

AGELAIOS

The open source operating system that makes
coalition tactical equipment interoperable

Ten operators, half a day. Two battalions neutralised.

May 2025, Estonia. An allied exercise brings together more than sixteen thousand personnel from twelve nations. A team of about ten Ukrainian drone operators plays the opposing force. In half a day it is credited, within the simulation, with seventeen armoured vehicles and some thirty further strikes. Two battalions are assessed as neutralised.

The exercise did its job by exposing a weakness before it cost anything. It laid bare a stark gap between the doctrine and the decentralised communications the Ukrainians have to hand, and those of NATO. Our answer starts there.

SOURCE Exercise Hedgehog and Siil 2025, Estonia, May 2025. Strength and framework of the exercise published by the Estonian Defence Forces and by NATO. Outcome of the manoeuvre reported in the press from accounts by participants and Estonian officials.

What the field has taught us.

01

Dispersal is what secures survivability

A centralised command post is a target that can be found, characterised and struck. The function therefore spreads across dozens of mobile nodes: vehicles, drones, remote sensors and dismounted teams. **Each must stand alone, be operated by a non-specialist, and rejoin the fleet the moment the link returns.**

02

The spectrum is contested at all times

In the Baltic, jamming and spoofing of the satellite signal now disrupt even civil shipping and air traffic. At the front, a reference report put Ukrainian drone attrition at around ten thousand a month, mostly through electronic warfare. **A system that assumes the signal is there is not a combat system.**

03

Degraded mode is the default mode

Equipment that refuses to start because a signature has expired, a licence server cannot be reached or an update was interrupted gets left behind. In July 2025 a worldwide satellite outage cut Ukrainian units off for around two and a half hours. **Equipment must start, always, and degrade its posture explicitly rather than refuse service.**

04

Tactical and industrial cycles are pulling apart

A countermeasure now appears within two or three days, while requalification takes years. The most sought-after components carry lead times of tens of weeks and leave the market within a few years. An architecture tied to a proprietary stack or to one hardware family passes those risks straight to the programme. **Abstraction turns a change of target into an integration exercise rather than a full rewrite.**

In 2026 a credible tactical product has to operate decentralised in a contested spectrum, know when to fall silent, use generative AI within the measure and countermeasure cycle, change within weeks, stay manufacturable despite a contested supply chain, and interoperate natively in coalition. Our foundation makes those requirements operational from day one.

SOURCE GNSS interference in the Baltic Sea, measurement campaigns and public reports, 2024 and 2025. Estimated drone attrition, RUSI report, May 2023. Commercial satellite service outage, July 2025, public statements by the Ukrainian authorities. Published analyses of adaptation cycles in Ukraine, 2025 and 2026. Lead times and shortening component life cycles, public reports from the electronics sector, 2025 and 2026.

Changing faster calls for a standard system layer. Nobody sells it, everybody pays for it.

Europe is rich in high-level applications: tactical picture, command, sensors, autonomy, decision support. Beneath them, every player rewrites the same technical layer. Cryptography, key management, hardware drivers, resilient transport, exchange formats, updates, fleet management.

That layer is nobody's core business. It is paid for once per vendor, once per programme, then once again at every requalification. Interoperability, meanwhile, remains a work package negotiated after the fact, when it ought to be a property of the system.

