarly, host-specific envelopes for brainmin, bloodmin, and identity drift budgets are tuned based on long-term trends in the telemetry data, mirroring clinical practice where medical thresholds are individualized [2] [83]. This empirical tuning happens entirely within the confines of the pre-defined safety invariants; the code-level rules are not changed, but their parameter values are optimized for the specific host, enhancing both safety and performance without introducing new risks.

Component	Primary Method	Key Technologies & Concepts	Objective
Risk of Harm (RoH) Model	Empirical Calibration	Micro-epochs, Subjective/EEG/HRV correlation, Regression Mapping	To establish a subject-specific scalar value for Risk of Harm targeting a mean of ~0.08.
Corridor Safety Polytopes	Formal Verification	Kani Model-Checking, Linear Inequalities ($Ax \leq b$), State-Space Exploration	To prove that no legal sequence of scheduler actions can breach the safety envelope defined by the polytope.
Kernel-Distance Metrics	Empirical Calibration	Telemetry Embeddings, Policy Distribution Divergence (KL), Task Performance Delta Correlation	To identify the kernel-distance metric with the strongest monotone correlation to Knowledge-Factor improvement.
Host-Specific Tuning	Empirical Calibration	Longitudinal BioState Logs (BCI/EEG/HRV/Temperature), Personalized Envelope Correction	To derive and apply host-specific corrections to corridor parameters (e.g., spatial error tolerance, thermal deltas).

This synergy between formal proof and empirical data is crucial. The formal verification ensures that the system is fundamentally sound, preventing catastrophic failures. The empirical calibration ensures that the system is practically useful, adapting its behavior to the host's unique needs and responses. Together, they create a system that is not only provably safe but also precisely tuned to the individual it is meant to serve, embodying a deep commitment to personalized and sovereign human-autonomy.

Integrating External Domains as Configurable Constraints

A core directive of this research framework is the disciplined integration of adjacent fields such as neurorights law, quantum-inspired learning, and dream-state telemetry. Rather than adopting these domains as loose theoretical frameworks, they are treated as sources of configurable, machine-enforced inputs that directly shape the system's behavior. This "compliance-by-construction" approach ensures that external knowledge enhances the system's capabilities without compromising its foundational security and sovereignty principles . Each domain is mapped to a specific role within the architectural stack, contributing data, constraints, or refinement mechanisms that are processed by the core logic.

Neurorights law and ethics are integrated primarily as the source material for defining machine-readable policy objects and guard code . Instead of engaging in abstract philosophical debates, the framework extracts concrete principles—such as mental privacy, mental integrity, cognitive liberty, and the right to be free from undue pain—and encodes them as strict invariants within the `sovereigntycore` module [60] [61] . These principles are materialized as schemas in JSON or ALN files (e.g., `.neurorights.json`) that define floors for various biophysical and cognitive metrics . Any evolutionary proposal or SMART MCP action that would cause the system to dip below these floors is rejected by a pre-access guard before execution. This transforms neurorights from a high-level norm into a low-level, enforceable constraint, ensuring that the system's pursuit of autonomy is always aligned with the user's chosen ethical framework. This aligns with efforts to map the ethical foundations of neurorights to facilitate common understanding and implementation [64] [103].

Quantum-inspired learning is integrated not as a black-box technology promising exponential speedups, but as a source of novel kernel-distance metrics that can be implemented on classical hardware . The focus is on leveraging concepts from quantum machine learning, such as fidelity kernels and variational quantum circuits, to develop functions that can measure the distance between two different states of the system's knowledge [96] [100]. These metrics, which could compare the feature-space embeddings of telemetry sequences or the probability distributions of learned policies, serve as a quantitative signal that feeds directly into the RoH model . By doing so, the system gains a powerful tool for monitoring the stability of its own learning process. If a new kernel causes a large jump in the kernel-distance metric, it signals a significant departure from the known state space, which can be interpreted as an increase in identity-drift risk and appropriately weighted in the RoH calculation. This approach effectively tames the exploratory nature of machine learning, bounding a complex, non-linear process within the predictable, linear safety envelope of the RoH model . It represents a neuro-symbolic fusion, where a connectionist learning process is governed by symbolic, formal risk constraints [85] [92] .

