KRY10

OT Network Guard

Assured protection at every critical boundary

COMMERCIAL
IN CONFIDENCE



WHITEPAPER_SEP 2026

Security isn't a feature, it's *a foundation*



About Kry10

At Kry10, we strengthen the foundations beneath the critical systems that society depends on every day. We bring mathematical assurance to critical embedded and agentic systems, building resilience deep into the technology, right from the foundation.

We work with those responsible for critical systems. From the operators to architects to strategic leaders working across critical national infrastructure, healthcare, defense, telecommunications, transportation and more. All the people who can't afford to get it wrong.

Our focused and growing team across the USA, UK, Australia and New Zealand strengthens what matters for the critical systems society depends on every day.

Our foundations are mathematically proven. Because critical should mean certain.

©2026 KRY10
All rights reserved. Kry10 and associated names, logos, graphics, and product identifiers are trademarks or registered trademarks of Kry10. Any other trademarks referenced remain the property of their respective owners.

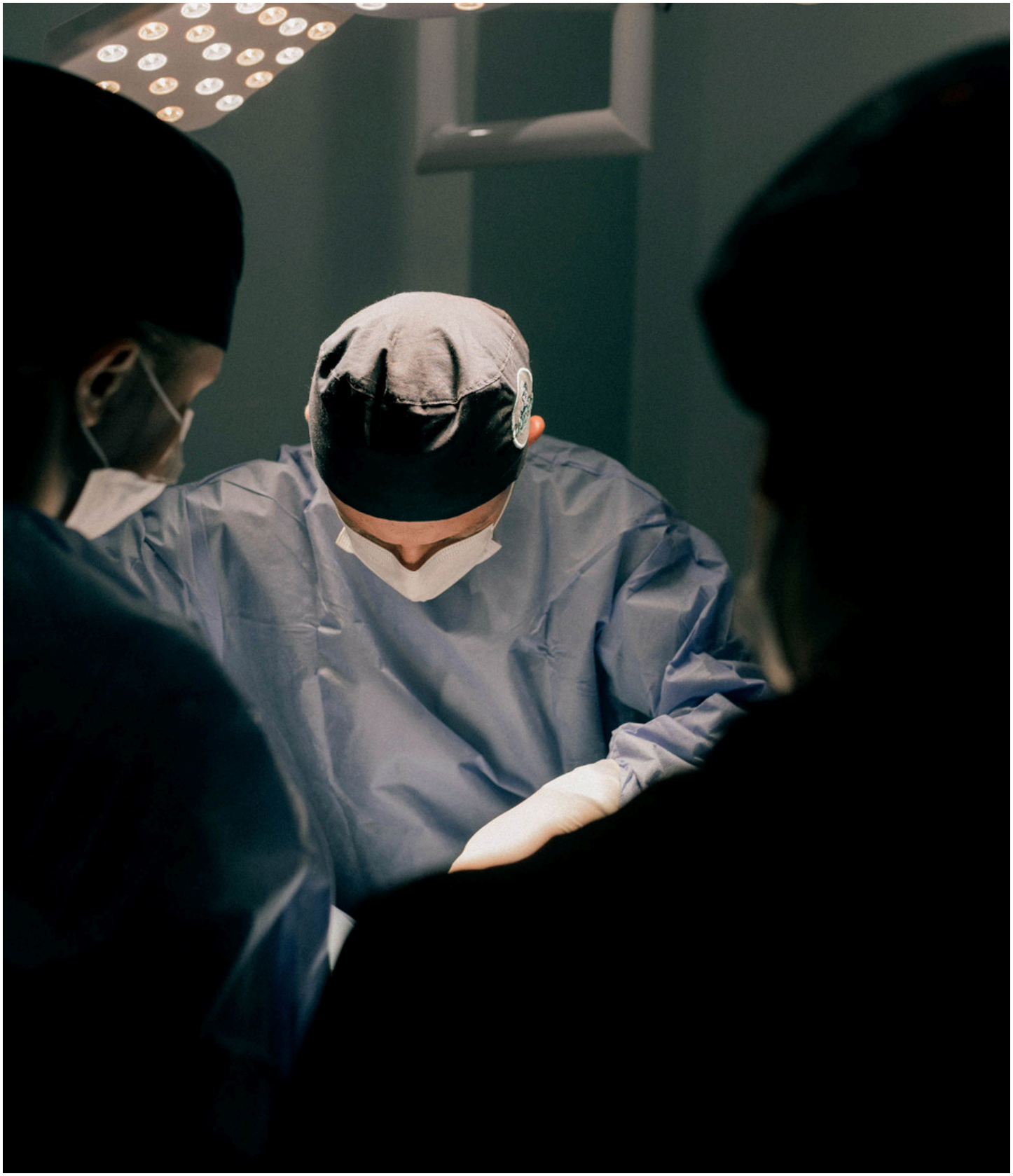


Critical infrastructure runs on equipment certified to do a job, not to defend itself against today's cyber threats.

