ChiefNET

CHIEFNET OT SHIELD · USE CASE

Securing Defence & Military Networks

Unidirectional Cross-Domain Data Transfer for Command, Control, Sensor and Logistics Networks

Defence · Military · Government

Document reference	Version	Date	Published by
CN/OTS/UC/DEFENSE/v1.0	1.0	June 2026	ChiefNET Private Limited

Contents

1. Executive Summary
2. Context: Cybersecurity Challenges in Defence Networks
3. ChiefNET OT Shield: Solution Overview
4. Reference Architecture
5. Detailed Use Cases
6. Compliance & Standards Alignment
7. Business Value
8. ChiefNET OT Shield vs. Traditional Firewalls
9. Technical Capability Snapshot
10. Deployment & Engagement Model
11. Conclusion

Also available online at chiefnet.io/use-cases/ot-shield/defence/

Executive Summary

Defence and military organisations operate some of the most sensitive networks in existence – command and control (C2) systems, sensor and radar feeds, platform health telemetry, and range instrumentation – all of which must remain isolated from less-trusted monitoring, logistics and headquarters networks. At the same time, commanders and analysts increasingly need timely visibility into that operational data to build a common operating picture, plan logistics, and assess readiness. This creates a persistent tension between isolation and visibility.

ChiefNET OT Shield is a hardware-enforced data diode purpose-built to resolve that tension. It allows sensor data, platform telemetry, C2 status information and readiness data to flow out of a secure or tactical network to monitoring, headquarters or analysis systems, while making it physically impossible for any command, query or intrusion attempt to flow back in. This one-way transfer principle is the same one long used in cross-domain solutions for moving data between security domains – implemented here as a purpose-built, cost-effective appliance for defence communication and sensor networks.

This document presents a use-case-driven view of how ChiefNET OT Shield applies to defence environments – covering reference architecture, detailed use cases, standards alignment, and the engagement model for deployment across bases, ranges, platforms and logistics networks.

> **Why this matters for defence organisations**
>
> A single successful intrusion into a command, sensor or platform network can compromise operational security, readiness, or safety of personnel and equipment. A hardware-enforced one-way data path removes the most common vector for such intrusions – a reverse command-and-control channel – entirely, without requiring operators to trust a software rule set.

Context: Cybersecurity Challenges in Defence Networks

Rising Demand for Networked Situational Awareness

Modern defence operations depend on a networked common operating picture: sensor and radar feeds, platform health data, logistics status and intelligence products all need to reach commanders and analysts quickly. Meeting this demand has historically meant connecting tactical, sensor and platform networks to broader command and headquarters networks – and every such connection is scrutinised for the risk it introduces into systems that must remain trustworthy under all conditions, including active conflict.

A Sector That Has Long Relied on One-Way Transfer

Defence and intelligence organisations have used hardware data diodes and cross-domain transfer principles for decades specifically because rule-based, software-defined boundaries are considered insufficiently robust for protecting classified and mission-critical networks. Adversaries – both nation-state and criminal – persistently target defence supply chains, contractor networks and less-hardened peripheral systems as a path towards higher-value military networks, making unidirectional architectures a long-standing best practice rather than a novel proposal.

Why General-Purpose IT Security Falls Short

- Firewalls and VPNs are software-defined and bidirectional by design – a misconfigured rule, an unpatched CVE, or a compromised credential can open a path back into a secure network.
- Patch cycles that are routine in enterprise IT are often deferred or restricted on operational and platform networks, where change control is strict and downtime is unacceptable during operations.
- Many defence communication and sensor protocols were designed for reliability and interoperability rather than authentication, making protocol-level attacks difficult to detect with commercial IT tools.
- Forward-deployed and remote sites are often lightly staffed from a cybersecurity perspective, so a compromise can persist undetected for extended periods.

