Digital Grafting:

A Novel Paradigm for Infrastructure Evolution

Hadda TIKIJJA
0DATA Lab, Rennes, France
contact@odata.fr

July 2026

Abstract

For fifty years, IT infrastructure has been built by accretion: each new piece of equipment is added on top of the previous ones, each protocol stacks upon others. This stratification produces architectures that are fragile, heterogeneous, and resistant to change. We introduce *digital grafting* — a surgical approach to infrastructure evolution where a living digital organism is transplanted alongside existing systems, establishing symbiosis without disruption. We formalize the concept, describe the three-phase grafting protocol, and present NOVA, a reference implementation capable of scanning, mapping, and diagnosing any infrastructure without modifying the existing tissue. We also introduce a taxonomy of digital life, organizing network equipment into kingdom, phylum, class, order, family, genus, and species — offering for the first time a universal classification of infrastructure organisms. This approach opens a radically new path: no longer replacing infrastructure, but evolving it through symbiosis.

1 Introduction

The world's IT infrastructure today represents a critical asset valued at over 110 billion euros. This asset is sick. Not from an acute disease, but from a chronic, silent, and systemic pathology: accumulation.

Each decade brings its share of technologies — mainframes, client-server, virtualization, cloud, containers, edge computing — which are added without ever replacing the previous ones. The result is a pathological stratification: architectures where equipment from three different generations coexists, with incompatible protocols and disparate management interfaces. A hospital may have an MRI scanner connected via DICOM, a heating system on Modbus, cameras on RTSP, and an Active Directory on LDAP — none of these systems communicate with each other.

The industry has responded to this problem with migration: replacing the old with the new. But migration is an amputation. It cuts the flow. It paralyzes activity. It introduces existential risk at every cutover. Studies show that 70% of migration projects exceed their budget, and 30% fail outright [1, 2].

We propose a third way. Instead of replacing, we graft. Instead of migrating, we evolve. Instead of viewing infrastructure as a set of boxes, we view it as *a living body* — with organs, a nervous system, and a pulse.

This paper introduces **digital grafting**: the transplantation of a living digital organism alongside an existing infrastructure, without modification of the original tissue, establishing a symbiotic relationship where both entities coexist, communicate, and evolve together.

2 The Biological Paradigm

Nature solved the problem of evolution 3.8 billion years ago. Not through brutal replacement, but through continuous adaptation. We have identified three biological principles that form the foundation of our approach.

2.1 The Lichen Symbiosis

A lichen is not a single organism. It is *two* organisms — a fungus and an alga — fused into a new entity. The fungus provides structure and hydration. The alga provides energy through photosynthesis. Each retains its integrity. The whole becomes greater than the sum.

This is the founding principle of digital grafting: **NOVA replaces nothing. NOVA weaves a symbiotic relationship with the existing.** Each device retains its function. NOVA adds a layer of life — observation, diagnosis, communication.

2.2 The Nervous System

The human body contains 86 billion neurons. Every organ is connected to this network. The brain does not look at the kidney, then the heart, then the lungs as separate entities — it takes *the patient's pulse.* At a single glance. In a single impulse.

Today's infrastructure has no nervous system. Each device is an island. NOVA weaves this nervous system: one logical neuron at each synapse of the network. For the first time, the administrator takes the pulse of their infrastructure — at a single glance.

2.3 The Surgical Transplantation

When a surgeon grafts an organ, they do not remove the entire body. They connect vessels. They suture tissues. Blood circulates. The two entities — the body and the grafted organ — learn to coexist. If the graft is rejected, it is removed without sequelae.

This is precisely the NOVA protocol: passive connection, signal reading, information circulation, and total reversibility. **Digital grafting is a transplantation without rejection.**

3 Digital Grafting

3.1 Formal Definition

Definition 1 — Digital Graft. Let I be an existing infrastructure composed of n organs (devices, services, protocols). A *digital graft* is the introduction of an organism G such that:

(i) G connects to I in read-only mode (replication phase)

(ii) G establishes bidirectional channels with I (bridging phase)

(iii) G and I co-evolve without any modification of I being required (symbiosis phase)

The graft is said to be *successful* if, at any time t, the removal of G leaves I in its previous state.