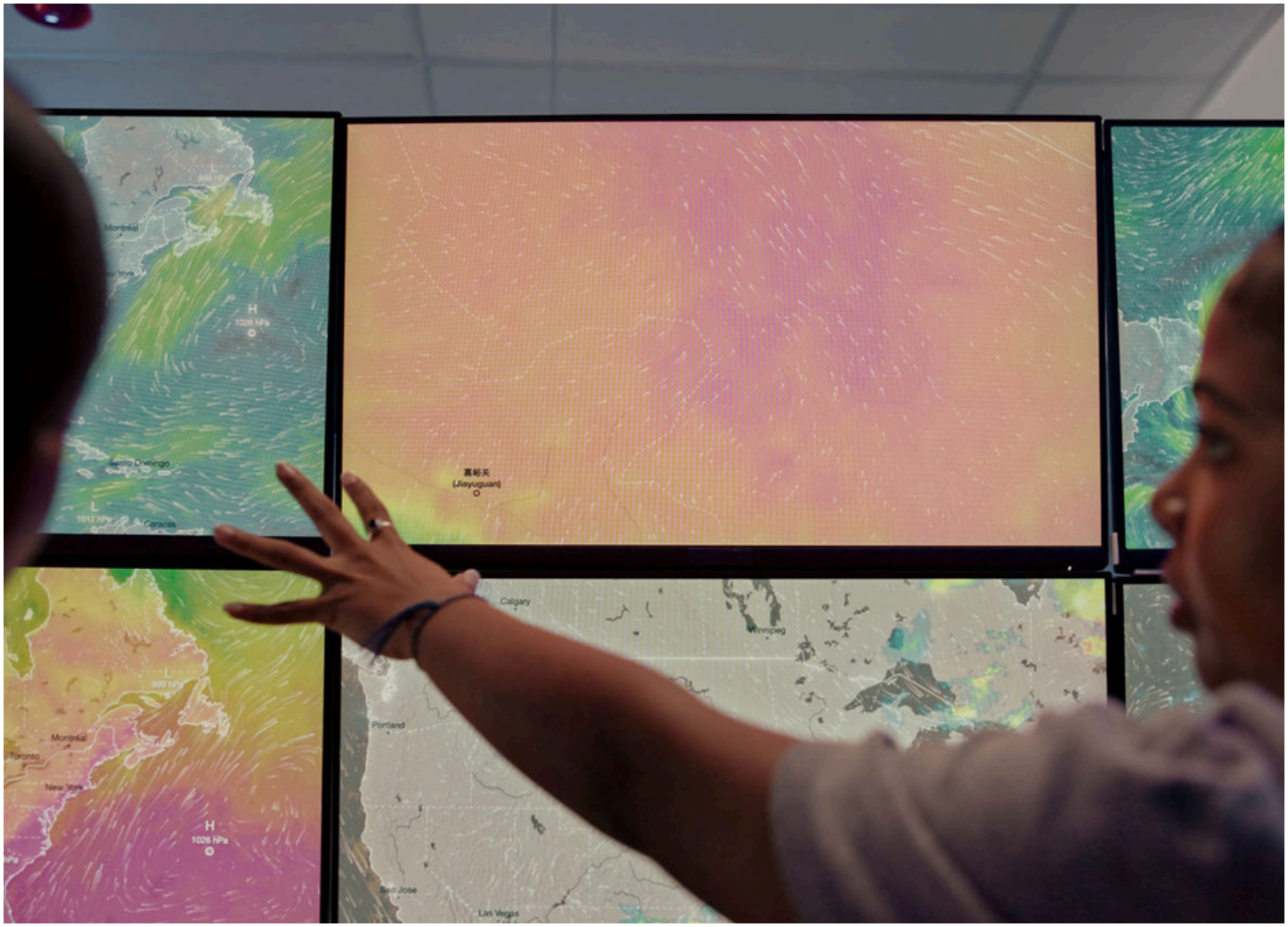
AI-assisted cyber offense has decisively changed the speed and sophistication of attacks. For operational technology, patching is not a scalable answer. Every change triggers costly recertification and justification of whether the risk of patching to an otherwise functional system is necessary.

Currently in pilot development, OT Network Guard is an appliance, built on a formally verified foundation, that sits inline between a trusted, safety-critical system and a lower-trust network. In critical systems, where the boundary between a trusted system and a low trust network cannot be allowed to fail, Network Guard determines and enforces what crosses the boundary.

Confidence is good, proof is better.



The constraints on Operational Technology



01 The threat landscape has changed

AI-assisted vulnerability discovery and threat actors such as Volt Typhoon have changed the offense-defense calculus in cybersecurity.

The growing AI cyber capability landscape means attackers can now find software flaws faster than defenders can respond.

For IT environments, AI-accelerated attacks create urgency. For operational technology, they create a structural crisis — one that faster detection and better patch programs (if there is one) cannot resolve.

02 The OT constraint is structural

Certified OT equipment carries the security posture of its software stack at the time of certification. The scope of what counts as a ‘modification’ is broad: software updates, firmware changes, configuration alterations.

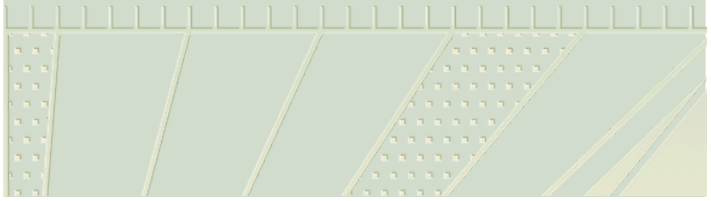
Recertification following any such change typically takes months, at significant cost. As a result, certified devices in field operations often carry vulnerabilities that cannot be addressed without triggering revalidation of the system.

The exposure trajectory is worsening as time passes. Smart factory programs, predictive maintenance, remote diagnostics, and supply-chain integration are all expanding the connectivity of OT systems with IT networks and external platforms. But legacy OT systems were never designed to connect to these networks and cannot now be hardened to defend against them.

