elecdan

MARCHÉ DÉFENSE ET SÉCURITÉ

DES DONNÉES AUX DÉCISIONS :

SOLUTIONS SÉCURISÉES POUR LE C2 (COMMANDE ET CONTRÔLE)

Q1 - 2026

Qui sommes-nous ?

1992

Région Parisienne (91)
Année de création

2017-2019-2021-2023

Evénements mondiaux
Salon Milipol

2024

Membre du GICAT

2025

Participation au salon
Techterre et à la 4e édition
des dialogues OTAN

Nous fournissons des solutions de contrôle d'affichages multi-écrans qui sont au cœur des systèmes d'informations.

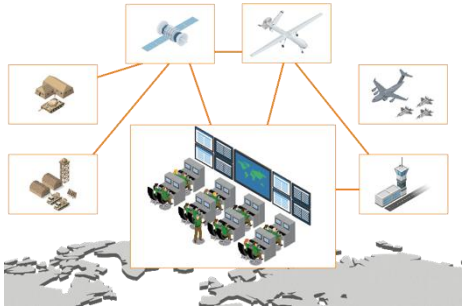
Plus de données et de complexité = Plus de risques

Supériorité de l'information

- Stratégie de domination décisionnelle grâce à une conscience situationnelle précise et rapidement disponible
- Utilisation efficace des ressources en assurant leur protection grâce à une utilisation ciblée de l'information
- La conscience situationnelle conjointe et la coopération entre différents centres de commandement sont essentielles

Augmentation massive des données pertinentes

- La Défense Définie par Logiciel (DDL) apporte un flot de données provenant de différentes sources d'information. (Numérisation : Sensor-Command-Actor incluant OpenSource)
- Les opérations multi-domaines apportent plus de complexité
- Le personnel du poste de commandement doit avoir accès à une grande variété de sources d'information ayant différents niveaux de sécurité.

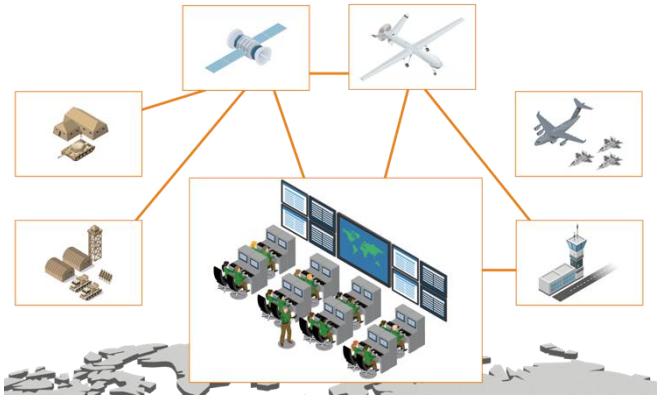


Risque de vol ou de corruption de données

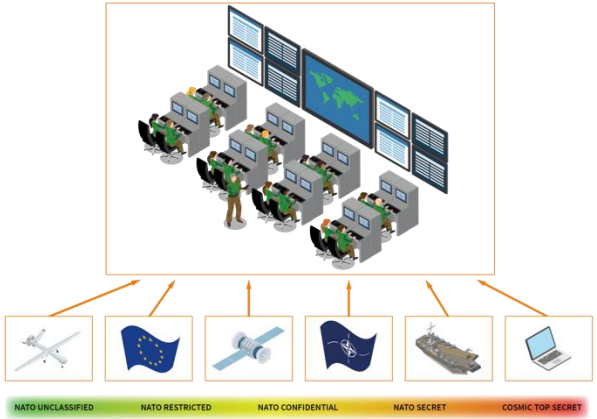
- L'accès incontrôlé aux informations classifiées offre la possibilité de falsifier, compromettre ou voler des données, que ce soit par négligence ou délibérée.
- Avec la collecte et le stockage croissants d'informations, les possibilités et l'impact des violations de sécurité croissent de façon exponentielle.
- Se défendre contre les cyberattaques et réduire les risques internes sont les plus grands défis

Les défis de la conscience situationnelle commune

Multi-domaines : augmentation du volume de données provenant de différentes sources



Multi-classes : complexité croissante grâce à des données provenant de différents domaines de sécurité



Elecdan propose des solutions de collaboration interdisciplinaires sécurisées pour accroître l'efficacité et la cybersécurité dans les centres de commandement et de contrôle (C2).