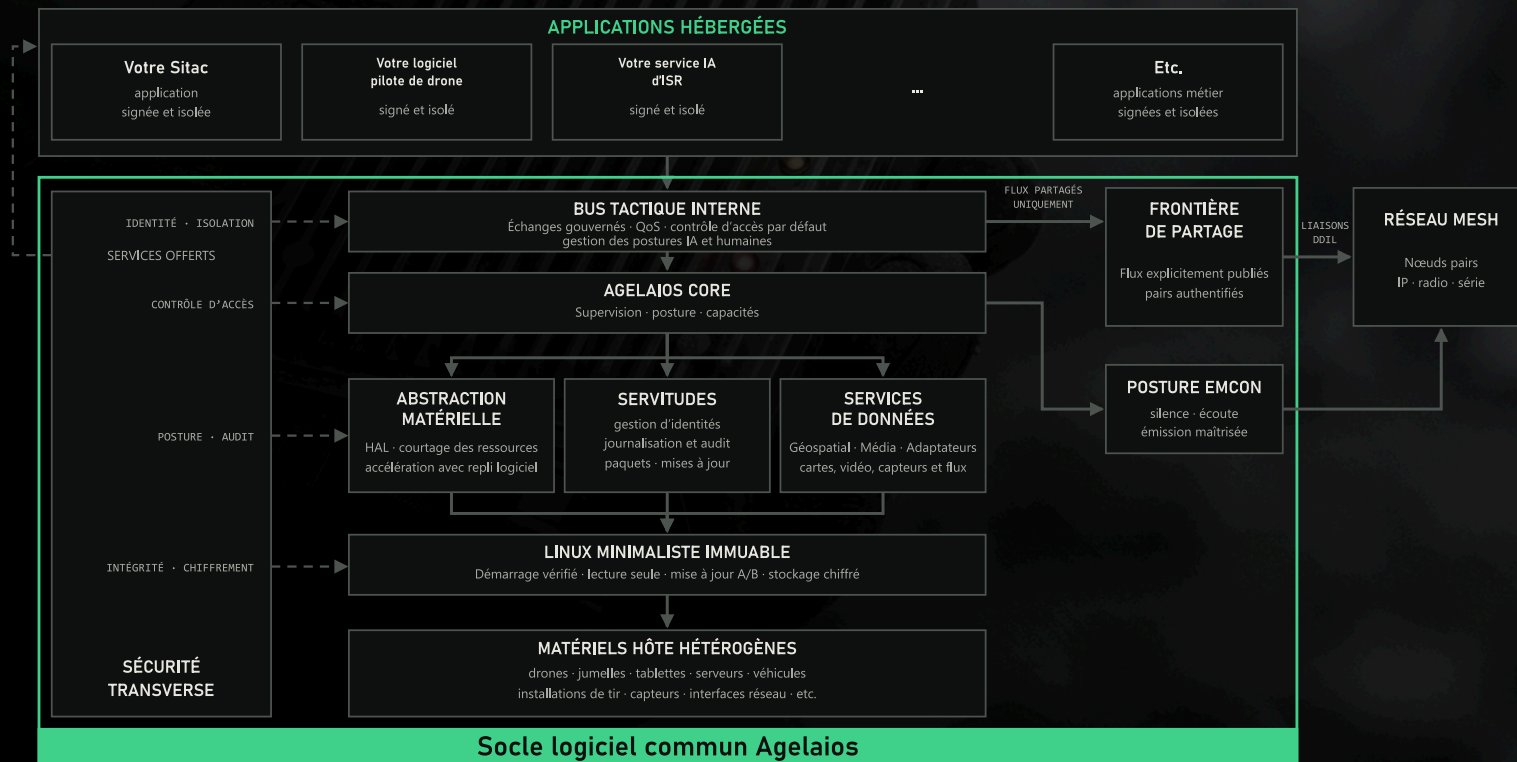
One technical layer.

**As many reimplementations as there are
players.**

One payer at the end of the chain.

An architecture that claims it will survive a real engagement in 2026 is judged by what it costs to change, not by how much it does.

The Ukrainians have Delta, the Americans have Lattice. We offer the European interoperability layer.



The basic functions every application ends up asking for are shipped as standard.

Video and transcoding

Common codecs, compliant real-time packetisation, controlled colorimetry and bit depths, industrial camera capture.

Tactical tracks

Standardised track model, life cycle, affiliation, correlation, fusion of heterogeneous sources.

Geography and terrain

Standard grids to ease voice reporting, elevation, line of sight and intervisibility, offline tiles, standard mapping services.

Sharing and coalition

Distribution of media streams and tactical tracks, coalition posture as standard, fleet key infrastructure.

Symbology

Standardised symbols and tactical graphics, imported and exported without proprietary conversion.

Time

Disciplined time sources, including where no satellite signal and no time server is available.

Civil sources

Air traffic, maritime traffic, position, alerts, fed in as neutral objects within the same picture.

Mesh network

Use of whatever physical layers are available, wired and radio alike, with emission control enforced at system level.