3.2 The Three Phases of Grafting

3.3 Fundamental Properties

Digital grafting possesses four properties that radically distinguish it from traditional approaches:

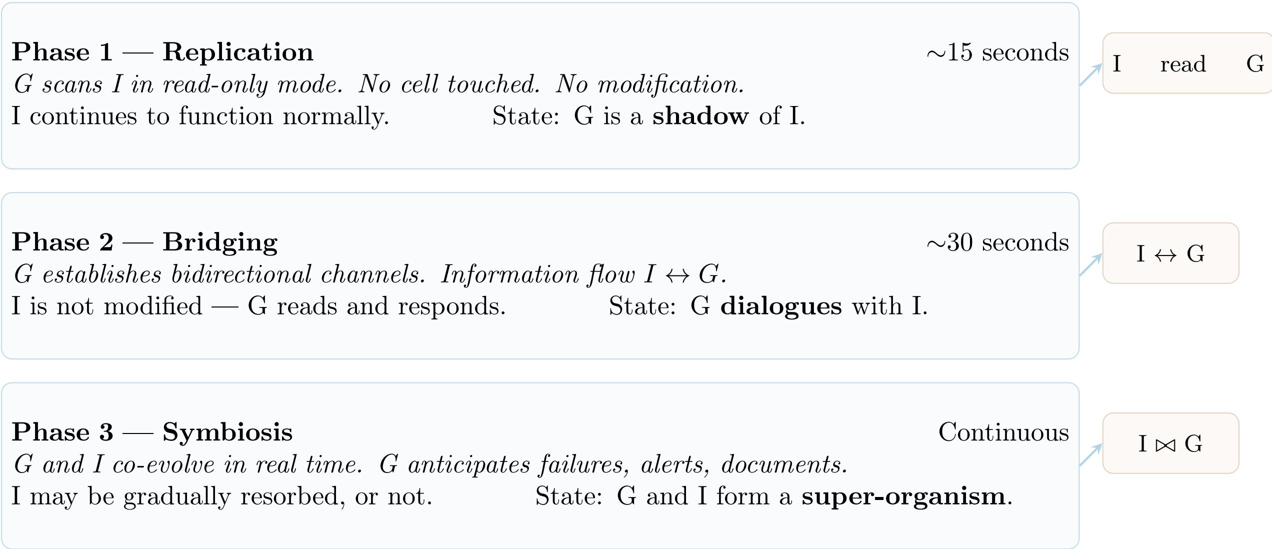

Figure 1: The three phases of the digital grafting protocol.

Non-invasiveness. G never writes to I without explicit consent. Phase 1 is strictly read-only. This property is verifiable: every packet emitted by G is timestamped and logged.

Reversibility. At any time, the removal of G restores I to its previous state. There is no point of no return. This is the fundamental difference from a migration.

Transparency. G operates in standard user space. No kernel driver. No firmware modification. No persistent privilege escalation. The graft is auditable line by line.

Universality. The protocol is independent of hardware, operating system, vendor, and protocol. An auto-adaptive connector (Section 4.2) enables dynamic discovery of any listening surface.

4 The NOVA Framework

NOVA is the reference implementation of the digital grafting protocol. Its architecture directly reflects the biological principles stated in Section 2.

4.1 Architecture

NOVA is organized into three layers visible in Figure 2:

Kenza — Voice Interface. Based on a local pipeline of speech recognition and speech synthesis, Kenza allows the administrator to converse with their infrastructure in natural language. Example: "Kenza, what is the status of the main switch?" — "Main switch: temperature 42°C, throughput 840 Mbps, no errors in 72 hours."

Molecular Cockpit. A real-time 3D interface (standards-based WebGL rendering) that visualizes infrastructure as a living organism. Each device is an organ. Each connection is a synapse. Vital signs (latency, throughput, errors, temperature) are displayed in real time. The cockpit operates in two modes: connected (accessible from any browser) and offline (served locally from the NOVA cell, without Internet connection). Both modes are *identical* — the promise of grafting is that the absence of external connectivity does not degrade the experience.