In IT environments, a compromised system can be isolated and remediated. In OT, a malicious command reaching a controller can cause physical damage, environmental release, or personnel harm before any responder can act. Detection without protection leaves an unacceptable residual risk when the consequences are irreversible.

Revalidation challenge in the real world

CVE-2022-38465 (CVSS 9.3) exposed the cryptographic keys protecting an entire family of Siemens SIMATIC S7-1200/S7-1500 controllers. A firmware fix exists but applying it to safety-certified devices triggers revalidation, so much of the global installed base stays exploitable years later. Patched at source, unpatched in the field.



03 Where current approaches fall short

The regulatory constraints facing OT environments are demanding individually, and harder in combination. Any candidate solution must provide inline protection, require no device modification, address the availability of risk of an inline appliance, and be resistant to compromise. Most deployed approaches currently available can satisfy some of those constraints, but no existing solutions can satisfy them all.

TABLE ONE: COMMON APPROACHES TO OT THREAT PROTECTION

Common Approach	The Limitations
PATCHING / FIRMWARE UPDATE	Any change invalidates certification. Not viable without triggering revalidation effort. Financially unviable to recertify regularly.
TRAFFIC LOGGING ONLY	Sees attacks but cannot prevent them. Physical consequences within OT can occur before any responder can act.
CONVENTIONAL INLINE FIREWALLS / INTRUSION DETECTION SYSTEMS	Run on a general-purpose OS. A single root compromise gives full control of the packet processing stack. Increases the attack surface for persistence and lateral movement.
NETWORK SEGMENTATION ALONE	Reduces exposure but does not protect against protocol-level threats arriving through legitimate network paths.

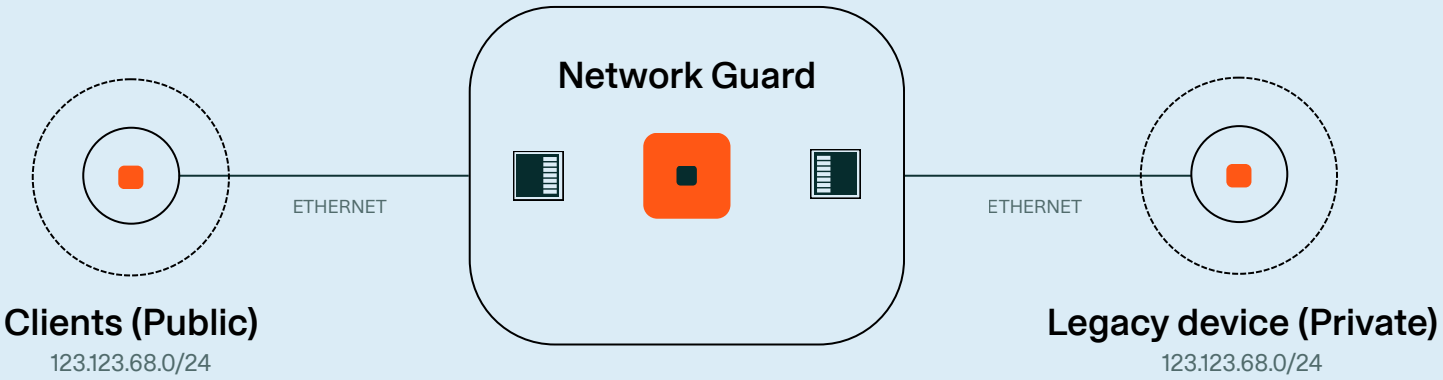


OT Network Guard

04 OT Network Guard: Fundamentals

Kry10's OT Network Guard is a physical inline appliance installed at the IT/OT boundary, where an untrusted network meets an OT device requiring protection. It requires no modification to the protected device at any stage: no firmware changes, no configuration alterations, and no network redesign.

FIGURE ONE:
STANDARD NETWORK GUARD ENVIRONMENT



Boundary inspection operates in both directions. Inbound traffic from the untrusted network must pass through all required phases (see page 10) before it can reach the OT device. Outbound traffic from the OT device is equally controlled. Commands and data leaving the protected system pass through equivalent inspection before they can reach the untrusted network.

OT Network Guard Inspection Phases

Every data packet passes through three inspection phases:

PHASE A	**Rules Based Validation**: Firewall rules, checksum verification, IP/portmatch.
PHASE B	**Formally Verified Protocol Parser**: Every packet's payload is validated against a formally verified parser, generated from the official protocol specification by EverParse (Microsoft Research's verified parser framework). Parser correctness is proven, not tested. There are no untested edge cases.
PHASE C	**Stateful Policy Compliance**: Message frequency, field value bounds, transaction pair matching against operator-defined operational policy.