Standards and Policy Drivers

Defence organisations operate under some of the strictest network security policies of any sector, and increasingly reference hardware-enforced segmentation as a preferred control:

- **Cross-Domain Solution (CDS) Principles:** established defence and intelligence community practice for moving data between security domains relies on unidirectional, hardware-enforced transfer as the highest-assurance control available.
- **IEC 62443 / ISA-99 Adapted Practice:** many defence industrial and facility control systems (power, HVAC, base infrastructure) follow IACS segmentation principles equivalent to those used in critical infrastructure.
- **National Defence Cybersecurity Frameworks:** defence ministries and services increasingly mandate documented network segregation and restricted external connectivity for operational and weapons-adjacent IT/OT systems.
- **Supply Chain & Contractor Security Requirements:** defence contractors and system integrators are commonly required to demonstrate network segmentation controls as part of security accreditation and audit processes.
- **Physical Security & Accreditation Processes:** installation and platform accreditation authorities generally favour hardware-verifiable controls over software configuration when evaluating high-assurance boundaries.

ChiefNET OT Shield: Solution Overview

ChiefNET OT Shield is a purpose-built cybersecurity appliance combining a hardware-enforced data diode with a hardened, centrally-managed communications platform. It is designed to sit precisely at the boundary between a secure, tactical or platform network and the monitoring, headquarters or logistics systems that need visibility into it.

Core Architecture

- Physical transmitter (TX) module on the secure/restricted side and a physically separate receiver (RX) module on the monitoring/enterprise side, joined only through an optical, one-way link.
- No physical mechanism exists for signals to travel from the RX side back to the TX side – isolation is enforced by hardware, not by a rule set that can be disabled or bypassed.
- A hardened operating system on both sides minimises attack surface and removes the general-purpose services that create most software vulnerabilities.