Systèmes de commandement et de contrôle – Statu Quo

Le défi du partage d'informations

- Systèmes informatiques et audiovisuels filaires, inflexible, pas protégé
- La collaboration entre les équipes dispersées est entravée
- Fusionner des données issues de différentes classifications est long et sujet aux erreurs
- La maintenance nécessite une équipe informatique en fonctionnement
- Environnement de travail improductif

Sécurité en informatique « Risque interne"

- Possibilité de violation accidentelle ou intentionnelle
- Ordinateur et câblage sans séparation physique
- Disques durs, ports USB, connexions réseau généralement accessibles à un large éventail d'utilisateurs
- Protéger l'accès aux machines

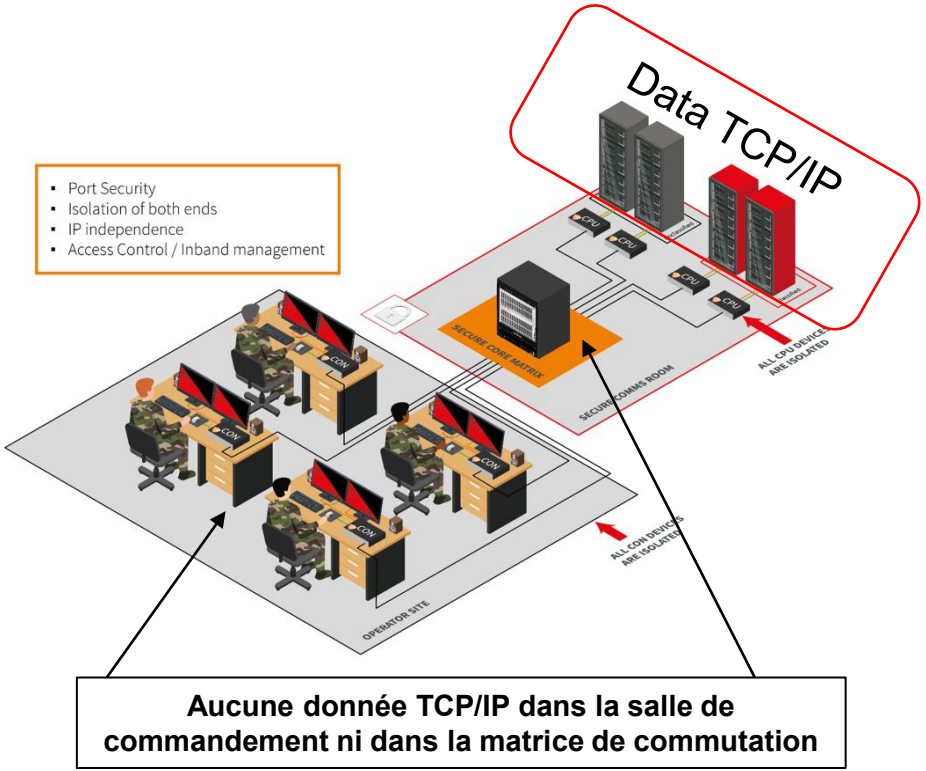
Maintien et évolutivité complexe

- Difficulté à créer des concepts de redondance efficaces
- Intégration de systèmes complexes
- Temps de mise en service plus longs pour les véhicules déployables
- Les systèmes décentralisés augmentent le coût du personnel de soutien
- Difficile à mettre à l'échelle ou à mettre à niveau à l'échelle de la technologie
- Forte consommation d'électricité, d'espace, de climatisation