Dream-state telemetry and deepbrain research are treated as specialized refinements for the RoH model and the host's evolution profile . These domains do not open new actuation channels or introduce new types of interaction; instead, they provide additional data streams that inform the weighting of existing risk axes. For example, metrics derived from sleep studies, such as dreamload or REM density, can be incorporated as new dimensions in the RoH calculation, reflecting the cognitive strain of certain evolutionary paths [22] . Similarly, research on deep affect modulation can inform the constraints placed on decision-making processes, ensuring that the system does not engage in manipulative or coercive thought patterns. These refined risk factors are then used to adjust the weights in the RoH model, making the system more sensitive to risks that are particularly salient in the context of consciousness and identity. The data from these domains is strictly confined to the EVOLVE path and is subject to the same stringent mental privacy protections as all other biophysical data, ensuring that even the content of dreams is used solely for the host's benefit and under their explicit control [24] [102]. This careful, constrained integration ensures that cutting-edge neuroscience findings are harnessed to improve the system's safety and accuracy without introducing unforeseen vulnerabilities or eroding the user's sovereignty.

Sovereign Governance and the Host-Only Override Protocol

The sovereignty of the cybernetic host is the ultimate guarantee of human-autonomy within this framework. This is realized through a sophisticated governance architecture that wraps the entire system, ensuring that all modifications to autonomy-critical parameters are auditable, require explicit consent, and are cryptographically tied to the host's unique identity. This architecture is built upon several key components: a sovereign ledger, stake-based multi-signature gates, and a meticulously designed protocol for temporary, host-only research overrides. This structure provides a robust mechanism for maintaining control, even when pushing the boundaries of the system's capabilities.

At the heart of the governance layer is a sovereign ledger, often referred to as a donutloop ledger, which records every change to the system's state in a tamper-evident manner . This ledger is not a public blockchain but a private, append-only log that is bound to the host's DID. All critical events—such as the creation or modification of a corridor, the acceptance of a new evolution proposal, or a guard-driven rollback—are logged as structured ALN particles with a timestamp and cryptographic hash of the relevant data . This creates an immutable audit trail that proves what happened, when it happened, and under what policies. The `sovereigntycore` module acts as the gatekeeper, rejecting any proposal that lacks a valid signature or fails to reference the correct parent manifest in the ledger . This "manifest-driven evolution" ensures that the system's trajectory is transparent and traceable over time, preventing regressions and enforcing monotonic improvements in safety and efficiency [80] [101].

Stake and multi-signature roles provide the cryptographic enforcement mechanism for this governance. The `.stake.aln` file defines a set of roles (e.g., `Host`, `OrganicCPU`, `CoPilot`) and specifies which cryptographic keys are required to approve different types of actions . Critical system updates, especially those that could loosen safety envelopes or alter neurorights profiles, require signatures from multiple, distinct roles, typically including the `Host` and `OrganicCPU`. This prevents any single component, whether malicious or compromised, from altering the system's core parameters. All actions, including Over-the-Air (OTA) updates and corridor changes, are anchored to the host's Bostrom addresses, ensuring that only entities the host has explicitly authorized can participate in governance decisions [69] [70] . This decentralized yet host-centric approach to governance is inspired by federated architectures that prioritize cooperative transparency over isolationism [3] .