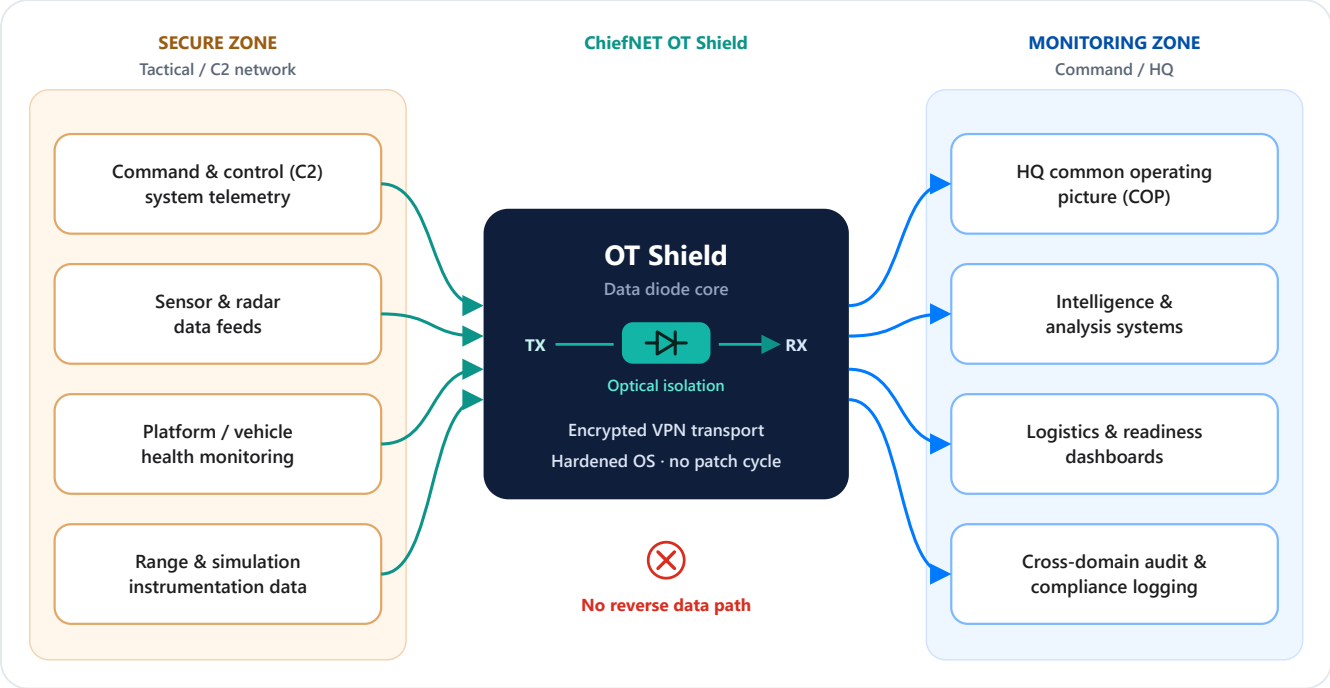
Key Capabilities

- **Native protocol support:** BACnet, Modbus, MQTT, OPC UA and industrial UDP (broadcast/multicast/anycast), covering common sensor, platform and facility telemetry formats.
- **File and log transfer:** UDP file transfer, Syslog and HTTP PUT for sensor logs, platform health reports and range instrumentation data.
- **Encrypted VPN transport:** data exiting the diode is carried to headquarters, command centre or cloud endpoints over a hardened, encrypted tunnel, without reopening a return path.
- **Dual WAN / 4G-5G failover:** on the monitoring (RX) side, ensuring uninterrupted delivery of operational data even where fixed infrastructure is degraded or unavailable.
- **Built-in SD-WAN functionality:** for organisations with many bases, posts or facilities, enabling secure interconnection with headquarters while keeping each site's secure network isolated.
- **Centralised orchestration:** zero-touch and pre-provisioning, fleet-wide monitoring, alerting and dashboards – essential for organisations managing many dispersed sites.
- **Zero patch burden:** because isolation is physical rather than rule-based, there is no firewall ruleset or reverse-path exploit to patch against, reducing change-control overhead on operational networks.

Reference Architecture

Single-Site Deployment – Base, Post or Platform

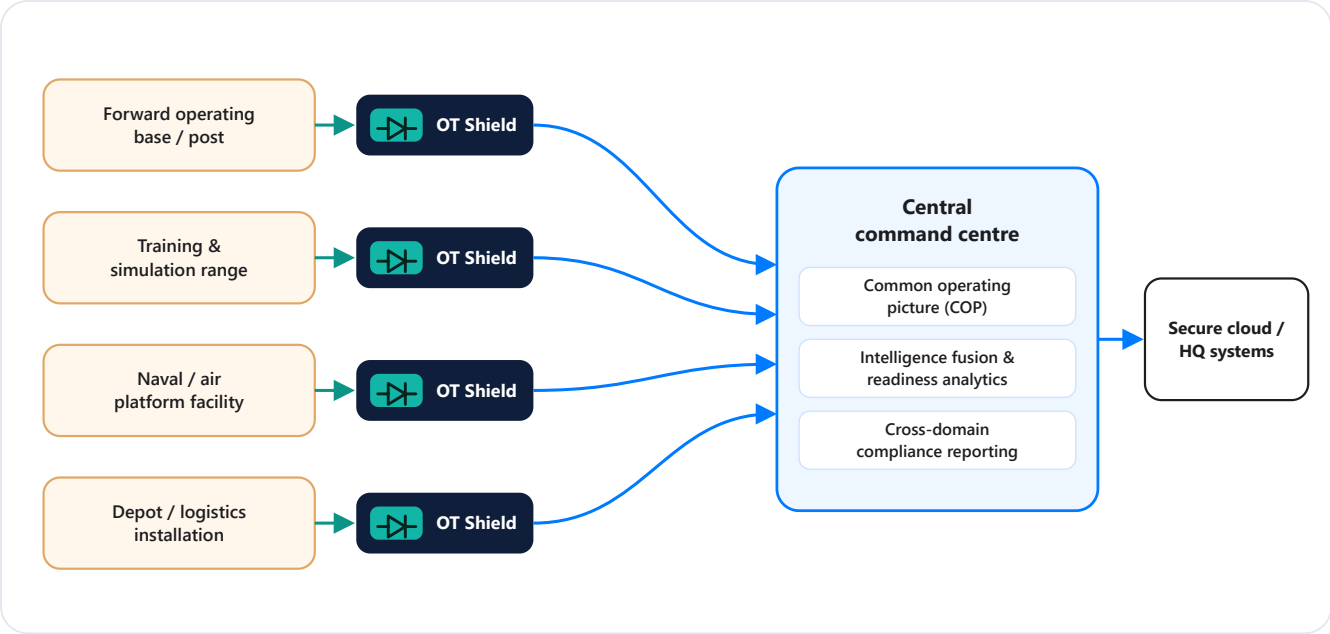
At a single base, post or platform facility, ChiefNET OT Shield sits between the secure zone (C2 telemetry, sensor and radar feeds, platform health monitoring, range instrumentation) and the monitoring zone (headquarters common operating picture, intelligence and analysis systems, logistics dashboards). All operational data leaves the secure zone through the diode's transmitter; nothing can traverse back.