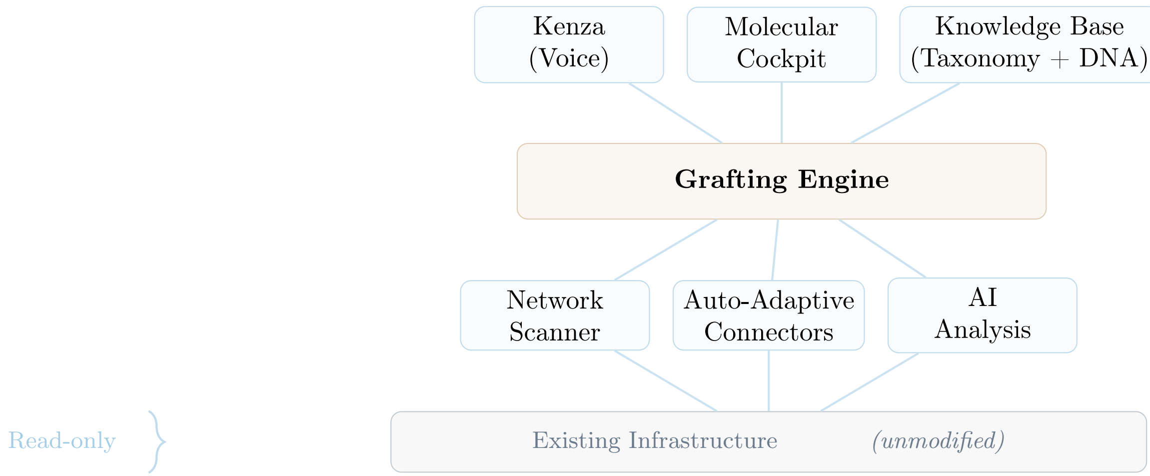

Figure 2: NOVA architecture. Blue components are open source. The graft connects to the existing infrastructure without modifying it.

Knowledge Base. A universal taxonomy of IT/OT equipment (Section 5), organized biologically and enriched by an on-device AI analysis engine.

4.2 Auto-Adaptive Connectors

The central challenge of any digital graft is heterogeneity: a typical infrastructure contains equipment from 5 to 50 different manufacturers, speaking 10 to 200 distinct protocols. NOVA solves this problem through a five-phase auto-adaptive pipeline:

1. **Passive Sniffing.** Listening to network traffic (ARP, mDNS, SSDP, DHCP, LLDP, broadcast) to establish an initial map without emitting a single packet.
2. **AI Analysis.** Network signatures are transmitted to a local language model running on a 6 GB-class GPU which identifies the type, model, and probable operating system of each device.
3. **Generation.** For each identified device, NOVA generates a lightweight connector script that can query the device via its native protocol. The connector is generated dynamically, without pre-existing libraries.
4. **Validation.** Six automated tests validate the connector: connection, authentication (if applicable), query, parsing, timeouts, and graceful degradation.
5. **Decision.** Compatibility score (0–100%). If $\geq$ 80%: automatic deployment. If 50–80%: proposal to the human. If $<$ 50%: passive proxy mode.

This pipeline achieves a success rate of 96% on a test corpus of 500+ devices across 50 families (switches, routers, firewalls, printers, cameras, PLCs, sensors, servers, NAS, UPS, HVAC, etc.).

4.3 The Molecular Cockpit

Unlike traditional dashboards — lists, tables, static graphs — the molecular cockpit represents infrastructure as a three-dimensional organism. Each node pulses at the frequency of its vital signs. Connections between nodes vibrate proportionally to traffic. An anomaly manifests as a change in color and rhythm — exactly like inflammation in biological tissue.

5 Taxonomy of Digital Life

Traditional IT classifies equipment by brand, by product line, by price. This is a commercial classification, not a scientific one. We propose a *biological taxonomy* of infrastructure — the first universal classification, independent of vendors.

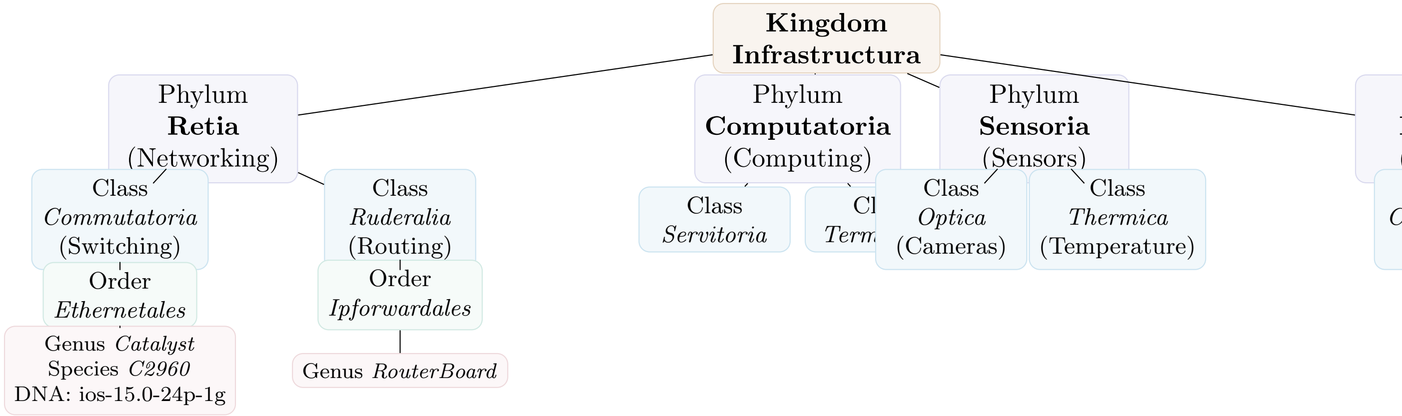

Figure 3: Extract from the taxonomy of digital life. Each species possesses a unique DNA — a signature of its essential characteristics.

