elecdan

DEFENSE AND SECURITY MARKET

FROM DATA TO DECISIONS:

SECURE SOLUTIONS FOR C2 (COMMAND AND CONTROL)

Q1 – 2026

Who are we?

1992

Greater Paris area (91)
Year founded

2017–2019–2021–2023

Global events
Milipol trade fair

2024

Member of GICAT

2025

Participation in the Techterre fair and the 4th edition of the NATO Dialogues

We provide multi-screen display control solutions that are at the heart of information systems.

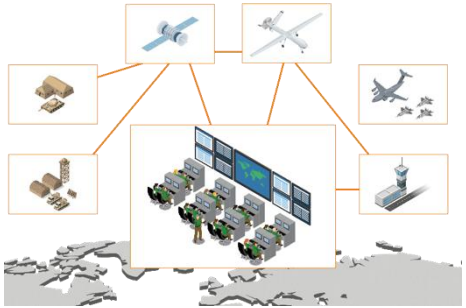
More data and complexity = More risk

Information superiority

- Strategy for decision dominance through precise, rapidly available situational awareness.
- Effective use of resources while ensuring their protection through targeted use of information
- Shared situational awareness and cooperation between different command centers are essential

Massive increase in relevant data

- Software-Defined Defence (SDD) brings a flow of data from different information sources.
- (Digitalisation: Sensor–Command–Actor including Open Source) Multi-domain operations add more complexity
- Command post staff must have access to a wide variety of information sources with different security levels.

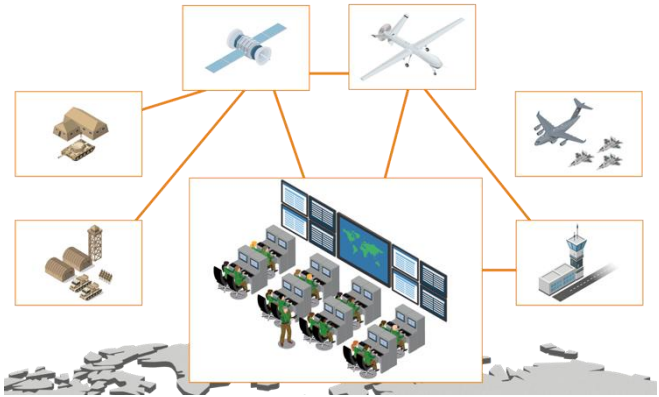


Risk of data theft or corruption

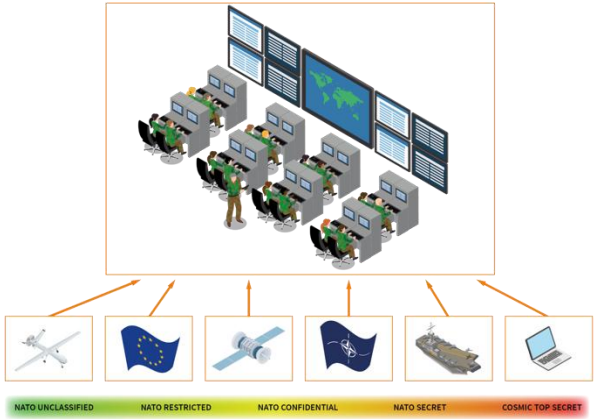
- Uncontrolled access to classified information enables the falsification, compromise or theft of data, whether through negligence or intent.
- With the growing collection and storage of information, the possibilities and impact of security breaches increase exponentially.
- Defending against cyberattacks and reducing insider risks are the greatest challenges

The challenges of common situational awareness

Multi-domain: increased data volume from different sources



Multi-class: growing complexity due to data from different security domains



Elecdan offers secure interdisciplinary collaboration solutions to increase efficiency and cybersecurity in Command and Control (C2) centers.