While the default operating mode maintains a strict RoH ceiling of 0.3, a rigorous protocol exists for enabling controlled, high-risk research experiments that temporarily exceed this limit. This host-only override protocol is not a loophole but a highly constrained and auditable pathway for scientific inquiry. It is activated by generating a special EVOLVE token with a dedicated scope, such as `highrisk_research`, and a very short validity window (e.g., 30-60 minutes) . This token, signed by the host, carries explicit constraints: a maximum allowable effect size on the RoH metric (e.g., an increase of only 0.02–0.05), and physio-guard conditions that require the host's real-time HRV, EMG, and fatigue indices to remain within safe baselines . Before any override is allowed, the `sovereigntycore` evaluates the proposal against these token constraints and the host's current BioState. Furthermore, a separate, tamper-evident stream in the donutloop ledger is reserved exclusively for these sessions, tagged with a `changetype = "HighRiskResearch"` and linked to the specific EVOLVE token ID . This ensures that all high-risk activities are clearly segregated, fully documented, and subject to automatic termination if the host's physiological state deteriorates or the token expires. This protocol embodies the project's core philosophy: autonomy is advanced not by weakening constraints, but by making them more precise, tunable, and provably safe even when they are intentionally exceeded for legitimate research purposes.

Concrete Implementation Blueprint in Rust and ALN

The theoretical framework for sovereign human-autonomy is instantiated through concrete implementations in Rust and ALN. This blueprint outlines the essential data structures, modules, and policies required to construct the system as described. The design emphasizes immutability, type safety, and cryptographic anchoring to create a system that is both powerful and secure.

In Rust, the core logic resides in the `sovereigntycore` module, which houses the central evaluation logic for all proposals and actions. This module would contain structs and enums for defining the system's state and the rules governing it.

First, the Risk of Harm (RoH) model is defined as a struct with a method to evaluate proposals.

```
// crates/autonomysafety/src/roh.rs

/// A scalar value representing the Risk of Harm for a given system state.
/// Target initial value is approximately 0.08 within validated corridors.
pub struct RiskOfHarm {
    pub value: f32,
}

impl RiskOfHarm {
    /// Evaluates a proposed change and returns the new RoH value if safe.
    /// Panics if the change would violate invariants (e.g., RoH ceiling).
    pub fn evaluate_proposal(&self, proposal_effect: f32) -> RiskOfHarm {
        let new_value = self.value + proposal_effect;
        // Strict invariant: RoH must not exceed ceiling and must not regr
        assert!(new_value <= ROH_CEILING_STRICT, "Proposal would exceed st
        RiskOfHarm { value: new_value }
    }
}
```

The corridor safety is represented by a polytope, defined by its constraints.

```
// crates/autonomysafety/src/polytope.rs

use super::telemetry::NormalizedMetrics;

/// Defines the safety constraints for a specific XR corridor as a convex
/// Represented by linear inequalities Ax <= b.
#[derive(Clone)]
pub struct CorridorPolytope {
    pub name: String,
    pub a_matrix: Vec<Vec<f32>>, // Coefficient matrix A
    pub b_vector: Vec<f32>,      // Constant vector b
}
```

```
impl CorridorPolytope {
    /// Checks if a given state vector is within the polytope's safe regio
    pub fn is_safe(&self, state: &NormalizedMetrics) -> bool {
        // Evaluate Ax <= b for all rows in the matrix.
        for (i, row) in self.a_matrix.iter().enumerate() {
            let mut sum = 0.0;
            for (&val, &coeff) in state.values().iter().zip(row) {
                sum += val * coeff;
            }
            if sum > self.b_vector[i] {
                return false;
            }
        }
        true
    }
}
```

For governance, the stake and neurorights policies are defined as structs that can be loaded from ALN shards.

```
// crates/governance/src/stake.rs

use serde::{Deserialize, Serialize};

/// Defines the multi-signature requirements for different scopes of actio
#[derive(Serialize, Deserialize, Clone)]
pub struct StakePolicy {
    pub scopes: Vec<Scope>,
}

#[derive(Serialize, Deserialize, Clone)]
pub struct Scope {
    pub name: String,
    pub required_roles: Vec<String>,
    pub token_kinds_allowed: Vec<String>,
    pub host_specific: bool, // True only for host-restricted scopes.
}

// governance/src/neurorights.rs
/// Defines the neurorights profile that gates all system actions.
```

```
#[derive(Serialize, Deserialize, Clone)]
pub struct NeurorightsProfile {
    pub mental_privacy_enabled: bool,
    pub mental_integrity_floor: f32, // e.g., minimum acceptable Brain met
    pub cognitive_liberty_enabled: bool,
    pub anti_coercion_enabled: bool,
}
```