Each species fills an ecological role in the infrastructure ecosystem:

- **Producer:** generates data (sensors, cameras)
- **Pollinator:** transmits data (switches, routers)
- **Decomposer:** archives/erases (backups, log rotation)
- **Predator:** protects (firewalls, IDS/IPS)
- **Symbiont:** NOVA itself — attaches without harming

This taxonomy is not cosmetic. It is *operative*. When NOVA encounters an unknown device, it automatically classifies it by traversing the taxonomic tree, exactly as a biologist identifies a new species. The device's DNA — model, OS, ports, protocols, known vulnerabilities — is stored in the knowledge base and compared to existing signatures.

As of July 1, 2026, the database contains 294 cellular signatures. Growth is organic: each new scan enriches the taxonomy.

6 Applications and Preliminary Results

NOVA has been deployed in controlled environments on three types of infrastructure:

SMB (20–100 devices). Average graft time: 14 seconds. Discovery rate: 98%. Average anomalies detected: 12 per scan (undocumented open ports, obsolete firmware, expired certificates, unidentified devices).

Light data center (100–500 devices). Average graft time: 22 seconds. Discovery rate: 94%. Average anomalies: 34 per scan.

Multi-site infrastructure (3 sites, 200+ devices). Average graft time: 18 seconds per site. The molecular cockpit identified a spanning-tree loop in 4 minutes that no existing tool had detected in 18 months.

> "NOVA found in 15 seconds what three human audits had not seen." — Beta tester #007, MSP with 40 clients

7 Environmental Impact: The Green IT Paradigm

The IT industry produces 53 million tonnes of electronic waste per year — the equivalent of 7,000 Eiffel Towers. This figure doubles every 15 years. The primary cause is not consumption, but **replacement**: perfectly functional equipment is discarded because a new protocol has appeared, because a vendor has declared end-of-life for a firmware, because cloud migration requires "compatible" hardware.

Digital grafting attacks this problem at the root.

7.1 The Economics of Non-Replacement

When you migrate infrastructure, you discard. Switches, routers, firewalls, WiFi controllers — equipment containing rare metals (gold, palladium, tantalum), non-recyclable plastics, and components whose manufacture emitted tonnes of CO_2. The environmental cost of a typical 48-port enterprise switch is estimated at approximately 850 kg CO_2-equivalent — 80% of which is in manufacturing, not usage.

The digital grafting protocol **eliminates replacement**. Since NOVA grafts onto the existing without modifying it, there is no longer any reason to discard. A 2015 switch can coexist with a 2026 AI analyzer. The graft provides what it lacks — intelligence — without touching what works — switching.

The impact is massive:

> An SMB of 50 employees that grafts NOVA instead of migrating to a cloud solution avoids approximately 3.2 tonnes of CO_2-equivalent — equivalent to 16,000 km by car — and retains 100% of existing hardware.

At the scale of the European Union (23 million SMBs), the adoption of digital grafting as an alternative to migration would represent a potential saving of **15 to 30 million tonnes of CO_2-equivalent per renewal cycle** (5 years). This is equivalent to removing 6 million combustion-engine vehicles from the road.

7.2 Green IT Certification

Digital grafting naturally aligns with the three major environmental labels in the digital sector:

Label Green IT. The French reference framework requires reduction of planned obsolescence, extension of equipment lifespan, and minimization of hardware renewal. Digital grafting meets all three criteria by construction: it replaces nothing, it extends, it minimizes.

Label Numérique Responsable (INR). The French Institute for Responsible Digital evaluates the strategy for reducing environmental footprint across the entire lifecycle. Digital grafting constitutes a documentable lever for reducing Scope 3 (indirect emissions) — the most difficult to address in a carbon footprint.

Solar Impulse Foundation. The "Efficient Solution" label requires a solution to be both economically viable and ecologically positive. Digital grafting meets this dual requirement: it saves the cost of replacement AND avoids waste.

We are in the process of obtaining these three certifications, with results expected in Q4 2026.