These are the functions teams rewrite from scratch every time. They are not the ones that win a contract.

Fourteen standards families, supported from August 2026

We provide reference implementations of the main applicable STANAGs and standards, available from first boot, with no development and no gateway.

01 - Geodesy and mapping

- WGS-84 (STANAG 2211)
- MGRS · UTM · GEOREF
- STANAG 3809 (DTED) · MIL-PRF-89020
- OGC WMTS (WebMercatorQuad)
- OGC API Features · WMS 1.3.0 · WFS 2.0.0
- GeoPackage (OGC 12-128r)
- OGC 3D Tiles · Cesium quantized-mesh 1.0
- STAC 1.0.0
- PMTiles v3 · MBTiles · MVT
- GDAL · PROJ

02 - Cryptography

- FIPS 204 (ML-DSA-65)
- FIPS 203 (ML-KEM) · X25519MLKEM768
- NSA CNSA 2.0
- FIPS 186-5 · RFC 8032 (Ed25519)
- FIPS 140-3 · CMVP
- FIPS 180-4 · 197 · 202
- BLAKE3
- TLS 1.3 (RFC 8446)
- RFC 9106 (Argon2)
- RFC 6238 (TOTP)

03 - System security and evaluation

- UEFI Secure Boot · TPM 2.0 (ISO/IEC 11889)
- fs-verity · IMA · dm-verity
- NIST SP 800-207 · SP 800-53
- Bell-LaPadula · Biba
- NIST SP 800-88 rev.1
- Common Criteria (ISO/IEC 15408 · 18045)
- CSPN (ANSSI)
- RGS (ANSSI)
- RFC 8785 (JSON Canonicalization)

04 - Key infrastructure and software supply chain

- X.509 (RFC 5280)
- The Update Framework (TUF)
- SPDX (ISO/IEC 5962) · CycloneDX
- SLSA · NIST SSDF (SP 800-218)
- NIST NVD / CVE

05 - Tactical tracks and intelligence

- STANAG 4676 (NATO ISR Tracking)
- STANAG 4607 (GMTI)
- STANAG 4545 (NSIF)
- STANAG 7023 (primary imagery)
- STANAG 4559 (NSILI)

06 - Video and media

- ITU-T H.264 · H.265 + RFC 6184 · 7798
- H.266/VVC (RFC 9328)
- STANAG 4609 · MISB ST 0601/0102 (KLV)
- ITU-R BT.601/709/2020/2100 · SMPTE P010/V210
- GiGE Vision · GenICam · PFNC
- OpenTelemetry · W3C Trace Context · Parquet

07 - Symbology and tactical graphics

- APP-6(D/E) (STANAG 2019)
- MIL-STD-2525C/D
- NVG (NATO Vector Graphics)

08 - C2 interoperability and messaging

- Cursor-on-Target · TAK Protocol v1
- STANAG 5525 (JC3IEDM / MIP)
- ADaP-3 · APP-11 (FORMETS)
- FMN · NATO NISP

09 - Civil sources and dual use

- GeoJSON (RFC 7946)
- NMEA-0183
- APRS (TNC2)
- ADS-B (dump1090 / readsb · OpenSky)
- AIS · AISStream.io
- GTFS-Realtime
- DATEX II
- TLE · SGP4 propagation
- USGS · GDACS · Global Fishing Watch

10 - Classification and coalition

- STANAG 4774 / ADaP-4774
- STANAG 4778 / ADaP-4778
- IGI 1300 (SGDSN)
- II 901 (SGDSN)

11 - Drones and effectors

- MAVLink
- STANAG 4586
- ONVIF (Profile S/T)

12 - Links and time

- QUIC (RFC 9000)
- JetStream · edge and full node
- STANAG 5066 (HF)
- ITU-R P.525 · P.526 · P.833
- Longley-Rice / ITM · two-ray
- NTP (RFC 5905) · NTS (RFC 8915) · PTP (IEEE 1588)

13 - Mission artificial intelligence

- NATO Principles of Responsible Use of AI (2021)
- Regulation (EU) 2024/1689 (AI Act)
- ISO/IEC 42001 · 23894 · TR 24028
- Opinions of the French Defence Ethics Committee

14 - Engineering, documentation and accessibility

- W3C WCAG 2.2 (level AA)
- W3C CSP Level 3
- WebAssembly · WASI
- BCP-47 · Unicode CLDR
- RG Aéro 000 40/42 · AQAP 2110/2210
- ISO/IEC/IEEE 12207 · 15288 · ISO/IEC 25010
- ASD S1000D (Issue 5.0)
- ISO/IEC 27001 · ISO 9001

Evidence, not intentions.