Besoins dans les centres C2

- Besoin d’accès aux sources en temps réel sans latence
- Alterner entre systèmes « rouge (classifié) » et « noir (non-classifié) »
  - Multi-classe et multi-domaine temps réel : IEC 62443 séparation de réseaux
  - Besoin d’isolation et de séparation des sources entre classifiées et non-classifiées
- Menaces sur les ports TCP/IP
- Centraliser les machines
  - Sécuriser l’accès aux machines
  - Empêcher la CEM (captation ElectroMagnétique) (Tempest)
  - Reduction de l’empreinte thermique
  - Simplifier la destruction des machines

Notre solution

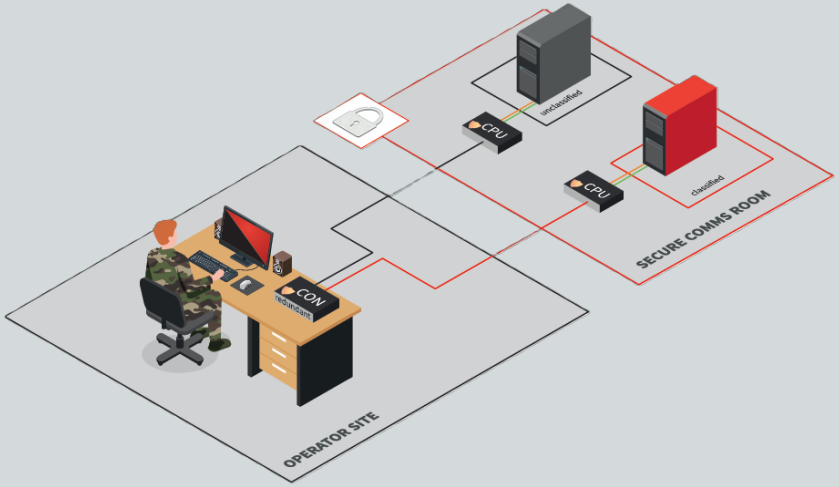


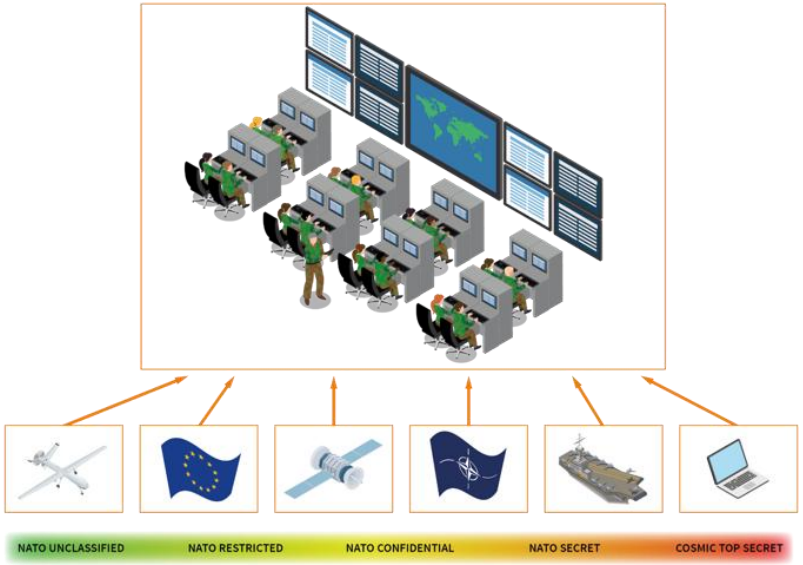
- **Interaction sans restriction entre unités d'état-major spatialement séparées**
  - Transmission en temps réel d'images situationnelles vers un nombre illimité de postes de travail sur de longues distances
  - Commutation flexible en temps réel entre les systèmes « rouge » et « noir »
- **Élimination du risque d'initié**
  - Aucun TCP/IP ou périphériques de stockage sur la console d'exploitation
  - Matériel/serveurs dans des salles sécurisées et USB/AV complètement isolés
  - Arrêt d'urgence en temps réel en cas d'accès non autorisé
- **Architecture temps réel entièrement redondante**
- **Reconfiguration rapide du centre de commandement et des stations de mission**