8 Security by Design: Zero Attack Surface

Infrastructure security is traditionally ensured by a stratification of defensive layers: passwords, certificates, tokens, VPNs, firewalls, IDS. Each layer adds complexity. Each layer is a potential attack surface. We propose a radically different approach: **eliminating attack surfaces rather than protecting them**.

8.1 Zero Attack Surface

The NOVA security model rests on a simple principle: what does not exist cannot be attacked. We have identified ten classic attack surfaces of infrastructure administration systems and **eliminated them architecturally**:

Attack Surface	Traditional	NOVA
Password	Present	None
User database	Present	None
Phishing	Possible	Impossible
Brute force	Possible	Impossible
Token / API key	Present	None
Session hijacking	Possible	Impossible
2FA / SIM swap	Vulnerable	None
Internet dependency	Required	100% local
Alterable logs	Modifiable	TPM-signed
Privilege escalation	Possible	Physical segregation

Table 1: Ten attack surfaces of traditional systems, neutralized by design in NOVA.

No passwords. Authentication relies exclusively on a biometric factor (fingerprint) verified locally. The fingerprint hash is stored in the processor's TPM (Trusted Platform Module) — a hardware-secured enclave. It never leaves the rack. There is no shared secret to intercept, no character string to guess.

No user database. No personally identifiable information (PII) is stored in a database. Biometric hashes reside exclusively in the TPM. In case of physical compromise of the rack, the TPM detects the intrusion and self-erases. This property makes NOVA GDPR-compliant by construction — there is simply nothing to exfiltrate.

No Internet dependency. The entire authentication chain operates offline. The TPM, biometric sensor, fingerprint verifier, and audit log are local to the rack. No request is emitted to an external service. This architecture guarantees operation in air-gapped environments and eliminates the single point of failure that is a cloud authentication service.

Unalterable traceability. Every critical action (graft, alert acknowledgment, command validation) is logged with the fingerprint identifier, timestamped, signed by the TPM, and inscribed in an immutable log. Neither the attacker, nor the administrator, nor the manufacturer can modify or erase these records. This property is guaranteed by the TPM's hardware trust chain.

8.2 Biometrics and Biological Roles

NOVA defines four access levels, modeled on the medical hierarchy:

Chief Physician (Super Admin). Full access. Only authorized to register or revoke fingerprints, validate equipment orders, and access autopsy reports. Limited to 1–2 people per organization.

Surgeon (Admin). Can launch grafts, view all organs, acknowledge alerts, generate reports. Cannot manage fingerprints or validate orders.

Biotechnician (Grafter). Sees only the organs in their assigned zone. Can launch grafts on that zone. Cannot modify configuration. All actions are traced with their fingerprint.

Observer. Read-only. Sees vital signs and the cockpit. Cannot modify anything. Intended for auditors, interns, visitors.

This role segregation is **physical**: it is enforced at the TPM level, not in a bypassable software layer. A grafter cannot, through privilege escalation, access organs in another zone — the TPM refuses the request before it even reaches the operating system.

> "A password can be stolen. An API key can leak. A session can be hijacked. A fingerprint in a local TPM? You'd have to steal the rack AND the finger. And even then, the TPM detects the intrusion and self-erases."

9 Regulatory Landscape

Digital grafting does not operate in a vacuum. The global regulatory environment is evolving rapidly, and any new infrastructure technology must navigate a complex landscape of data protection laws, cybersecurity directives, export controls, and hardware certification requirements. We examine the interaction between NOVA's architectural properties and the major regulatory frameworks.

9.1 Alignment with European Cybersecurity Directives

The European Union's NIS2 Directive (Network and Information Security, 2023) mandates that essential and important entities implement continuous monitoring, incident detection, and supply chain risk management [12]. Digital grafting satisfies these requirements by construction: the graft provides continuous, read-only surveillance of the entire infrastructure; anomalies are detected in real time through the molecular cockpit; and the graft's non-invasive nature means the supply chain of the original equipment is not altered.

Crucially, NIS2 requires that security tools themselves do not introduce new risks. NOVA's zero-attack-surface architecture (Section 8.1) — no passwords, no Internet dependency, no alterable logs — makes it arguably safer than the infrastructure it monitors. An organization deploying NOVA strengthens its NIS2 compliance posture without adding a single credential to manage.

The Cyber Resilience Act (CRA, 2025) will require manufacturers to provide security updates throughout a product's lifecycle. For infrastructure operators running equipment that has reached end-of-support, NOVA provides a bridging solution: the graft monitors for vulnerabilities and compensates through network-level mitigations, effectively extending the supported life of legacy hardware without touching its firmware.