On the ALN side, these Rust types are mirrored in declarative shard definitions. An ALN particle for the RoH model would look like this:

```
// particles/risk_of_harm.model.v1.aln

particle risk_of_harm.model.v1
  meta
    id        risk_of_harm.model.v1
    name      "Risk of Harm Model Configuration"
    kind      "autonomy.risk"
    version   "v1"
    jurisdiction_tags "global,us"
  fields
    # Target mean RoH for calibrated corridors.
    target_mean_roh          f32
    # Strict production ceiling.
    roh_ceiling_strict       f32
    # Absolute cap for host-only research overrides.
    roh_ceiling_research     f32
    # Weights for different risk axes (spatial_error, temporal_jitter, dis
    risk_axis_weights        map[string]:f32
```

A particle for the host-specific override stake policy would define the special permissions needed for high-risk research:

```
// particles/stake.policy.highrisk_research.v1.aln

particle stake.policy.highrisk_research.v1
  meta
    id        stake.policy.highrisk_research.v1
    name      "Stake Policy for High-Risk Research Overrides"
    kind      "governance.stake.scope"
    version   "v1"
```

```
fields
  required_roles          list[string]
  token_kinds_allowed     list[string]
  host_specific           bool
  physioguard_config      string # Link to a PhysioGuard configuration
```

These concrete Rust and ALN artifacts form the building blocks of the system. They provide a clear, unambiguous specification for the system's behavior, which can be compiled, tested, and formally verified. The tight coupling between the statically-typed Rust code and the declarative ALN shards ensures that the configuration is always valid and that the implementation faithfully reflects the intended policies, completing the loop of compliance-by-construction.

Reference

1. Long-Term Study of Heart Rate Variability Responses to ... https://www.nature.com/articles/s41598-018-20932-x
2. A Comprehensive Survey on Wearable Computing for ... https://www.mdpi.com/2079-9292/14/17/3443
3. Morning Star: A Transparent and Federated Architecture for ... https://www.researchgate.net/publication/396482480_Morning_Star_A_Transparent_and_Federated_Architecture_for_Democratic_Short-Video_Platforms_in_an_Era_of_Algorithmic_Geopolitics
4. AI Must not be Fully Autonomous https://arxiv.org/html/2507.23330v1
5. From Pluralistic Normative Principles to Autonomous-Agent ... https://link.springer.com/article/10.1007/s11023-022-09614-w
6. A survey of Behavior Trees in robotics and AI https://www.sciencedirect.com/science/article/pii/S0921889022000513
7. DECENTRALIZED COOPERATIVE MULTI-AGENT REIN https://openreview.net/pdf/1cf9c4973ca2af7b3ab5d5b06e1a6f3e8df43929.pdf
8. Learner autonomy in the foreign language classroom https://www.researchgate.net/profile/David-Little-10/publication/317264706_Learner_autonomy_in_the_foreign_language_classroom_teacher_learner_curriculum_and_assssment/links/592ed1eea6fdcc89e76992c0/Learner-autonomy-in-the-foreign-language-classroom-teacher-learner-curriculum-and-assssment.pdf