Niveau supervision

Accès a des sources classifiées et non-classifiées depuis un même poste

Séparation et isolation des sources





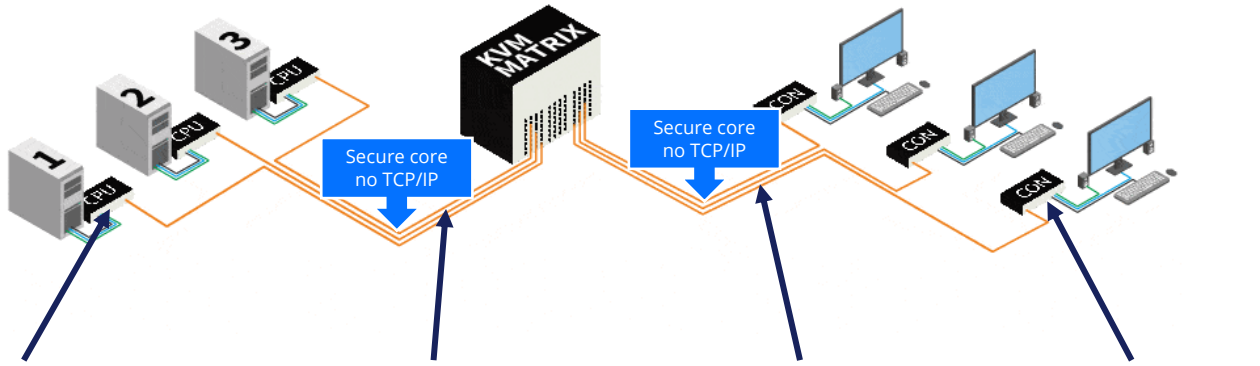
- Architecture sécurisée sans TCP/IP
- Principe de zoning IEC 62443
- Collaboration en temps réel
- Composants flux unidirectionnels conforme NIAP

La technologie KVM répond efficacement à ces besoins

- **KVM clavier - vidéo – souris**

  - Simplicité unité d'extension

- **Accès/gestion de plusieurs machines sur un seul poste utilisateur**
- **Indépendant matériel/logiciel - Pas d'installation de pilotes logicielles**
- **Extension – commutation – distribution**



Combiner et chiffrer les signaux vidéo/clavier/souris en un seul flux

Étendre Distances jusqu'à 60 km

Distribution vers plusieurs points

Accès totalement flexible

Les 4 piliers de la technologie KVM

Solution sécurisée

Extension du signal

Ordinateur dans une pièce sécurisée. Aucun trafic de données TCP/IP entre l'ordinateur et la console d'exploitation

Cœur de matrice sécurisé

Commutation de sources entre plusieurs types de classifications dans une seule infrastructure

Contrôle sécurisé matriciel

Administration rapide et sécurisée Out of Band

Sécurisé avec isolateur de données (diodes)

Extrémités des prolongateurs

Certifications

EAL4+ certifie que les prolongateurs sécurisés offrent le niveau de sécurité le plus élevé requis par l'OTAN et les pays de l'OTAN.

- EAL4+ est le niveau le plus élevé possible grâce aux caractéristiques techniques du système.
- Une certification importante pour les environnements sécurisés au sein du gouvernement et de l'OTAN.
- Exigé pour les achats en vertu de l'accord de reconnaissance des critères communs

Les Critères Communs, EAL4 certifie les solutions testées par le fabricant pour un niveau de sécurité sélectionné par un laboratoire d'essais indépendant.