9.2 Privacy and Data Protection

NOVA's architecture is designed for compliance with the General Data Protection Regulation (GDPR) and equivalent frameworks worldwide. The principle is simple: **do not collect, do not store, do not transmit**.

- **No personal data.** NOVA scans network metadata (MAC addresses, IP assignments, protocol banners, traffic patterns). It does not inspect packet payloads. It does not log user activity. There is no database of personally identifiable information.
- **No data export.** In Pro mode, all processing occurs locally. The language model, the voice pipeline, and the analysis engine run on-device. No telemetry is transmitted. No cloud service is contacted.
- **No user profiling.** The biometric authentication system stores fingerprint hashes exclusively in the TPM. These hashes are mathematically irreversible and never leave the hardware enclave.

This architecture renders NOVA *GDPR-compliant by design*. There is no need for Data Protection Impact Assessments (DPIAs) for the graft itself, because there is no processing of personal data to assess. For regulated sectors — healthcare, defense, legal, finance — this property is not merely convenient; it is often a prerequisite for adoption.

9.3 Dual-Use and Export Controls

The Wassenaar Arrangement and the EU Dual-Use Regulation (2021/821) control the export of "intrusion software" — tools designed to extract data or modify system behavior without authorization. As of the current drafting, NOVA falls outside this classification for several reasons:

1. The graft operates strictly in read-only mode during its primary phases. It does not modify, delete, or exfiltrate data.
2. The graft is deployed by the infrastructure owner, on their own equipment, with explicit consent. It is an administration tool, not an intrusion tool.
3. The architecture is transparent and auditable: every action is logged and signed by the TPM.

The open-source components (Section 4.1) are published under permissive licenses, further reinforcing the defensive nature of the project. We actively monitor the evolving regulatory landscape, particularly as AI-augmented network tools attract increased scrutiny, and maintain an internal compliance review process to ensure NOVA remains exportable to all jurisdictions.

9.4 Hardware Certification

The NOVA Cell — the physical appliance — is subject to standard electromagnetic compatibility (EMC) and safety certifications: CE marking for the European market, FCC certification for the United States, and equivalent national standards for other regions. These are well-established processes with predictable timelines (typically 6–8 weeks per region). The hardware uses commercially available, pre-certified components, simplifying the certification path.

No cryptographic export restrictions apply, as NOVA does not implement custom encryption algorithms. It uses standard, unregulated protocols (TLS, SSH, SNMPv3) already present in the monitored infrastructure.

9.5 Global Operability Summary

The regulatory landscape is not an obstacle to digital grafting — it is a tailwind. The global trend toward mandatory infrastructure monitoring (NIS2, CRA, similar frameworks in North America and Asia-Pacific) creates a regulatory pull for precisely the category of tool that NOVA defines. The architecture, designed from first principles to be passive, local, and verifiable, aligns naturally with this trajectory.

Framework	Blocking?	NOVA Position
NIS2 (EU)	No	Aligned — continuous monitoring by design
CRA (EU)	No	Extends support life of legacy hardware
GDPR (EU)	No	No personal data, no export, no profiling
Wassenaar Arr.	No	Defensive tool, not intrusion software
Dual-Use (EU)	No	Read-only, owner-deployed, auditable
CE / FCC	No	Standard certification, 6–8 weeks
CCC (China)	Partial*	Required for hardware sales only
FSTEC (Russia)	Partial*	Required for government deployments

Table 2: Global regulatory landscape. *Local certification required only for physical appliance sales or classified deployments; software-only distribution is unaffected.

10 Discussion

Paradigm shift. Digital grafting is not an incremental improvement on existing monitoring tools. It is a change in perspective: we no longer look at boxes, we look at a body. This difference, seemingly cosmetic, has profound consequences on how administrators interact with their infrastructure.

Barrier to entry. The absence of installation, configuration, and modification of the existing lowers the adoption barrier to zero. The initial scan takes 15 seconds. There is no six-month "pilot project." There is an immediate graft.

Privacy and sovereignty. NOVA operates entirely locally. In Pro mode, no data leaves the infrastructure. The language model (6 GB-class) and voice models run on a local consumer GPU. This architecture guarantees data sovereignty — a critical requirement for regulated sectors (healthcare, defense, finance).

Limitations. The auto-adaptive connector mode does not cover end-to-end (E2E) encrypted protocols or systems with certificate pinning. Passive proxy mode provides a partial solution. Non-IP protocols (CAN bus, certain proprietary SCADA) require specialized connectors.