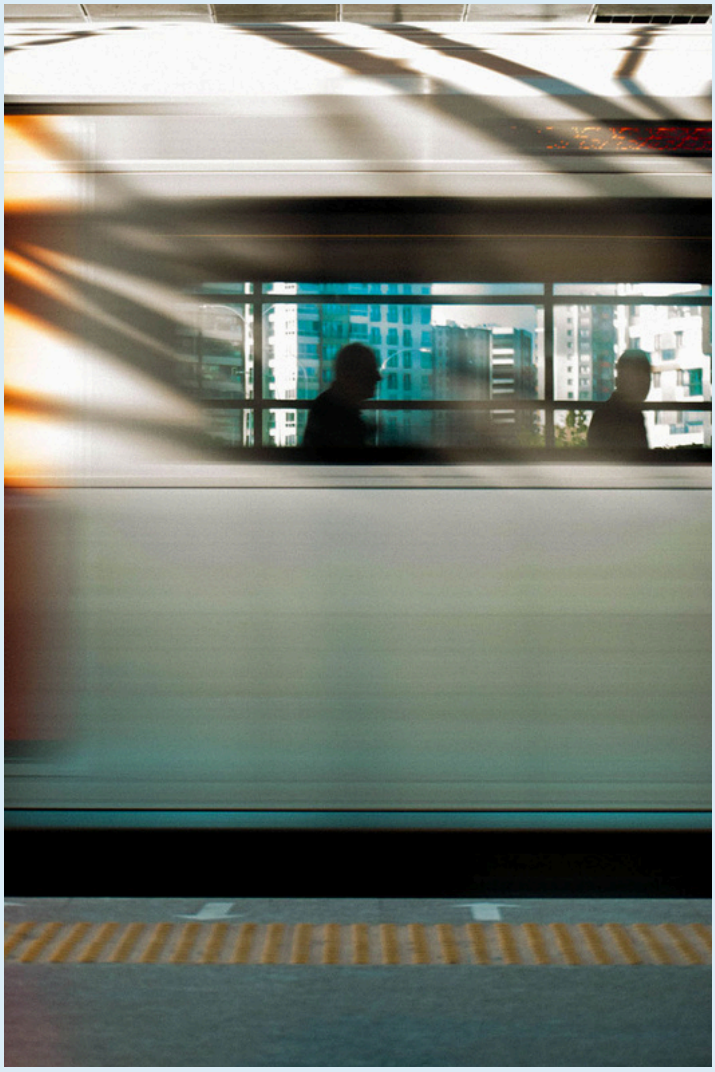
OT Network Guard's operating platform is KOS, built on seL4® — the only formally verified operating system kernel, whose isolation and security properties have been mathematically proven. Other application-specific OT firewalls run on general- purpose operating systems and inherit the associated attack surface. A vulnerability in the underlying OS can undermine and disable any protection entirely. KOS's formally verified isolation prevents faults from crossing component boundaries.

No opportunity to exploit with OT Network Guard

A malformed packet crafted to exploit an edge case in an OT asset's firmware finds no such opportunity. With active filtering and three complementary classes of deep packet inspection including a formally verified protocol parser, the protected device never sees it.



05 OT Network Guard: Benefits



01 Resilience investment

Even without an active threat actor, an unplanned outage is costly. OT Network Guard adds logging, deep packet inspection, and secure remote support outside the certification boundary. Increasing visibility of system health, speeding recovery, and reducing the remediation and downtime costs that a degraded device incurs. The unprotected device itself is the availability risk; the guard is what you invest in to manage it.

02 Become a harder target

Certification takes time. Once a vulnerability is known, an attacker can act immediately, but the operator will still need to re-certify. This leaves known vulnerabilities unmitigated in the field. Adversaries can count on it — state-sponsored pre-positioning like Volt Typhoon targets exactly this type of unpatched OT. Firewalls built on general-purpose operating systems inherit the same flaws attackers already exploit. KOS (seL4) and formally verified parsers reject malformed packets by mathematical proof, not by chance.

03 Buy time against an evolving threat

Patching cannot keep pace with exploit development, and AI is accelerating it. Formal verification is the forward step: the parser is proven correct against the official specification across every possible input: not inferred from testing. It holds against the vulnerabilities no one has discovered yet.

06 Sector-based threat protection challenges

These challenges appear across multiple sectors:

TABLE TWO: SECTOR-BASED THREAT PROTECTION CHALLENGES

Sector	Application
INDUSTRIAL OT / SCADA	Protection for unpatched PLC and SCADA systems in energy, utilities (including water and wastewater services), resource extraction, telecommunications and manufacturing processes.
MEDICAL DEVICES, SYSTEMS AND EQUIPMENT	Formally verified packet inspection for network-connected medical devices in clinical environments.
AVIONICS SYSTEMS	Protection for maintenance systems connecting to untrusted networks on the ground.
TRANSPORTATION	Deep packet inspection for signaling systems, operating under safety certifications and enforcing policy compliance.
DEFENSE PLATFORMS	Protection for defense platforms against targeted AI-assisted exploitation.



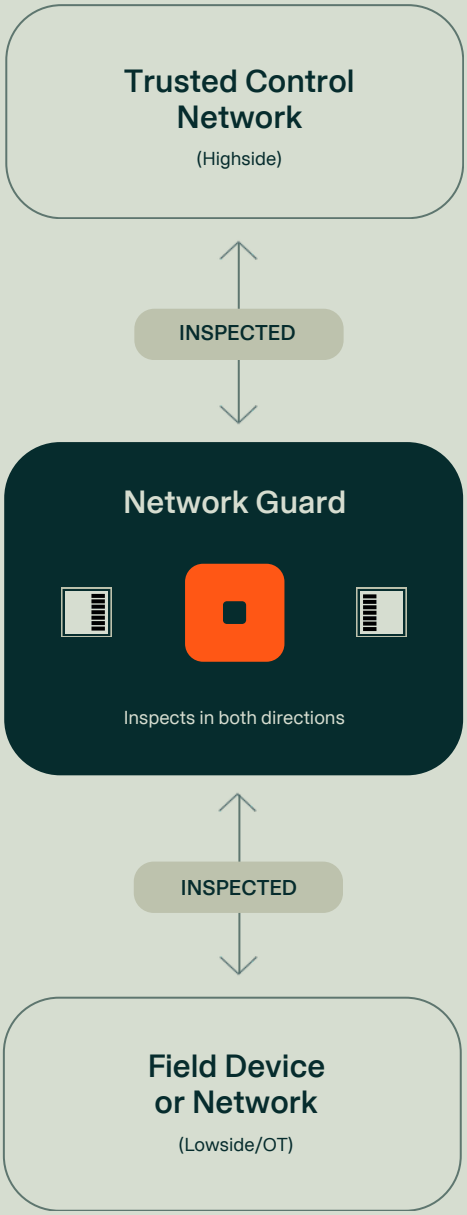
07 Network Guard Configurations

Network Guard comes in a base configuration (Configuration 1, page 14). Capability options governing how traffic and data moves between the two sides can be layered on top in various configurations, depending on client requirements.