TEMPEST OTAN SDIP 27, Niveau A, B ou C, soutient la sécurité des systèmes de sécurité de l'information contre les radiations compromettantes

- Les connexions à fibre optique évitent le rayonnement
- Le contenu interceptable est bloqué à une distance de 0, 20 ou 100 mètres ou plus.
- D'autres exigences Tempest peuvent être gérées en fonction des applications nécessaires

Si nécessaire, un durcissement environnemental contre les chocs/vibrations ou l'humidité est également disponible en option.

NIAP PP4.0 PSD, il s'agit d'un profil de protection (Protection Profile) défini par le NIAP (National Information Assurance Partnership), qui établit les exigences de sécurité auxquelles doivent se conformer les Péripheral Sharing Devices (PSD)

- Le PP4.0 définit **les exigences minimales de sécurité** pour qu'un PSD soit certifié.
- Il garantit qu'aucune donnée ne peut transiter d'un ordinateur vers un autre via le commutateur ou les périphériques.
- Cette version 4.0 (2019) est alignée sur les critères Common Criteria v3.1 révision 5 et introduit une séparation entre le profil de base et des modules selon les types d'interfaces.
- C'est aujourd'hui **le standard le plus strict** pour les KVM sécurisés et dispositifs similaires.

Portefeuille de produits IHSE Secure en un coup d'œil

Secure Extender

- Conception modulaire et compacte entièrement redondante et économe en énergie
- Interfaces vidéo multiples avec une faible latence jusqu'à 4k60Hz
- Conception sans ventilateur & interfaces à face unique
- Certifié EAL4+ et Tempest (homologué NIAPC)
- Le coût opérationnel le plus bas est rendu possible grâce aux liaisons vidéo de 1 Go/s

Accès IP sécurisé SIRA

- Vidéo jusqu'à 4k30
- Isolation complète du système de noyau
- Connexion LDAP et Active Directory
- Transmission entièrement chiffrée
- Connexion réseau redondante

Commutateur KVM sécurisé

- Plateforme évolutive pour jusqu'à 576 ports dans une seule matrice
- Cœur sécurisé : TCP/indépendant de l'IP
- Commutation immédiate sans délai
- Technologie Flex Port (chaque port est une entrée/sortie)
- Hot Plug & Swap - architecture entièrement redondante

Les solutions IHSE Secure sont commercialisées dans le monde entier sous la marque « Draco »

- Validation OTAN
- Produits disponibles sur le site du catalogue NIAPC - OTAN

Portefeuille de produits High Secure Lab – gamme certifiée

Extendeur sécurisé

- Certification NIAP PP 4.0
- Tempest niveau B
- Vidéo jusqu'à 4k30
- Capture EDID
- Déport cuivre ou fibre

Isolateurs

- Certification NIAP PP 4.0
- Système à diode
  - unidirectionnalité des signaux
- Jusqu'à 4k30

Mini matrice et Multiviewer

- Certification NIAP PP 4.0
- Vidéo jusqu'à 4k30
- Unidirectionnalité des signaux
- Multi-vues
- Multi-sources

Portefeuille de produits High Secure Lab – gamme certifiée et renforcée

Extendeur sécurisé

- Certification NIAP PP 4.0 PSD
- Tempest niveau A
- Robustesse : MIL-STD-810G
- Vidéo jusqu'à 4k30
- Capture EDID
- Déport cuivre ou fibre