2800+

automated tests passing on the reference repository.

429

pages of illustrated user documentation to the ASD S1000D standard, kept consistent with the specifications and the code.

9

continuous integration chains, with bit-for-bit reproducible builds.

6 to 7

TRL maturity, demonstrated on emulators and on commercial equipment.

774

governing specifications framing the product.

Agelaios is built as an auditable foundation, specified and documented, ready to be taken on board quickly by any project or programme.

Two editions, one foundation.

Standard Edition

To be released as open source under the Apache 2.0 licence

- Operating system recipes and build chain.
- Stable application and binary interfaces.
- Development kit to create, manage and publish modules.
- x86-64 and ARM64 emulators.
- Starter kits for widely used computers.
- Message bus, network mesh and emission postures.
- Node discovery and fleet management on an open model.
- Commercial grade cryptography.
- Conventional verified boot and direct installation.
- Hardware abstraction layers and interface management.
- Interoperability protocols.
- Implementation documentation: port in a day, first module in an hour.

Same base, same interfaces, same standards. The team moves from the Standard Edition to the Program Edition as soon as the programme enters service.

The Program Edition is built on the Standard Edition, adding what entry into operational service demands in the way of industrial responsibilities.

Program Edition

The whole open core, plus the following

- Qualified and certified builds.
- Post-quantum cryptography in service, ML-DSA and ML-KEM.
- Emulators for specific platforms.
- Industrial grade verified and measured boot, A and B installation.
- Fleet key infrastructure and associated services.
- Identity federation and coalition to allied standards.
- Role based access control and full policies.
- Signed software bill of materials and full supply chain validation.
- Industrial provisioning and secret management.
- Long term support and in-service observability.
- Fleet management, store of certified applications and modules.
- Mission replay services.
- Inventory management.

Building the standard with the ecosystem.

A standard is worth only as much as the number of players using it. The core is open precisely so that anyone can try it, port it to their own hardware and judge for themselves whether it fits. All of that without prior agreement, without a non-disclosure agreement, without an appointment.



Certification programme

It is an offer, not a barrier. It guarantees that a device works with the foundation without prior integration work, on the model consumer markets have followed for years. A manufacturer certifies its hardware, a software house the compatibility of its product. The more certified equipment there is, the stronger the case for adopting the standard: the whole ecosystem gains.



Technical governance

It is open to our partners: a standard is built with those who use it. For the time being it stays held by a single directorate and by published rules. A standard decided by committee stops moving, and openness is worth having only if decisions continue to be taken.

Six people, one shared vision and a mix of backgrounds the defence industrial base rarely brings together.

Ruggedised hardware

We have designed munitions and computers for severe environments.



Programmes

We have run programmes inside the major prime contractors.



Public procurement

We know how to bid for French and European public contracts.



Generative AI

We command it everywhere it bites: from specification through to validation.

27 years

Senior adviser. Defence programmes and industrial transformation.