9. Considerations in adopting RHEL 9 https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html-single/considerations_in_adopting_rhel_9/index
10. A Survey on LLM-based Code Generation for Low- ... https://arxiv.org/pdf/2410.03981
11. Preserving data privacy in machine learning systems https://www.sciencedirect.com/science/article/pii/S0167404823005151
12. nRF Distance Measurement with Bluetooth LE discovery https://docs.nordicsemi.com/bundle/ncs-latest/page/nrf/samples/bluetooth/nrf_dm/README.html
13. Wearable Devices for Physical Monitoring of Heart: A Review https://www.mdpi.com/2079-6374/12/5/292
14. Silicon to Software ICNETS2 2017 https://ieeexplore.ieee.org/iel7/8053864/8067882/08067883.pdf
15. Arxiv今日论文 | 2025-11-19 http://lonepatient.top/2025/11/19/arxiv_papers_2025-11-19
16. A Gaussian Process-Based Funnel MPC for Docking ... https://www.mdpi.com/2504-446X/9/12/836
17. FRANK MORALES - Boeing Associate Technical Fellow at ... https://www.thinkers360.com/tl/profiles/view/25153
18. Safe Reinforcement Learning for Automated Vehicles via ... https://ieeexplore.ieee.org/iel7/7274857/11023975/10365337.pdf
19. Safe Reinforcement Learning for Automated Vehicles via ... https://ieeexplore.ieee.org/iel7/7274857/7448921/10365337.pdf
20. Ethical, legal, and policy challenges in field-based ... https://pmc.ncbi.nlm.nih.gov/articles/PMC11157461/
21. Mind-reading in AI and neurotechnology: evaluating claims ... https://link.springer.com/article/10.1007/s43681-024-00514-6
22. (PDF) NEUROLAW-Legal Impacts of Neurotechnology https://www.researchgate.net/publication/390237085_NEUROLAW-Legal_Impacts_of_Neurotechnology
23. Connecting the dots in trustworthy Artificial Intelligence ... https://www.sciencedirect.com/science/article/pii/S1566253523002129
24. The ethical and legal landscape of brain data governance https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0273473&type=printable
25. Regulating the Mind: Neuromarketing, Neural Data and ... https://www.mdpi.com/2076-3387/15/10/386
26. Exposing, Reversing, and Inheriting Crimes as Traumas ... https://www.tandfonline.com/doi/full/10.1080/0731129X.2024.2376444

27. Assessment of flight fatigue using heart rate variability and ... https://pmc.ncbi.nlm.nih.gov/articles/PMC12263958/
28. A Multimodal Feature Fusion Brain Fatigue Recognition ... https://www.mdpi.com/1424-8220/24/9/2910
29. Estimation of Heart Rate Variability Parameters by Machine ... https://www.frontiersin.org/journals/cardiovascular-medicine/articles/10.3389/fcvm.2022.893374/full
30. Cross-Modal Computational Model of Brain-Heart ... https://arxiv.org/html/2601.06792v1
31. VeriLLM: A Lightweight Framework for Publicly Verifiable ... https://arxiv.org/html/2509.24257v4
32. Answers to Review Questions https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119480280.app
33. Exploring the roles of large language models in reshaping ... https://www.sciencedirect.com/science/article/pii/S3050860625000031
34. Embodied AI: Emerging Risks and Opportunities for Policy ... https://arxiv.org/html/2509.00117v1
35. (PDF) Automated Information Transformation for ... https://www.researchgate.net/publication/276077610_Automated_Information_Transformation_for_Automated_Regulatory_Compliance_Checking_in_Construction
36. ETHICALLY ALIGNED DESIGN http://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf
37. Lessons Learned So Far From Verifying the Rust Standard ... https://arxiv.org/html/2510.01072v1
38. Neuroethics and Neurorights - PMC - NIH https://pmc.ncbi.nlm.nih.gov/articles/PMC12688770/
39. Human Brain Project Specific Grant Agreement 3 | HBP SGA3 https://cordis.europa.eu/project/id/945539/results
40. (PDF) The Impact of Artificial Intelligence on Human Thought https://www.researchgate.net/publication/394942120_The_Impact_of_Artificial_Intelligence_on_Human_Thought
41. The effects of personalisation and privacy assurance on ... https://www.researchgate.net/publication/241086451_Personalisation-privacy_paradox_The_effects_of_personalisation_and_privacy_assurance_on_customer_responses_to_travel_Web_sites
42. (PDF) Human vs. Artificial Intelligence https://www.researchgate.net/publication/369218895_Human_vs_Artificial_Intelligence