Configuration 1: Base Configuration

One Guard, bidirectional traffic, no diode

Every message between the two sides passes through the one Guard, in both directions, and is inspected before it is delivered. There is no physical barrier, bad traffic is prevented based on what the Guard chooses to allow or block.



NETWORK GUARD BUILDING BLOCKS

GUARD
The configurable inspection appliance

HIGH/LOW SIDE
The trusted side vs the potentially compromised side

SOFTWARE DIODE
A fully software enforced one-way data path

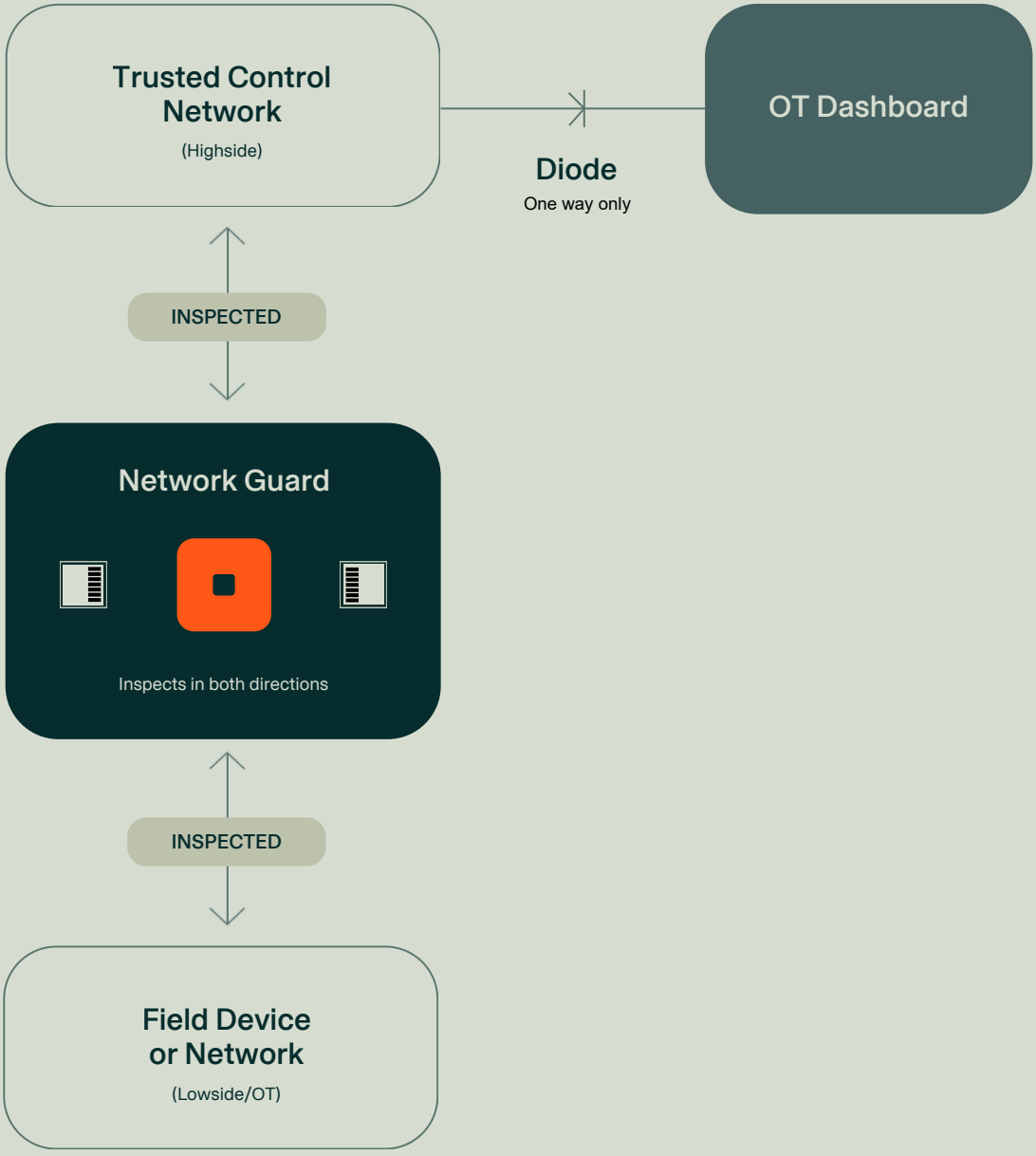


Beyond the base configuration, add additional observability and encryption options:

- **Configuration 2** adds a second, physically separate link to provide observability to your OT team. Not even a fully compromised OT device can send anything back through the data diode.
- **Configuration 3** adds a VPN to the same set-up, allowing encrypted remote access.