Command and control systems – Status quo

The challenge of information sharing

- Wired IT and audiovisual systems, inflexible, unprotected
- Collaboration between dispersed teams is hindered
- Merging data from different classifications is time-consuming and error-prone
- Maintenance requires an operational IT team
- Unproductive working environment

IT security “In-house risk”

- Possibility of accidental or intentional breach
- Computer and cabling without physical separation
- Hard drives, USB ports, network connections generally accessible to a wide range of users
- Protect access to machines

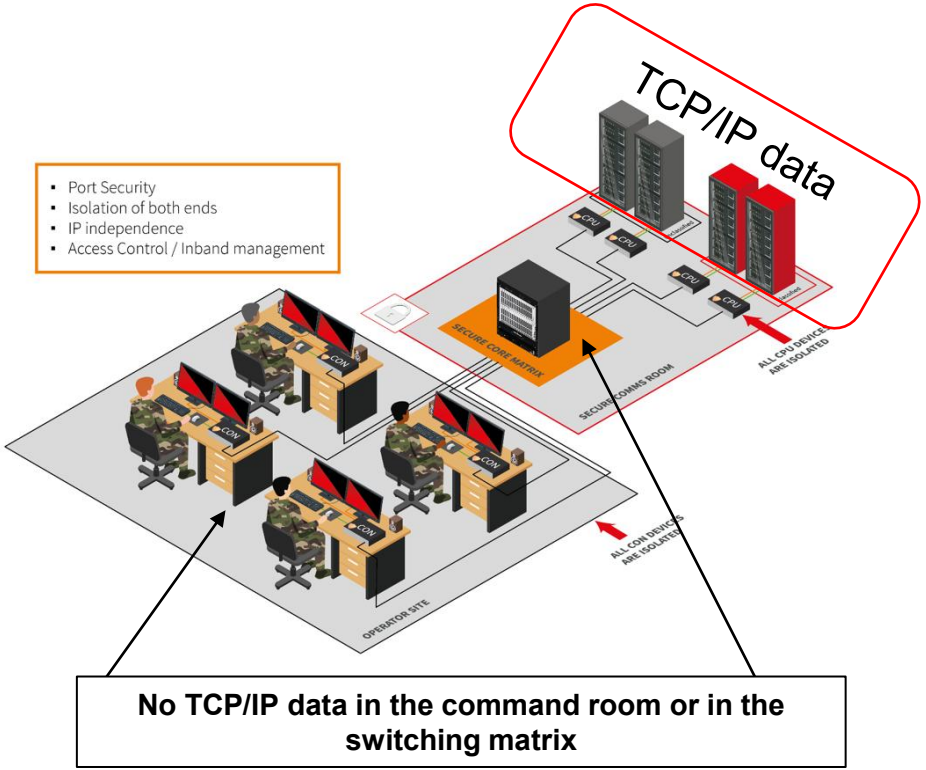
Complex maintenance and scalability

- Difficulty creating effective redundancy concepts
- Complex systems integration
- Longer commissioning times for deployable vehicles
- Decentralised systems increase support staffing costs
- Hard to scale or upgrade at the pace of technology
- High consumption of electricity, space, air conditioning

Needs in C2 centres

- Need access to real-time sources without latency Switch between “red (classified)” and “black (unclassified)” systems
  - Real-time multi-class and multi-domain: IEC 62443 network separation Need for isolation and separation of sources between classified and unclassified
- Threats to TCP/IP ports
- Centralization of the machines
  - Secure access to machines
  - Prevent EM capture (TEMPEST)
  - Reduce thermal footprint
  - Simplify destruction of machines