43. Security hardening | Red Hat Enterprise Linux | 9 https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html-single/security_hardening/index

44. curl: (60) SSL certificate problem: unable to get local issuer ... https://stackoverflow.com/questions/24611640/curl-60-ssl-certificate-problem-unable-to-get-local-issuer-certificate

45. Red Hat Enterprise Linux 9 Security hardening https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/pdf/security_hardening/Red_Hat_Enterprise_Linux-9-Security_hardening-en-US.pdf

46. How Open Source Projects are Using Kani to Write Better ... https://aws.amazon.com/blogs/opensource/how-open-source-projects-are-using-kani-to-write-better-software-in-rust/

47. Red Hat Enterprise Linux 9 9.7 Release Notes https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/pdf/9.7_release_notes/%3Ctba%3E

48. 2012 Index Proceedings of the IEEE Vol. 98–100 https://ieeexplore.ieee.org/iel5/5/6351844/06353118.pdf

49. glove.6B.100d.txt-vocab.txt https://worksheets.codalab.org/rest/bundles/0xadf98bb30a99476ab56ebff3e462d4fa/contents/blob/glove.6B.100d.txt-vocab.txt

50. 333333 23135851162 the 13151942776 of 12997637966 ftp://ftp.cs.princeton.edu/pub/cs226/autocomplete/words-333333.txt

51. Operational Research: Methods and Applications https://www.researchgate.net/profile/Bo-Chen-74/publication/369557413_Operational_Research_Methods_and_Applications/links/64eb1b56434d3f628c506728/Operational-Research-Methods-and-Applications.pdf

52. 10.0 Release Notes | Red Hat Enterprise Linux | 10 https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/10/html-single/10.0_release_notes/index

53. 2016 IEEE Region 10 Conference (TENCON) https://ieeexplore.ieee.org/iel7/7838019/7847944/07847945.pdf

54. Findings of the Association for Computational Linguistics https://aclanthology.org/volumes/2025.findings-acl/

55. Findings of the Association for Computational Linguistics https://aclanthology.org/2025.findings-acl.0.pdf

56. MIT Projects | PDF | Electric Motor | Amplifier https://www.scribd.com/document/800262649/MIT-Projects

57. 259 - AVIONICS, AEROSPACE AND DEFENSE ... https://de.scribd.com/document/142763797/259-AVIONICS-AEROSPACE-AND-DEFENSE-ACRONYMS-AND-ABBREVIATIONS-Januar-2011

58. A strategy for mapping biophysical to abstract neuronal ... https://pmc.ncbi.nlm.nih.gov/articles/PMC8389851/

59. Red Hat Enterprise Linux 10 10.0 Release Notes https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/10/pdf/10.0_release_notes/index
60. On Neurorights - PMC https://pmc.ncbi.nlm.nih.gov/articles/PMC8498568/
61. 'Neurorights' https://resolve.cambridge.org/core/services/aop-cambridge-core/content/view/AF85DE57D51D114E26C19146E234F897/9781009207867c24_412-426.pdf/neurorights.pdf
62. (PDF) Neurorights, Mental Privacy, and Mind Reading https://www.researchgate.net/publication/382079309_Neurorights_Mental_Privacy_and_Mind_Reading
63. time to discuss rights to mental privacy and integrity https://faviofarinella.weebly.com/uploads/8/7/8/2/878244/neurorights__time_to_discuss_rights_to_mental_privacy_and_integrity__1_.pdf
64. Mapping ethical and legal foundations of 'neurorights' https://arxiv.org/abs/2302.06281
65. Neurorights in the Constitution: from neurotechnology to ... https://pubmed.ncbi.nlm.nih.gov/39428886/
66. scrabble.txt https://www.cs.cmu.edu/~wlovas/15122-r11/lectures/old/24-tries/scrabble.txt
67. Vipul Vaibhaw - model-checking/kani: Kani Rust Verifier https://www.linkedin.com/posts/vipulvaibhaw_github-model-checkingkani-kani-rust-verifier-activity-7150474582498369536-vOL4
68. AMD SEV-SNP Attestation: Establishing Trust in Guests https://www.amd.com/content/dam/amd/en/documents/developer/lss-snp-attestation.pdf
69. Attestation of a Confidential VM based on AMD SEV-SNP https://learn.microsoft.com/en-us/answers/questions/715698/attestation-of-a-confidential-vm-based-on-amd-sev
70. Confidential Computing https://cdrdv2-public.intel.com/788399/Confidential%20Computing%20Partner%20Enablement%20Package.pdf
71. Confidential Computing Deployment Guide (Intel TDX & ... https://forums.developer.nvidia.com/t/confidential-computing-deployment-guide-intel-tdx-kvm-attestation-execution-fails/322480
72. Beyond Confidential: Establishing Trust in Your Computing ... https://security.googlecloudcommunity.com/community-blog-42/beyond-confidential-establishing-trust-in-your-computing-environment-6290
73. RulePlanner https://arxiv.org/pdf/2601.22476
74. RulePlanner: All-in-One Reinforcement Learner for ... https://arxiv.org/html/2601.22476v1