Configuration 2:
1+ Diode to OT

Data diode straight to OT is added, independent of the Guard



NETWORK GUARD BUILDING BLOCKS

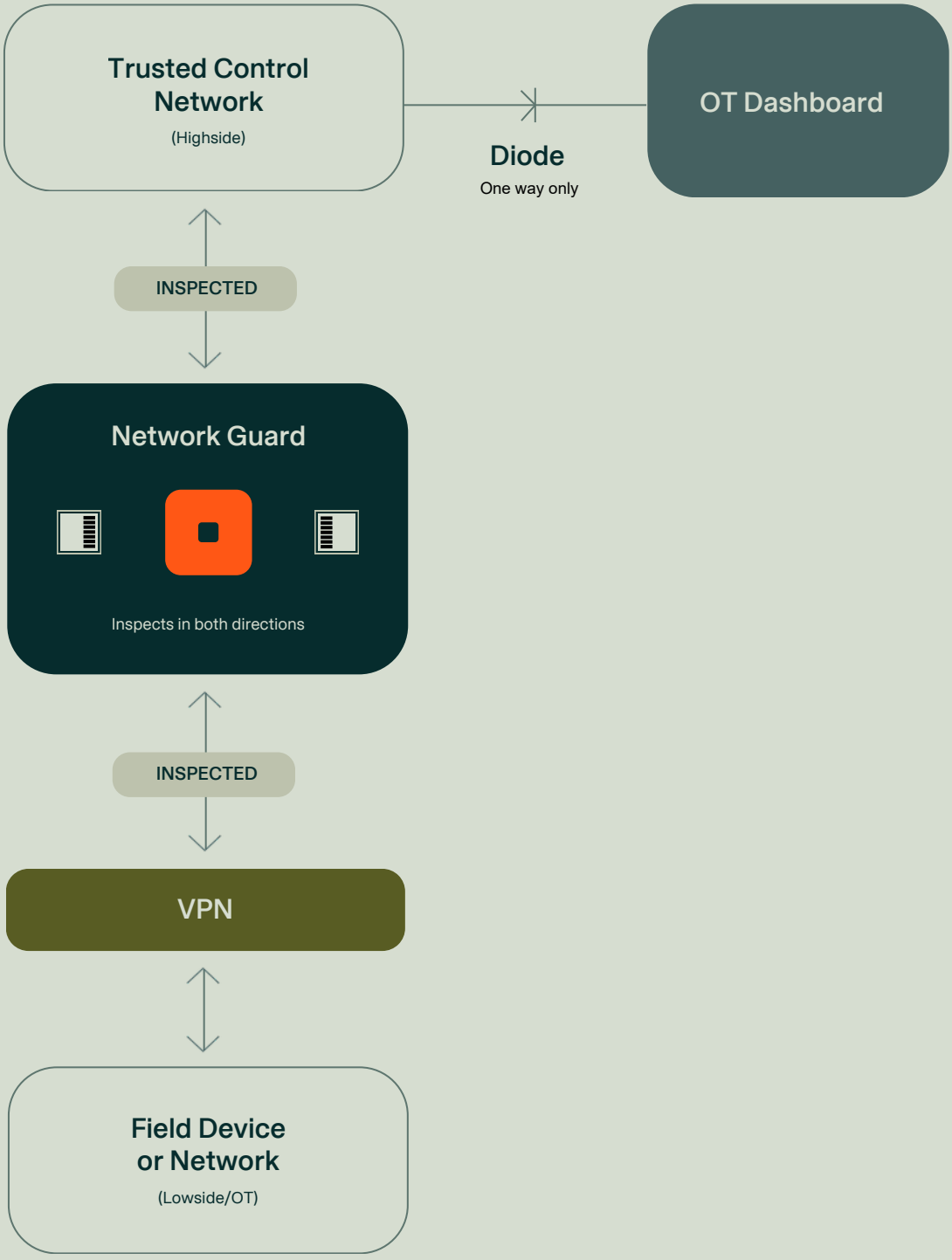
GUARD
The configurable inspection appliance