Our solution

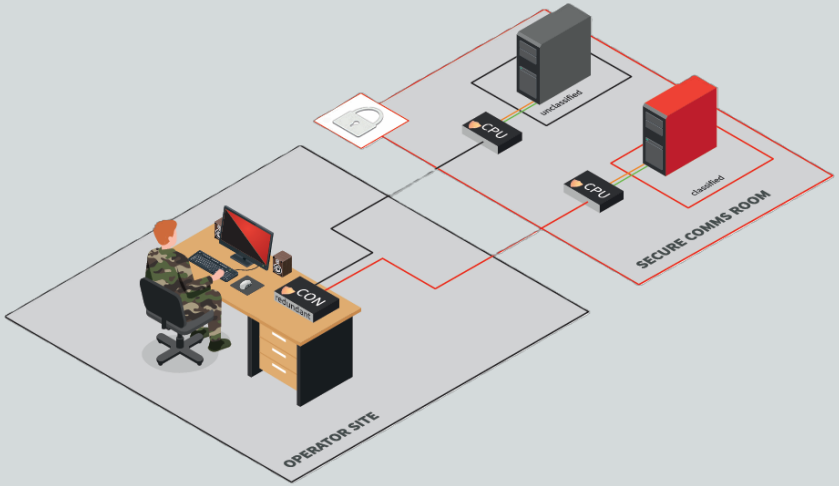


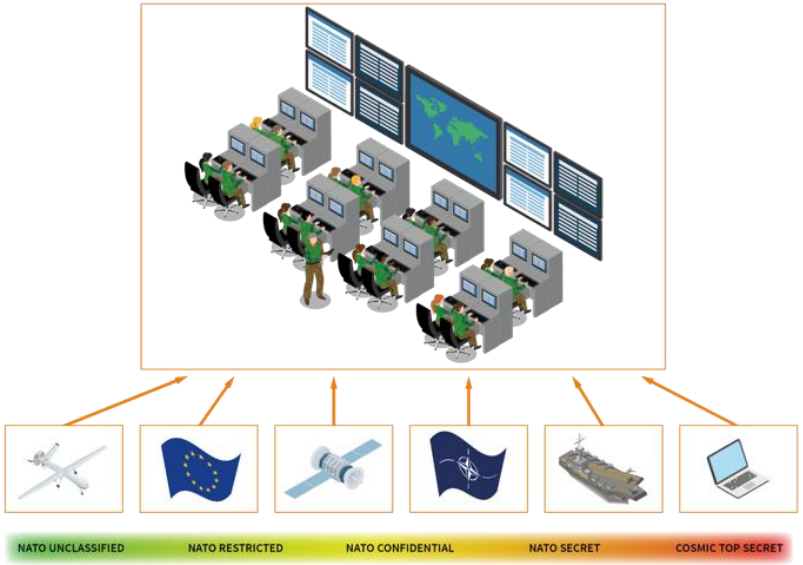
- **Unrestricted interaction between staff units that are spatially separated**
  - Real-time transmission of situational pictures to an unlimited number of workstations over long distances Flexible real-time switching between “red” and “black” systems
- **Elimination of insider risk**
  - No TCP/IP or storage devices at the operator console Hardware/servers in secure rooms and USB/AV completely isolated Real-time emergency shutdown in case of unauthorised access
- **Fully redundant real-time architecture Rapid reconfiguration of the command centre and mission stations**