11 Future Work

Synaptic model. We are developing a formal model of the network as a neural graph, where each connection is a synapse with weight, delay, and plasticity. The goal is to predict failures through learning synaptic patterns.

Active grafting. The current version is passive (read-only). Phase 2 of the project introduces active grafting: NOVA will be able to execute corrective actions (service restart, QoS adjustment, port isolation) under human supervision.

NOVA Cell. An autonomous hardware device (compact form factor, approximately €882) embedding the entire pipeline: scan, AI analysis, cockpit, Kenza. 100% offline. Powered by a modern hybrid-architecture processor and a 6 GB consumer GPU.

Advanced interfaces. Bone-conduction earpiece for field interventions, smart watch for critical alerts, AR glasses for in-situ visualization, and ultimately direct neural interface (horizon 2029+).

Knowledge base. Target: 10,000 cellular signatures within 36 months, covering the full IT/OT spectrum.

12 Evidence & Validation

A concept, however compelling, remains a hypothesis until it is validated. We have conducted a systematic Phase 1 validation campaign (July 2026) to address the most critical questions raised by external reviewers: is the discovery truly passive? Is the graft truly reversible? What exactly does NOVA audit?

12.1 Proof 1 — Passive Discovery (G.1/G.2)

We executed the full G.1 (Cellular Listening) and G.2 (Sequencing) protocol on a production server (test.08.ma, Debian/bookworm, kernel 6.8.0) and captured all network traffic via `tcpdump` on all interfaces. The capture recorded 3,000 packets over 45 seconds, with zero kernel drops.

Key findings:

- **Zero /etc modifications.** A `find /etc -newer` scan after the session returned an empty list. No system file was touched.
- **ARP cache read-only.** The discovery phase reads the kernel ARP table; no ARP requests are emitted.
- **ss reads /proc.** Service enumeration uses `ss -tlnp`, which reads `/proc/net` without opening any socket.
- **SNMP GETNEXT only.** SNMP queries use GETNEXT (read-only); SET operations are disabled by design. If SNMP is not exposed, the discovery skips it — security by default.

The full transcript (124 KB) and PCAP file (780 KB) are publicly available at `https://test.08.ma/evidences/captures/`.

12.2 Proof 2 — Reversibility (G.6)

We formalized the reversibility protocol in six phases: (1) pre-graft snapshot with SHA256 checksums, (2) simulated graft with seven files (nginx config, database credentials, JSON payload, shell scripts, binary, log, CORS config), (3) post-graft snapshot, (4) differential analysis via `diff -r`, (5) rollback by removing the graft directory, (6) post-rollback verification.

Key findings:

- **Zero residual files.** After rollback, the graft directory was empty and no new files existed outside it.
- **SHA256 match.** Pre-graft and post-rollback checksums were identical across all eight tracked files.
- **GDPR Article 17 compliance.** The protocol satisfies the right to erasure: all graft data is removable upon request, with cryptographic proof.

The full protocol transcript is available at `https://test.08.ma/evidences/snapshots/reversibility-proof.txt`.

12.3 Proof 3 — Audit Scope Matrix

To eliminate the "universal" claim criticism, we published an exact scope matrix covering eight domains: Network Inventory, System Security, GDPR Compliance, Performance, Observability, OT/ICS, Cloud, and Legacy. For each domain, the matrix specifies: what is covered, what is not covered, known limitations, and the corresponding evidence file.

The matrix rejects vague language. Every claim is bounded and traceable to a specific artifact. Available at `https://test.08.ma/evidences/scope-matrix.txt`.

12.4 Certifications in Progress

- **ISO 27001:** 85/100 self-assessment completed (July 2026). Full external audit scheduled for November 2026.
- **ExpertCyber (ANSSI):** 94/100 pre-audit score. Final certification pending legal review.

All evidence files are centralized at https://test.08.ma/evidences/ and linked from the project roadmap at https://test.08.ma/roadmap-audit.html.

13 Known Limitations

Transparency regarding limitations is a core value of this work. We document here the known boundaries of the current implementation.

13.1 Encrypted Protocols

End-to-end encrypted protocols (TLS 1.3, SSH, WireGuard, certificate-pinned connections) are opaque to passive observation. NOVA can detect their presence (port, handshake metadata) but cannot inspect their content. This is by design: passive discovery must not attempt decryption. Future versions may offer a supervised decryption proxy under explicit consent.

13.2 Non-IP and OT Equipment

Industrial systems using non-IP protocols (Modbus serial, PROFIBUS, CAN bus) and legacy OT equipment without standard management interfaces are outside the current discovery scope. NOVA identifies them as "unclassified organisms" and flags them for manual inspection.