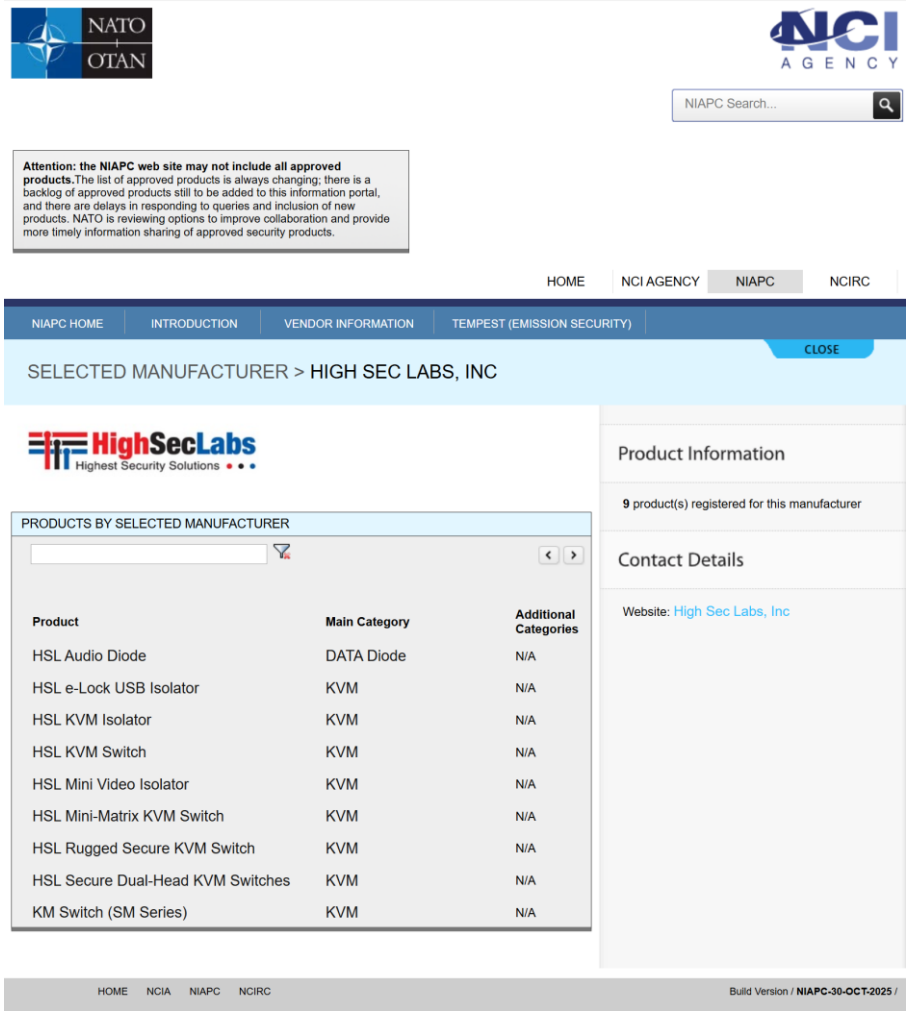
Switch KVM sécurisé

- Certification NIAP PP 4.0 PSD
- Tempest niveau A
- Robustesse : MIL-STD-810G
- Vidéo jusqu'à 4k30
- IP67

Mini matrix et kvm combiners

- Certification NIAP PP 4.0 PSD
- Robustesse : MIL-STD-810G
- Vidéo jusqu'à 4k30
- Unidirectionnalité des signaux
- Multi-vues
- Multi-sources

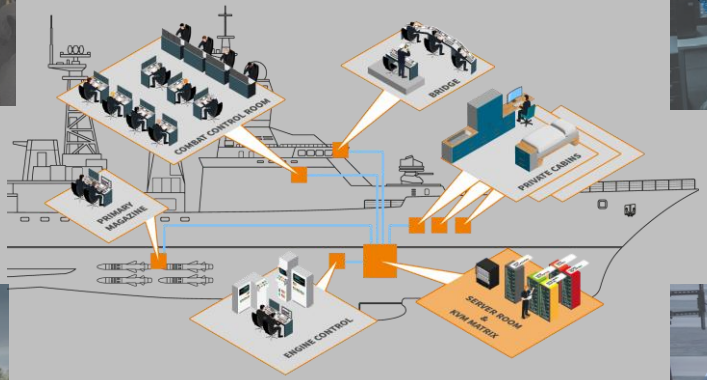
- Validation OTAN
- Produits disponibles sur le site du catalogue NIAPC - OTAN



Cas d’usages typiques

Postes de commandement mobile

Naval



Grands centres C2

Centres de commandement tactique

ATM

Questions

Merci pour votre attention.