Supervision level

Access to classified and unclassified sources from the same workstation

Separation and isolation of sources





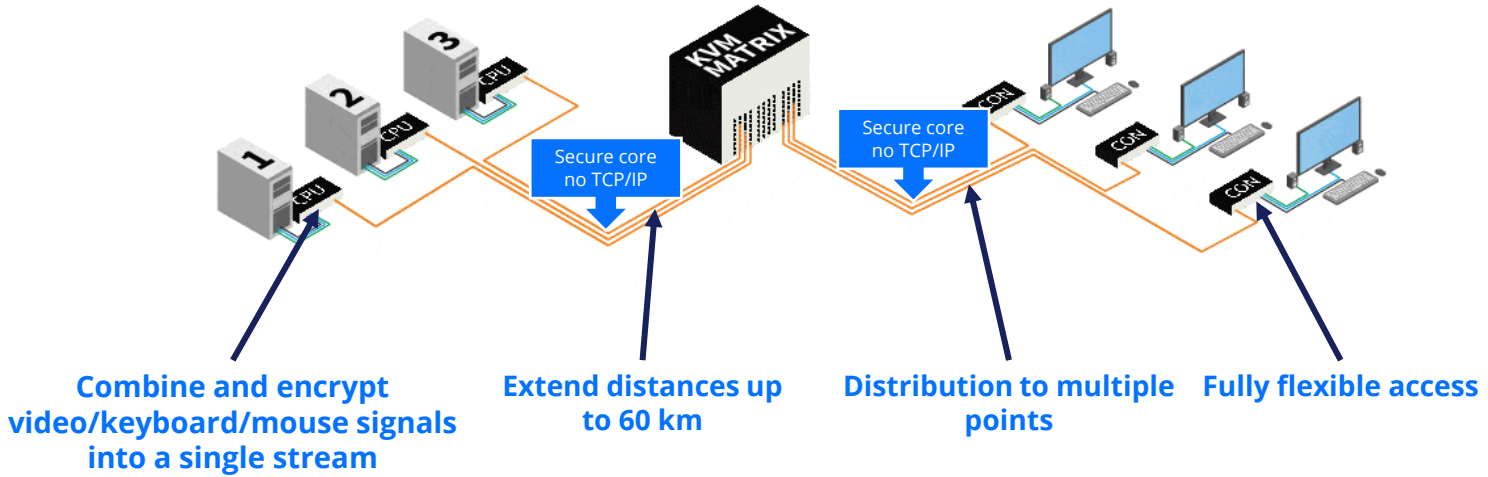
- Secure architecture without TCP/IP
- IEC 62443 zoning principle
- Real-time collaboration
- NIAP-compliant unidirectional flow components

KVM technology addresses these needs effectively

- **KVM keyboard – video – mouse**

  - Simple extender unit

- **Access/manage multiple machines on a single user workstation**
- **Hardware/software independent – No installation of software drivers**
- **Extension – switching – distribution**



The four pillars of KVM technology

Secure solution

Signal extension

Computer in a secure room. No TCP/IP data traffic between the computer and the operator console

Secure matrix core

Source switching between several types of classifications within a single infrastructure

Secure matrix control

Fast, secure out-of-band administration

Secured with data isolator (diodes)

Extender endpoints

Certifications - Compliancy

EAL4+ certifies that secure extenders offer the highest level of security required by NATO and NATO countries.

- EAL4+ is the highest level possible based on the system's technical characteristics. An important certification for secure environments within government and NATO. Required for procurement under the Common Criteria Recognition Arrangement

Common Criteria EAL4 certifies solutions tested by the manufacturer for a security level selected by an independent testing laboratory.

NATO TEMPEST SDIP 27, Level A, B or C, supports the security of information security systems against compromising emanations

- Fibre-optic connections prevent radiation Interceptable content is blocked at a distance of 0, 20 or 100 metres or more. Other TEMPEST requirements can be addressed depending on the necessary applications

If required, environmental hardening against shock/vibration or moisture is also optionally available.

NIAP PP4.0 PSD is a Protection Profile defined by NIAP (National Information Assurance Partnership), which sets out the security requirements that Peripheral Sharing Devices (PSD) must meet

- PP4.0 defines **the minimum security requirements** for a PSD to be certified.
- It ensures that no data can pass from one computer to another via the switch or peripherals.
- This version 4.0 (2019) is aligned with Common Criteria v3.1 revision 5 and introduces a separation between the base profile and modules according to interface types.
- Today it is **the strictest standard** for secure KVMs and similar devices.