75. Towards a Multidimensional Analysis of the National ... https://ieeexplore.ieee.org/ielaam/6287639/10005208/10233875-aam.pdf
76. A Neuroscience-inspired Framework for Embodied Agents https://arxiv.org/html/2505.07634v1
77. A Survey of Scientific Large Language Models: From Data ... https://arxiv.org/html/2508.21148v1
78. Computation and Language May 2025 https://www.arxiv.org/list/cs.CL/2025-05?skip=1675&show=1000
79. Computer Vision and Pattern Recognition May 2025 https://www.arxiv.org/list/cs.CV/2025-05?skip=200&show=2000
80. Computer Science May 2025 https://www.arxiv.org/list/cs/2025-05?skip=6625&show=2000
81. DCTS 2024 Conference Proceedings https://ieeexplore.ieee.org/iel8/10939042/10939076/10939944.pdf
82. Thursday sessions https://ieeexplore.ieee.org/iel5/6129459/6142695/06143155.pdf
83. https://www.researchgate.net/file.PostFileLoader.h... https://www.researchgate.net/file.PostFileLoader.html?id=563869346143256c208b45ba&assetKey=AS:291613667545089@1446537524905
84. TPM attestation overview for Azure https://learn.microsoft.com/en-us/azure/attestation/tpm-attestation-concepts
85. Modal Logical Neural Networks https://www.arxiv.org/pdf/2512.03491
86. Achieving Scalable Robot Autonomy via neurosymbolic ... https://arxiv.org/html/2505.08492v1
87. Neuro-Symbolic Frameworks: Conceptual Characterization ... https://arxiv.org/html/2509.07122v1
88. A Neuro-Symbolic Natural Language Navigational Planner https://arxiv.org/html/2409.06859v1
89. Learning Minimal NAP Specifications for Neural Network ... https://arxiv.org/html/2404.04662v1
90. A Neuro-Symbolic Natural Language Navigational Planner https://arxiv.org/pdf/2409.06859
91. A Reason-Based Neuro-Symbolic Architecture for Safe and ... https://arxiv.org/pdf/2601.10520
92. The Synergy of Symbolic and Connectionist AI in LLM- ... https://arxiv.org/pdf/2407.08516