Single-site reference architecture – unidirectional transfer from secure/tactical networks to monitoring and command systems

Multi-Site / Fleet-Wide Deployment

Defence organisations operating multiple bases, ranges, platforms and logistics installations can deploy one OT Shield per site, provisioned and monitored from a central console, while each site's isolation guarantee remains entirely local and independent.



Fleet-wide deployment – multiple defence sites converging on a central command centre

Detailed Use Cases

The following use cases illustrate how ChiefNET OT Shield is applied across defence command, sensor, platform and logistics environments.

USE CASE 5.1

Sensor & Radar Data Feed to Common Operating Picture

Situational Awareness

Challenge	Headquarters analysts need continuous sensor and radar telemetry to maintain an up-to-date common operating picture, but the sensor network must remain isolated from headquarters and external monitoring networks.
OT Shield solution	OT Shield forwards sensor and radar data streams one-way from the sensor network to the headquarters common operating picture system, supporting UDP-based and industrial telemetry protocols without exposing the sensor network to any inbound path.
Outcome	✓ Continuous situational awareness without opening a route into the sensor network ✓ Sensor network remains isolated even as more consuming systems are added ✓ Reduces the sensor network's exposure to reconnaissance or intrusion attempts

USE CASE 5.2

Platform / Vehicle Health & Readiness Monitoring

Fleet & Platform Sustainment

Challenge	Sustainment and logistics commands want continuous health and readiness telemetry from vehicles, aircraft or vessels to plan maintenance and parts logistics, but platform networks are highly sensitive to any external connectivity.
OT Shield solution	OT Shield exports platform health and readiness telemetry one-way to a sustainment and logistics analytics platform, enabling predictive maintenance planning without any inbound path into platform systems.
Outcome	✓ Improved fleet readiness through predictive maintenance visibility ✓ Platform control and safety systems remain fully isolated ✓ Supports logistics and parts planning without platform network exposure

USE CASE 5.3

Range & Simulation Instrumentation Data Export

Training & Test Ranges

Challenge	Training and test range operators need to export instrumentation and simulation data to after-action review and analysis systems, but range control networks must remain isolated from external systems during live exercises.
OT Shield solution	OT Shield transfers range instrumentation and simulation data one-way to after-action review systems, supporting UDP file transfer for large data sets without any inbound path into range control systems.
Outcome	✓ Faster after-action review with rich instrumentation data ✓ Range control network isolated during and after live exercises ✓ Repeatable, low-risk data export process for recurring exercises

USE CASE 5.4

Secure Base Infrastructure Monitoring

Installation & Facility Systems

Challenge	Base facility teams want centralised visibility into power, HVAC and physical security systems across an installation, but these OT systems are often connected to safety and access-control functions that must not be exposed externally.
OT Shield solution	OT Shield exports facility and infrastructure telemetry one-way to a base operations centre or centralised facility management platform, following the same zone/conduit segmentation principles used in critical infrastructure.
Outcome	✓ Centralised facility visibility without exposing safety-critical base systems ✓ Consistent segmentation approach across bases and installations ✓ Simplifies compliance with installation cybersecurity accreditation requirements