IHSE Secure product portfolio at a glance

Secure Extender

- Fully redundant, compact modular design with low energy consumption Multiple video interfaces with low latency up to 4K60Hz Fanless design & single-face interfaces EAL4+ and TEMPEST certified (NIAPC approved) The lowest operational cost enabled by 1 Gbps video links

Secure IP access SIRA

- Video up to 4K30 Complete isolation of the core system LDAP and Active Directory connectivity Fully encrypted transmission Redundant network connection

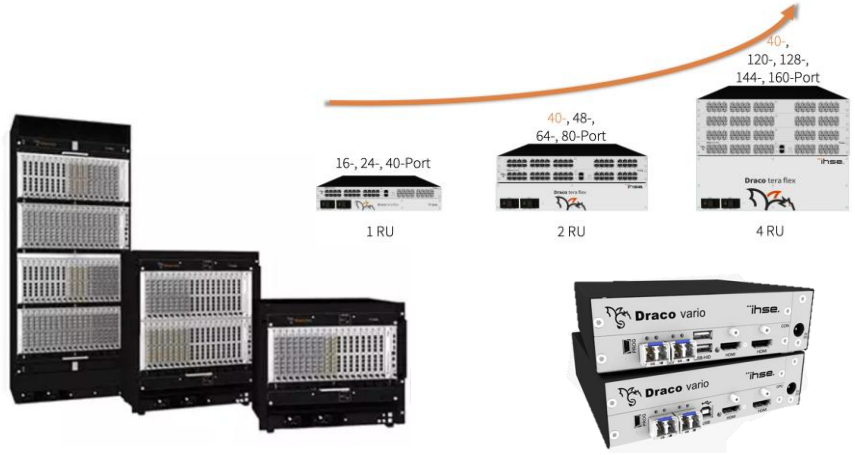
Secure KVM switch

- Scalable platform for up to 576 ports in a single matrix Secure core: TCP/IP-independent Instant switching with no delay Flex Port technology (each port is an input/output) Hot Plug & Swap – fully redundant architecture
- Multiscreen: Keyboard–mouse sharing across 2 to 8 screens
- Multi viewer: Customizable video display layout controlled via keyboard shortcut

IHSE Secure solutions are marketed worldwide under the “Draco” brand

More insights

- Modular systems based on cards and chassis
- Cards available with all video interfaces
- Support for both modern and legacy machine fleets
- Core of the secure KVM solution: dedicated non-IP redundant protocol
- Support for physical machines or VMs (RDP, VNC, SSH)
- Unit tropicalization (depending on version)
- EAL4+ Certification
- Manufactured in Germany



Advantages of the IHSE product ranges

- Modularity: Easy scalability of the solution
- Density: 1U = 6 × 4K60Hz streams + HID
- Possibility to combine the use of different cards
- Hot-swappable cards
- Use of low-power FPGA technology

- NATO validation
- Products available on the NIAPC – NATO catalogue website

Our partner
High Secure Labs

Manufacturer of security systems certified NIAP PP 4.0 and NATO-approved for accessing sensitive machines in the defense and industrial sectors

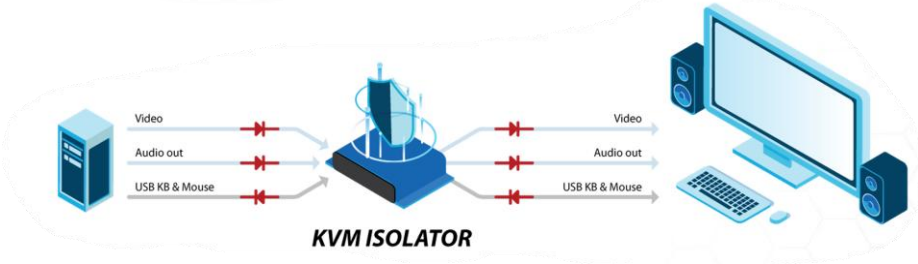
Operation of isolators:

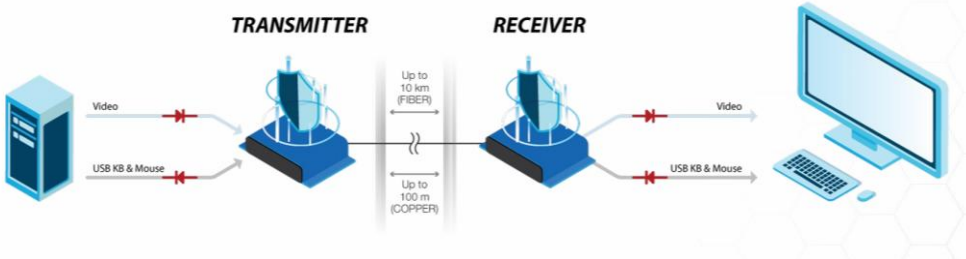
Isolators ensure a strictly unidirectional flow between the computer and the peripherals, preventing any risk of data leakage or the insertion of malicious code.

Operation of extenders:

KVM diode extenders transmit signals while enforcing a unidirectional data flow to ensure secure data transmission.

HighSecLabs
Highest Security Solutions





High Secure Lab product portfolio – certified range

Secure extender

- NIAP PP 4.0 certification
- TEMPEST level B
- Video up to 4K30
- EDID capture Copper or fibre extension

Isolators

- NIAP PP 4.0 certification
- Diode system
  - signal unidirectionality
- Up to 4K30

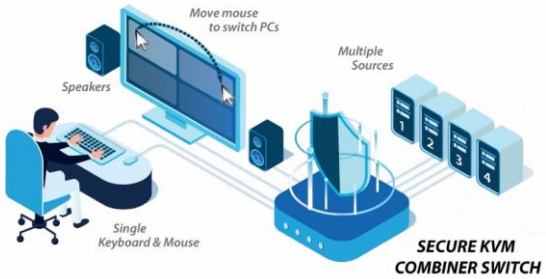
Mini matrix and Multiviewer

- NIAP PP 4.0 certification
- Video up to 4K30
- Signal unidirectionality
- Multi-view Multi-source

Our partner
High Secure Labs

HighSecLabs
Highest Security Solutions

- Secure multiviewer with KVM Switch functions integrated
  - NIAP Common Criteria PP4.0
  - Up to 16 sources on one screen
  - Up 2 screen in output



High Secure Lab product portfolio – certified and ruggedised range

Secure extender

- NIAP PP 4.0 PSD certification
- TEMPEST level A
- Ruggedness: MIL-STD-810G
- Video up to 4K30
- EDID capture Copper or fibre extension