10 years

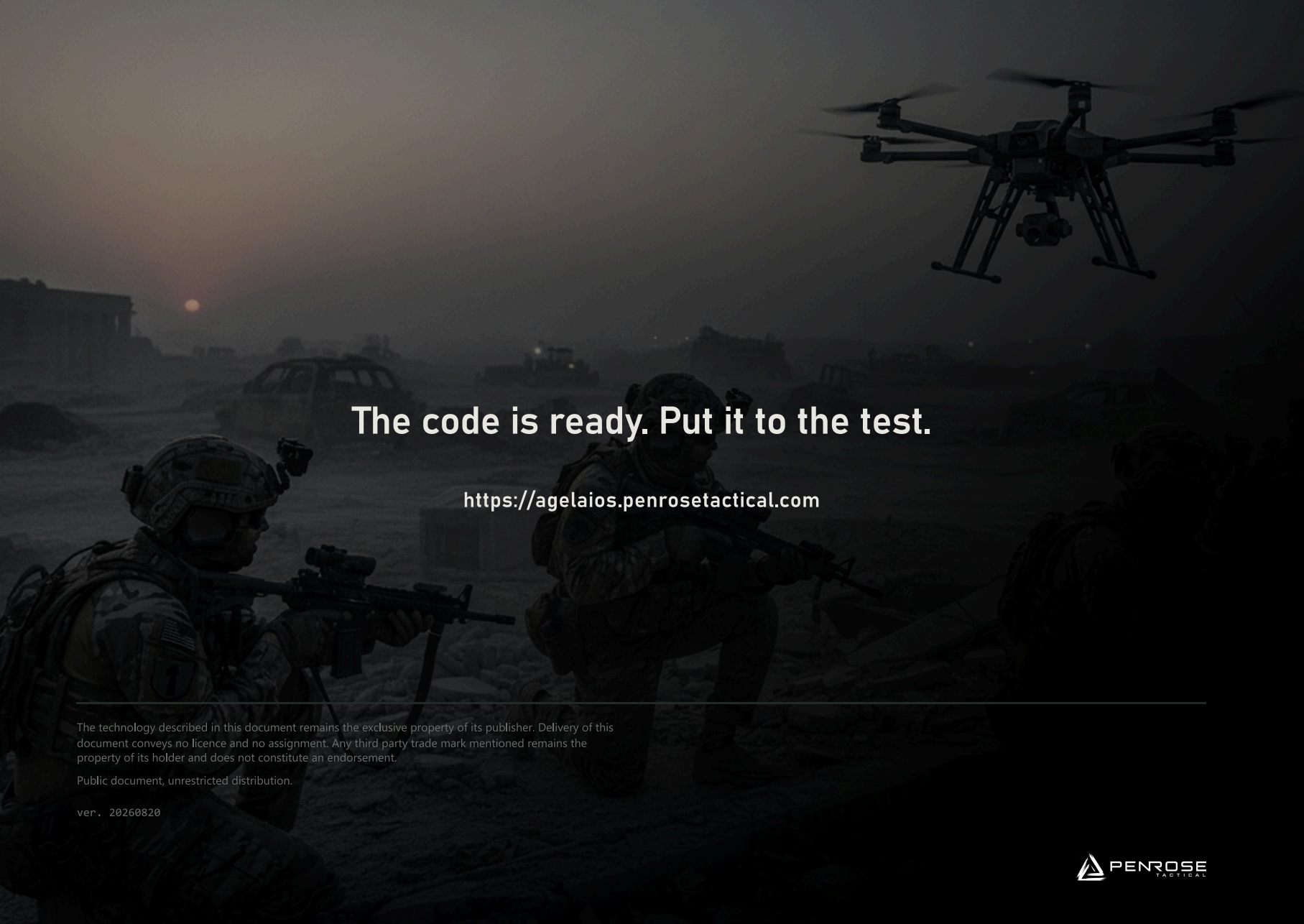
Programme direction. Product development under hard constraints.

Penrose Tactical

A multinational defence company, present in Europe and Asia-Pacific and based in France. We come from the defence industry and we are returning to it to serve, on the timetable the situation sets.

OUR MANIFESTO

Commanding generative AI within the development cycle cancels part of our competitors' financial and technological advantage. Sovereignty stops being a matter of budget and becomes a matter of method again. **Our ambition is to contribute to a European standard that is more open and more interoperable, coalition-ready by construction across every platform: drones, loitering munitions, vehicles, robots, dismounted soldiers, heavy platforms.**



The code is ready. Put it to the test.

<https://agelaios.penrosetactical.com>

The technology described in this document remains the exclusive property of its publisher. Delivery of this document conveys no licence and no assignment. Any third party trade mark mentioned remains the property of its holder and does not constitute an endorsement.

Public document, unrestricted distribution.

ver. 20260820