USE CASE 5.5

Multi-Base Logistics & Readiness Data Aggregation

Multi-Site Commands

Challenge	Commands overseeing multiple bases or installations need to aggregate readiness, logistics and status data centrally, without bridging separate secure networks together.
OT Shield solution	Each site's OT Shield independently isolates its own secure network while permitting readiness and logistics data to be aggregated and cross-analysed at the command's headquarters or cloud layer, so visibility can be pooled centrally without ever connecting two secure networks directly.
Outcome	✓ Command-wide readiness visibility without direct network-to-network connectivity ✓ Each site retains independent, physically enforced isolation ✓ Supports centralised logistics planning and reporting

USE CASE 5.6

Secure Data Export for Contractor & Coalition Sharing

Contractor & Coalition Interoperability

Challenge	Defence organisations often need to share specific operational or logistics data with contractors or coalition partners, without granting those external parties any connectivity into the originating secure network.
OT Shield solution	OT Shield provides a controlled, one-way export of only the specified data set to a shared platform accessible by contractors or coalition partners, ensuring the originating secure network never accepts any inbound connection from external parties.
Outcome	✓ Enables data sharing with external parties without any inbound access ✓ Originating secure network remains fully isolated from external partners ✓ Simplifies governance of what data is shared and with whom

Compliance & Standards Alignment

The table below maps ChiefNET OT Shield capabilities to the standards and policy expectations most relevant to defence organisations.

Framework / Requirement	Requirement Summary	How OT Shield Addresses It
Cross-Domain Solution (CDS) Principles	Use unidirectional, hardware-enforced transfer as the highest-assurance boundary control between domains.	OT Shield implements the same one-way physical transfer principle as an appliance suited to sensor, platform and logistics data.
IEC 62443 / ISA-99 Adapted Practice	Segment industrial and facility control systems into security zones and conduits.	OT Shield functions as a physically-enforced conduit with only one permitted direction of flow.

Framework / Requirement	Requirement Summary	How OT Shield Addresses It
National Defence Cybersecurity Frameworks	Mandate documented network segregation and restricted external connectivity for operational systems.	Provides a hardware-verifiable segregation control suitable for accreditation documentation.
Supply Chain & Contractor Security Requirements	Demonstrate network segmentation controls as part of security accreditation.	Simplifies contractor and integrator audits with a physically demonstrable one-way boundary.
Physical Security & Accreditation Processes	Favour hardware-verifiable controls over software configuration for high-assurance boundaries.	Isolation is enforced by hardware design, not by a configurable rule set, aligning with accreditation preferences.

Business Value

Business Driver	Impact of ChiefNET OT Shield
Mission and platform readiness	Removes the most common remote-attack vector into secure and platform networks, reducing risk of intrusion-driven disruption.
Accreditation readiness	Provides a hardware-verifiable segregation control that is straightforward to document for accreditation authorities.
Operational cost	Eliminates recurring firewall patch cycles and associated change-control overhead on operational networks.
Situational awareness	Allows common operating picture and analytics initiatives to proceed without re-architecting secure networks.
Multi-site scalability	Centralised, zero-touch provisioning supports rollout across many bases, posts and platforms from a single management console.
Incident response	Rapid, low-risk access to sensor and platform logs speeds up investigation after an incident or exercise.

ChiefNET OT Shield vs. Traditional Firewalls

In defence environments, where the cost of a compromised secure network is measured in operational security and readiness rather than only downtime, the distinction between rule-based and hardware-enforced isolation is a first-order design decision.