HIGH/LOW SIDE
The trusted side vs the potentially compromised side

SOFTWARE DIODE
A fully software enforced one-way data path

Configuration 3:
1+ Diode to OT + VPN

In this configuration example, the VPN allows encrypted remote access



NETWORK GUARD BUILDING BLOCKS

GUARD
The configurable inspection appliance

HIGH/LOW SIDE
The trusted side vs the potentially compromised side

SOFTWARE DIODE
A fully software enforced one-way data path

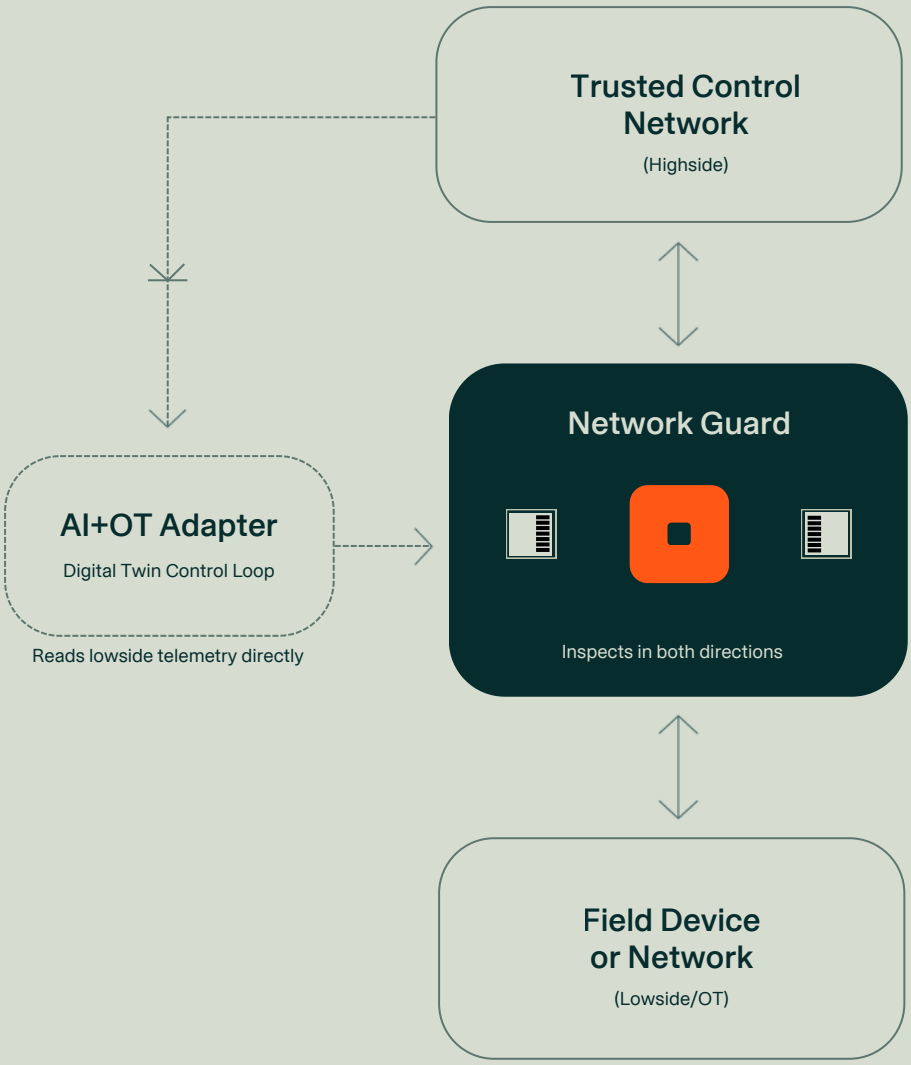


08 Future OT Network Guard Configurations

Configuration 4:
Configurations 1–3 + Control AI Loop

An AI module is added to your chosen Guard/Diode configuration. The AI continuously reads telemetry from the trusted control network (highside), building a live model of expected behaviour and feeds that back to the trusted control network (highside) through the Guard. Anomalies or control decisions can be automated.

Shown applied to Configuration 1, the Control AI Loop can layer on to any of Configurations 1–3



FUTURE NETWORK GUARD BUILDING BLOCKS

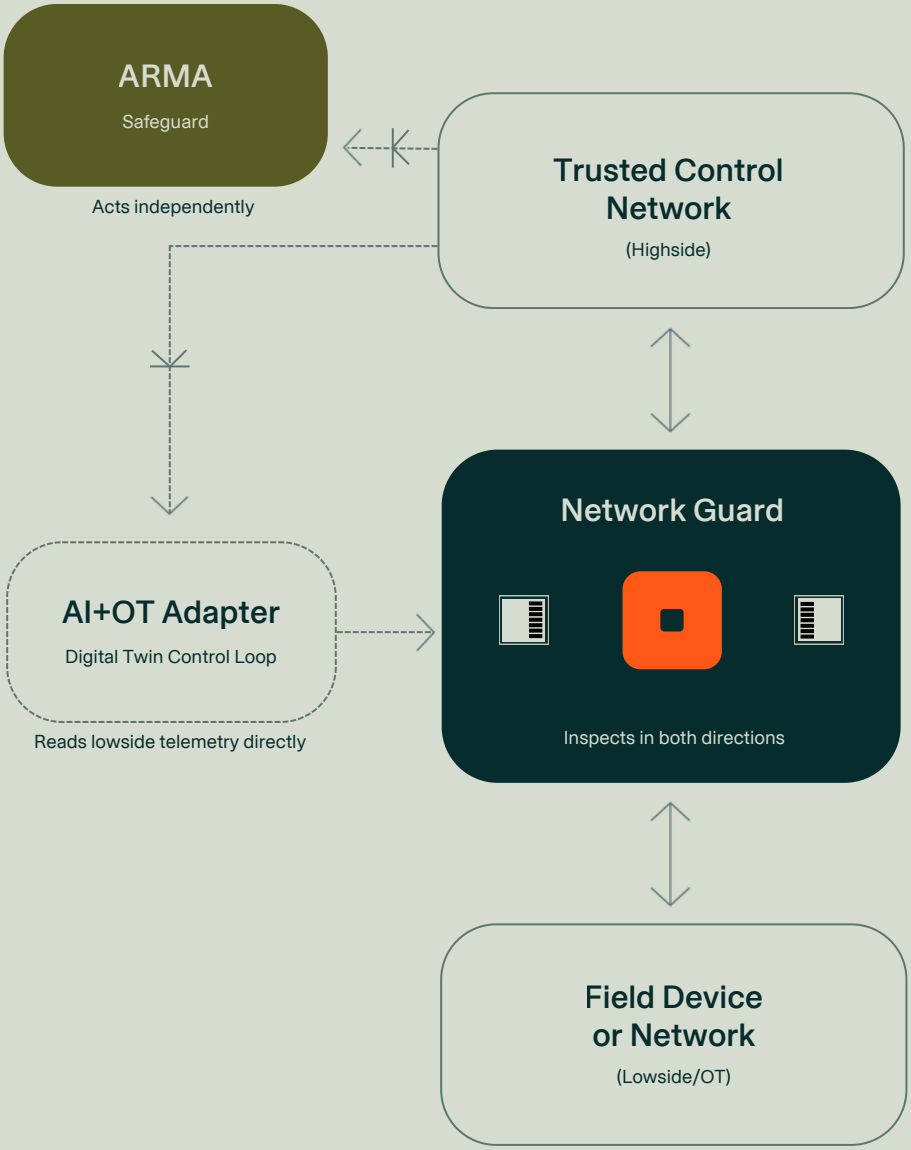
AI +OT ADAPTER
Customised element that reads lowside telemetry directly and loop back through the Guard