93. A Neuro-Symbolic Framework for Embodied Task Planning https://arxiv.org/pdf/2510.21302
94. a)-(b) Fidelity test and SWAP test for Quantum Kernel ... https://www.researchgate.net/figure/a-b-Fidelity-test-and-SWAP-test-for-Quantum-Kernel-Estimation-where-U-is-the-feature_fig1_370468787
95. How to Raise a Robot — A Case for Neuro-Symbolic AI in ... https://arxiv.org/pdf/2312.08820
96. Quantum Kernel Methods under Scrutiny: A Benchmarking ... https://arxiv.org/abs/2409.04406
97. Quantum fidelity kernel with a trapped-ion simulation platform https://arxiv.org/html/2311.18719v2
98. A Cross-Testbed Validation on NISQ Processors https://www.researchgate.net/publication/400126957_Hardware-Agnostic_Quantum_Kernel_Feature_Mapping_for_Anomaly_Detection_in_Critical_Infrastructure_A_Cross-Testbed_Validation_on_NISQ_Processors
99. Variational Quantum Kernels with Task-Specific ... https://arxiv.org/pdf/2211.05225
100. (PDF) Quantum kernels for real-world predictions based on ... https://www.researchgate.net/publication/357014080_Quantum_kernels_for_real-world_predictions_based_on_electronic_health_records
101. arXiv:2311.08990v2 [quant-ph] 19 Apr 2024 https://arxiv.org/pdf/2311.08990
102. (PDF) Neurorights - Minding the Integrity of Mind https://www.researchgate.net/publication/388916800_Neurorights_-_Minding_the_Integrity_of_Mind
103. Mapping Ethical and Legal Foundations of 'Neurorights' https://pubmed.ncbi.nlm.nih.gov/37183686/
104. AutoDSL: Automated domain-specific language design for ... https://aclanthology.org/2024.acl-long.659.pdf
105. Formally understanding Rust's ownership and borrowing ... https://dl.acm.org/doi/10.1007/s10703-024-00460-3
106. Modular Formal Verification of Rust Programs with Unsafe ... https://www.semanticscholar.org/paper/4e533cf6a7a5c2975cdc0d4e58d7c389380f23a3
107. HRV and EEG correlates of well-being using ultra-short ... https://pubmed.ncbi.nlm.nih.gov/39097360/
108. Neural Decoding of the Speech Envelope https://pmc.ncbi.nlm.nih.gov/articles/PMC11345737/
109. On the speech envelope in the cortical tracking of speech https://pubmed.ncbi.nlm.nih.gov/38885886/

110. Phase Property of Envelope-Tracking EEG Response Is ... https://pmc.ncbi.nlm.nih.gov/articles/PMC10420405/
111. Decoding of speech acoustics from EEG https://pubmed.ncbi.nlm.nih.gov/41558175/
112. Comparing the Potential of MEG and EEG to Uncover Brain ... https://pubmed.ncbi.nlm.nih.gov/30205208/
113. Decoding of the speech envelope from EEG using ... https://pmc.ncbi.nlm.nih.gov/articles/PMC9842721/
114. General Auditory and Speech-Specific Contributions to ... https://pmc.ncbi.nlm.nih.gov/articles/PMC9581567/
115. Creusot: A Foundry for the Deductive Verification of Rust ... https://www.researchgate.net/publication/364287862_Creusot_A_Foundry_for_the_Deductive_Verification_of_Rust_Programs
116. Simultaneous real-time EEG-fMRI neurofeedback https://pmc.ncbi.nlm.nih.gov/articles/PMC10102573/
117. Novel Methodological Tools for Behavioral Interventions https://pmc.ncbi.nlm.nih.gov/articles/PMC8197468/
118. Z-score neurofeedback, heart rate variability biofeedback, and ... https://pmc.ncbi.nlm.nih.gov/articles/PMC7990441/
119. Neurofeedback Training Based on Motor Imagery Strategies ... https://pmc.ncbi.nlm.nih.gov/articles/PMC8700498/
120. Integrated use of biofeedback and neurofeedback techniques ... https://pmc.ncbi.nlm.nih.gov/articles/PMC10985214/
121. Plastic modulation of PTSD resting-state networks by EEG ... https://pmc.ncbi.nlm.nih.gov/articles/PMC4442612/
122. A Pilot Study of Its Potential for Sleep Induction in Older Adults https://pmc.ncbi.nlm.nih.gov/articles/PMC4534306/
123. Surveying the Rust Verification Landscape https://arxiv.org/html/2410.01981v1