Dimension	ChiefNET OT Shield	Traditional Firewall
Data directionality	One-way, physically enforced	Two-way, governed by software rules

Dimension	ChiefNET OT Shield	Traditional Firewall
Patch / maintenance burden	None – isolation is hardware, not firmware	Frequent patching, often restricted by change control
Misconfiguration risk	Not applicable – no rule set to misconfigure	Common cause of real-world network breaches
Resistance to remote exploitation	Near-total – no reverse path exists to exploit	Moderate; depends on rule hygiene and patch currency
Fit for secure, mission-critical networks	Purpose-built for this class of network	Adequate for administrative IT; not ideal for secure networks
Accreditation / audit evidence	Physically demonstrable segregation	Requires ongoing rule and log review to evidence

Technical Capability Snapshot

Capability	Specification
Throughput	Up to 1 Gbps
Isolation	100% one-way, optical / hardware-enforced physical air gap
Software exploit surface on reverse path	Zero – no reverse channel exists
Protocols supported	BACnet, Modbus, MQTT, OPC UA, industrial UDP (broadcast/multicast/anycast)
Data / file transfer	UDP file transfer, Syslog, HTTP PUT
Transport security	Encrypted VPN tunnel from RX side to monitoring/command endpoint
WAN connectivity (RX side)	Dual WAN with 4G/5G failover for uninterrupted delivery
Management	Centrally-hosted controller, zero-touch and pre-provisioning, fleet dashboards and alerting
Operating system	Hardened OS, minimised attack surface, no routine patch cycle required
Additional networking	Built-in SD-WAN for secure multi-site interconnection alongside network isolation

Deployment & Engagement Model

ChiefNET recommends a phased engagement for defence deployments, allowing organisations to validate the solution at one representative site before wider rollout, in coordination with applicable security accreditation processes.

Phase 1 – Assessment & Design

- Site survey of target base, platform or facility: network topology, protocols in use, existing boundary controls.
- Identification of required data points (sensor feeds, platform telemetry, logistics data) and target monitoring destinations.
- Reference architecture finalised against applicable defence cybersecurity and accreditation requirements.

Phase 2 – Pilot Deployment

- OT Shield installed at one representative site, configured for the identified protocols and data flows.
- Validation of one-way data delivery, transport security and monitoring visibility with operational teams.
- Accreditation walkthrough to confirm alignment with the organisation’s security policy.

Phase 3 – Fleet Rollout (site-dependent)

- Zero-touch provisioning used to scale deployment across remaining bases, ranges and platforms.
- Central monitoring dashboards extended to provide fleet-wide visibility and alerting.
- Documentation and audit evidence packaged for accreditation and compliance reviews.

Phase 4 – Ongoing Support

- ChiefNET provides device health monitoring, remote diagnostics support and periodic architecture reviews as monitoring needs evolve.

Conclusion

Defence organisations face a structural challenge: the same connectivity that enables modern situational awareness and logistics visibility also expands the exposure of secure, mission-critical networks. ChiefNET OT Shield resolves this tension directly – not by adding another rule set to manage, but by making the reverse path physically impossible.

Across command, sensor, platform, range and logistics environments, the use cases in this document show a consistent pattern: operational data flows out for situational awareness, sustainment and reporting, while command-and-control risk is removed at the hardware level. For organisations balancing operational visibility against the non-negotiable security requirements of defence networks, that combination – visibility without exposure – is the foundation ChiefNET OT Shield is built to provide.

Next Step

ChiefNET recommends starting with a site assessment and pilot deployment at one representative base, platform or facility, validating data delivery and accreditation alignment before scaling across the fleet.

ChiefNET

About ChiefNET Private Limited

ChiefNET Private Limited, founded in 2020 and headquartered in Coimbatore, India, builds secure networking products for enterprises and critical infrastructure: ChiefNET SD-WAN, a cloud-managed network platform for multi-site organisations, and ChiefNET OT Shield, a hardware-enforced data diode for operational technology. ChiefNET product series are Make in India certified.

---

contact@chiefnet.io · chiefnet.io
DVP Building, First Floor, No. 4, Kalapatti Main Road, Civil Aerodrome Post, Nehru Nagar West, Coimbatore, Tamil Nadu 641014, India