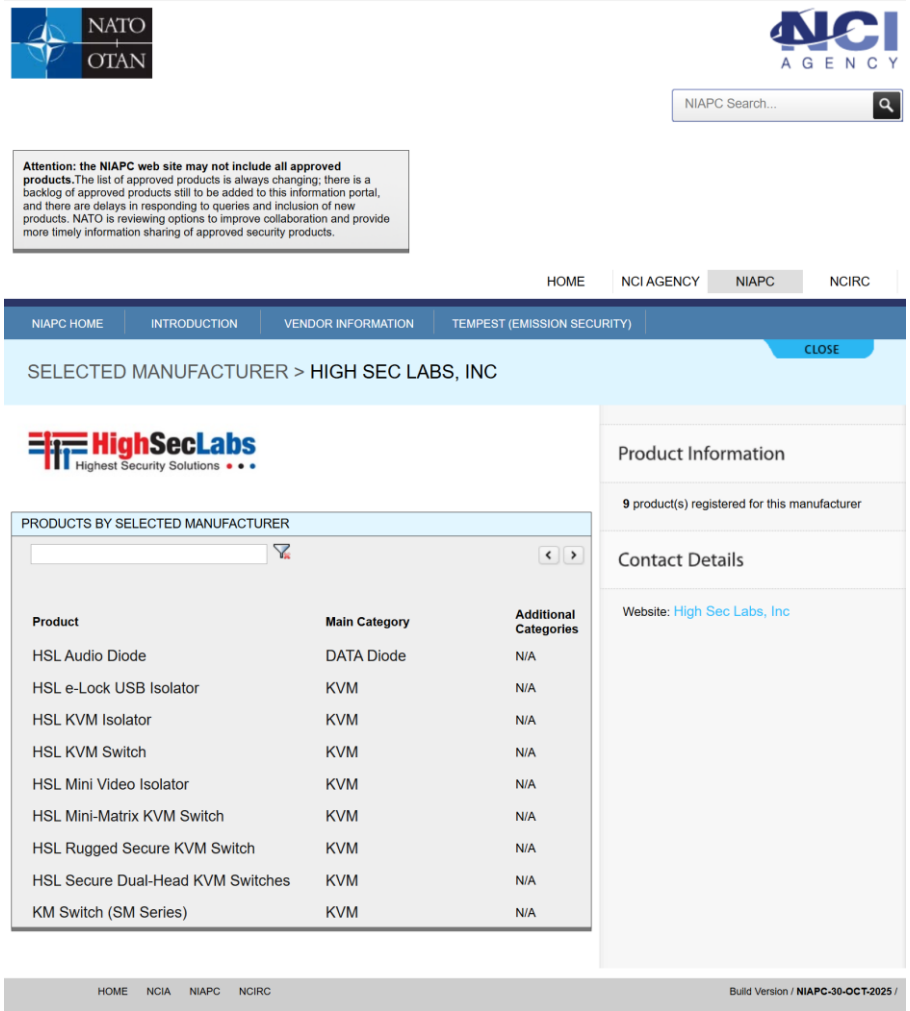
Secure KVM switch

- NIAP PP 4.0 PSD certification
- TEMPEST level A
- Ruggedness: MIL-STD-810G
- Video up to 4K30 IP67

Mini matrix and KVM combiners

- NIAP PP 4.0 PSD certification
- Ruggedness: MIL-STD-810G
- Video up to 4K30
- Signal unidirectionality
- Multi-view Multi-source

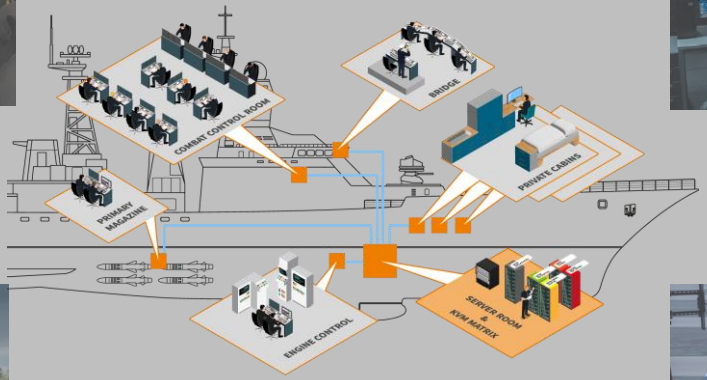
- NATO validation
- Products available on the NIAPC – NATO catalogue website