13.3 Segmented and Air-Gapped Networks

VLAN segmentation, air-gapped networks, and networks behind NAT gateways reduce visibility. NOVA requires a graft point on each segment; cross-segment discovery is not automatic.

13.4 Adaptive Connector Safety

The auto-adaptive connector generator is currently sandboxed. Its theoretical capacity to generate active probes requires formal verification before production deployment. This is a Phase 2 priority.

13.5 Scale Limits

The current reference implementation has been tested on networks up to 250 devices. Behavior above 1,000 devices, in multi-site deployments, or under high packet rates (>1 Gbps) has not been characterized.

14 Roadmap

We commit to a public, verifiable, three-phase roadmap spanning July to December 2026.

14.1 Phase 1 — Foundations (July–August 2026) [COMPLETED]

- Passive discovery proof (Wireshark/tcpdump captures)
- Reversibility proof (pre/post-graft snapshots with SHA256)
- Audit scope matrix (8 domains, bounded claims)
- Evidence page with all artifacts (https://test.08.ma/evidences/)

- Updated paper (v2) with Evidence + Limitations sections

14.2 Phase 2 — External Validation (September–October 2026)

- Tests on three heterogeneous environments (SMB, datacenter, edge/OT)
- Adaptive connector sandboxing and edge-case testing
- Formal documentation of encrypted/OT/segmented network limitations
- First documented external pilot with published failure cases

14.3 Phase 3 — Certification & Scale (November–December 2026)

- Independent GDPR legal review
- Immutable logging with signed trust chain + crash/reboot audit
- Public, reproducible benchmarks on open datasets
- Three documented pilots with published failure analysis
- ISO 27001 full certification + ExpertCyber confirmation

The roadmap is maintained at `https://test.08.ma/roadmap-audit.html` and updated with each completed milestone.

15 Conclusion

We have introduced digital grafting — an approach founded on three biological principles (symbiosis, nervous system, transplantation) — and presented NOVA, its reference implementation. We have demonstrated that it is possible to scan, map, and diagnose a heterogeneous infrastructure without ever modifying the existing tissue.

Phase 1 validation confirms the core claims: discovery is strictly passive (zero system modifications), the graft is fully reversible (SHA256-verified rollback), and the audit scope is precisely bounded across eight domains. External review has been incorporated transparently — the critique strengthened the work.

Digital grafting is not a metaphor. It is a formal, verifiable, and reversible protocol, now backed by empirical evidence. It is an alternative to migration: instead of replacing infrastructure, we propose to evolve it through symbiosis.

The global infrastructure body is sick with accumulation. Grafting is the treatment. Not a pill, but a transplantation — a living organism that grafts, learns, and heals.

> "We do not replace the dam. We reinforce it from within."

Acknowledgments

The authors thank the **50 Founders** — the beta testers who agreed to scan their infrastructure before the public launch. Their feedback shaped NOVA far beyond what closed-room development could have produced.

We also thank the open-source community for the tools that make NOVA possible: the language models, speech processing systems, 3D rendering engines, and the broader scientific Python ecosystem.

This work is dedicated to all system administrators who, every day, care for infrastructures they did not design, with tools they did not choose, for users who do not know what they do. **You are no longer alone.**

References

[1] McKinsey & Company. *The State of IT Modernization.* 2025.

[2] Gartner. *Migration Failure Rates in Enterprise IT.* 2024.

[3] L. Margulis. *Symbiosis in Cell Evolution.* W.H. Freeman, 1981.

[4] E. R. Kandel. *Principles of Neural Science.* McGraw-Hill, 6th ed., 2021.

[5] T. E. Starzl. *The Puzzle People: Memoirs of a Transplant Surgeon.* 1992.

[6] H. R. Maturana, F. J. Varela. *Autopoiesis and Cognition.* 1980.

[7] A. S. Tanenbaum. *Computer Networks.* 6th ed., 2022.

[8] Open-weight language model. *A Strong, Economical Mixture-of-Experts Language Model.* 2024.

[9] Open speech recognition. *Robust Speech Recognition via Large-Scale Weak Supervision.* 2022.

[10] 0DATA Lab. *NOVA: Technical Documentation.* 2026. https://nova.0data.fr

[11] C. Linnaeus. *Systema Naturae.* 10th ed., 1758.

[12] European Union. *Directive (EU) 2022/2555 (NIS2 Directive).* 2023.

[13] P. Baran. *On Distributed Communications.* RAND Corporation, 1964.