ARMA
Assured Reserve Mode Architecture (ARMA): pre-registered configurations to protect an asset

Configuration 5: Configurations 1–4 + ARMA

Shown applied to Configuration 4, the ARMA layers on to any of Configurations 1–4

ARMA adds an independent safeguard on the protected asset itself, that can act independently of the network, Guard or AI to stop the asset being driven into a damaging state.



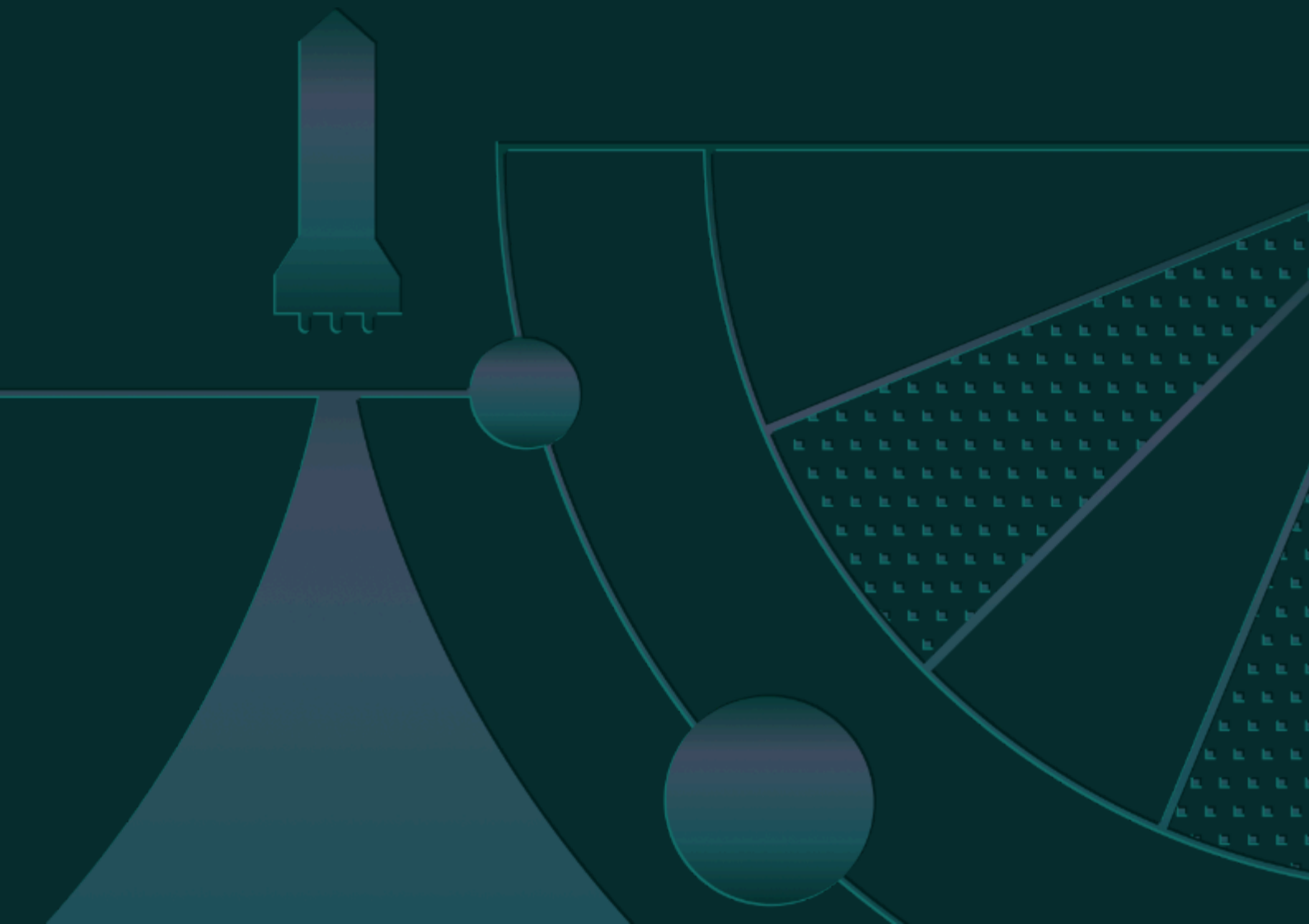
FUTURE NETWORK GUARD BUILDING BLOCKS

AI +OT ADAPTER
Customised element that reads lowside telemetry directly and loop back through the Guard

ARMA
Assured Reserve Mode Architecture (ARMA): pre-registered configurations to protect an asset

Access Network Guard for your OT environment

Kry10 is currently developing OT Network Guard for tailored deployments with early adoption partners. We have active programs in smart manufacturing, defense, critical national energy infrastructure and healthcare.



We're ready to *partner*

Let us help you strengthen what matters

KRY10.COM
HELLO@KRY10.COM
USA/UK/AUS/NZ

KRY10