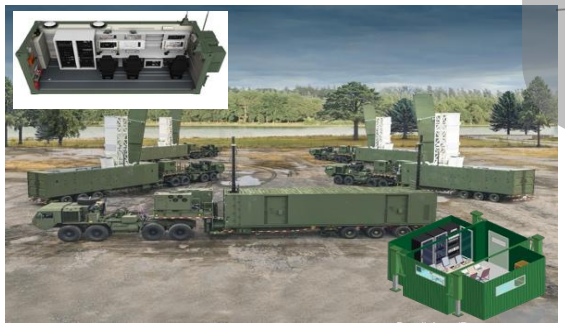
Typical use cases

Mobile command posts

Naval



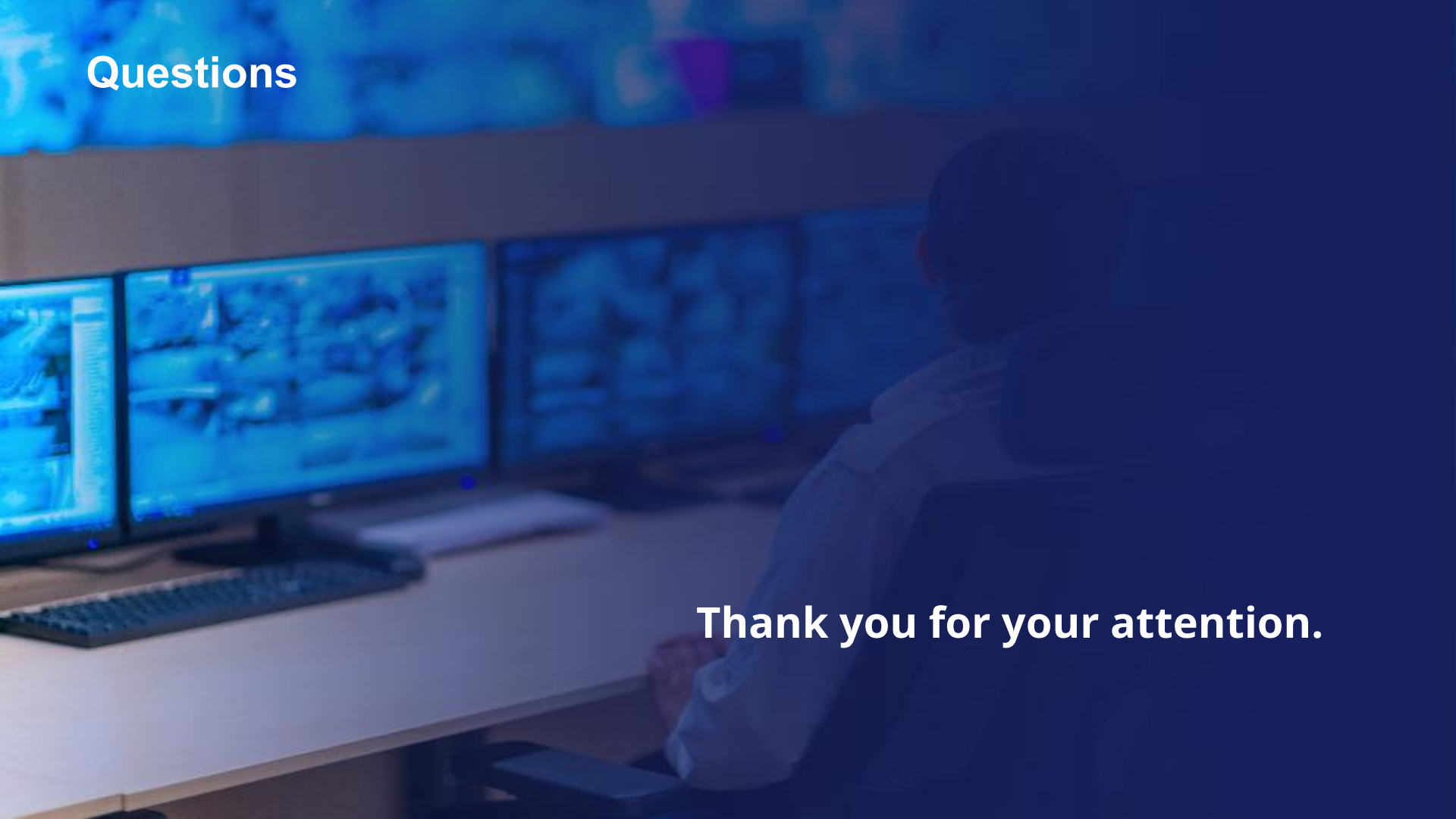
Large C2 centres



Tactical command centres

ATM

Questions



Thank you for your attention.