



PM  SCADA

CYBERSÉCURITÉ

A grayscale background image of an industrial robotic arm in a factory setting. The arm is positioned on the left side of the frame, reaching towards the center. The background shows various industrial equipment and structures, creating a sense of a manufacturing environment.

PM SCADA

CYBERSÉCURITÉ

TABLE DES MATIÈRES

- ▶ Qui sommes-nous?
- ▶ Notre expertise
- ▶ Qu'est-ce qu'un système SCADA?
- ▶ Quelles sont les vulnérabilités et menaces liées à un système SCADA?
- ▶ Comment mitiger les risques liés aux menaces et vulnérabilités?
- ▶ Questions

PM SCADA **Cybersécurité**

- ▶ 25 ans d'expertise dans la maîtrise des **systèmes de contrôles industriels** et des procédés automatisés (SCADA).
- ▶ 2010 : la firme intègre la cybersécurité à son savoir-faire.
- ▶ 2016 : **acquisition de BCI Bedrich**, chef de file en gouvernance, gestion de risques et conformité NIST, CFAT, NERC, UFC 4-010-01, C2M2 et ISO 27XXX.

L'EXPERTISE DES **SYSTÈMES CRITIQUES**
NE **S'INVENTE PAS.**

FORCES

NOTRE CAPITAL
HUMAIN

NOS
INNOVATIONS

NOS
PARTENAIRES

DÉVELOPPER NOTRE **EXPERTISE**

- ▶ **75 %** de notre chiffre d'affaires réalisé en cybersécurité des installations critiques, les audits et les services de consultation.
- ▶ **25 %** de notre chiffre d'affaires réinvesti dans la recherche et le développement en cybersécurité industrielle afin de soutenir nos opérations pendant les trois prochaines années.

Notre
objectif :

Devenir un
leader de la
sécurité de
l'industrie 4.0

Robert Nastas, associé

Architecte en cybersécurité, systèmes de contrôles industriels



- ▶ Homme d'affaires aguerri, M. Nastas a effectué le chemin inverse du parcours typique des experts en cybersécurité des systèmes des T.O.
- ▶ Il s'est d'abord bâti une carrière notable en automatisation et, ayant toujours eu un intérêt marqué pour la sécurité, il se spécialisa par la suite en cyberdéfense.
- ▶ Fort de sa longue expérience chez Hydro-Québec et unique expert certifié CSSA (*Certified SCADA Security Architect*) à Montréal, M. Nastas est une référence dans les secteurs de l'énergie, du transport et des services publics.
- ▶ Son mantra : comprendre les systèmes dans toute leur complexité avant de les sécuriser.

Youssef Jad, associé

Architecte et expert-conseil en cyberdéfense



- ▶ Maîtrise en science de l'informatique de l'Université de l'Oklahoma.
- ▶ Plus de 15 années en cybersécurité et en conformité des systèmes et infrastructures critiques de télécommunications, ICS/SCADA.
- ▶ Créateur du concept ICDA (*Integrated Cyber Defence Architecture*).
- ▶ M. Jad s'est taillé une place de choix sur l'échiquier international de la cybersécurité en participant à de nombreuses missions pour endiguer les campagnes d'hameçonnage, de rançongiciel, et d'attaques ciblées. Lors de l'attaque massive du 12 mai dernier, Trend Micro USA en a fait son *Task Force Team Lead* mondial pour coordonner la contre-attaque et la cyberintelligence du rançongiciel *WannaCry*, en collaboration avec le DHS et FBI.
- ▶ En plus de faire partie de plusieurs équipes spéciales (Red Team), il conseille les hautes directions de grandes entreprises nationales et multinationales dans la prise de décisions avant d'implanter des solutions intégrées de cyberdéfense pour la protection des infrastructures critiques.

QU'EST-CE QU'UN SYSTÈME **SCADA**?

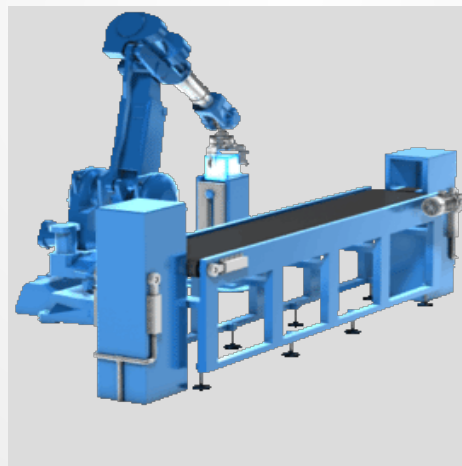
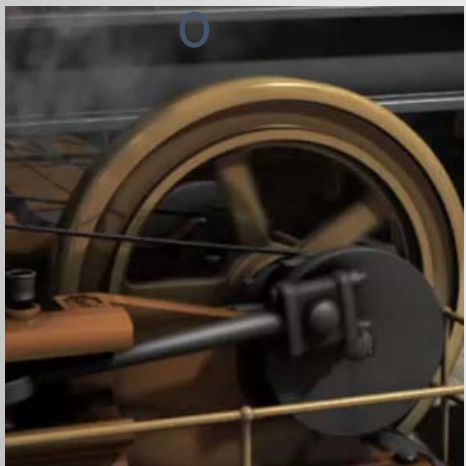
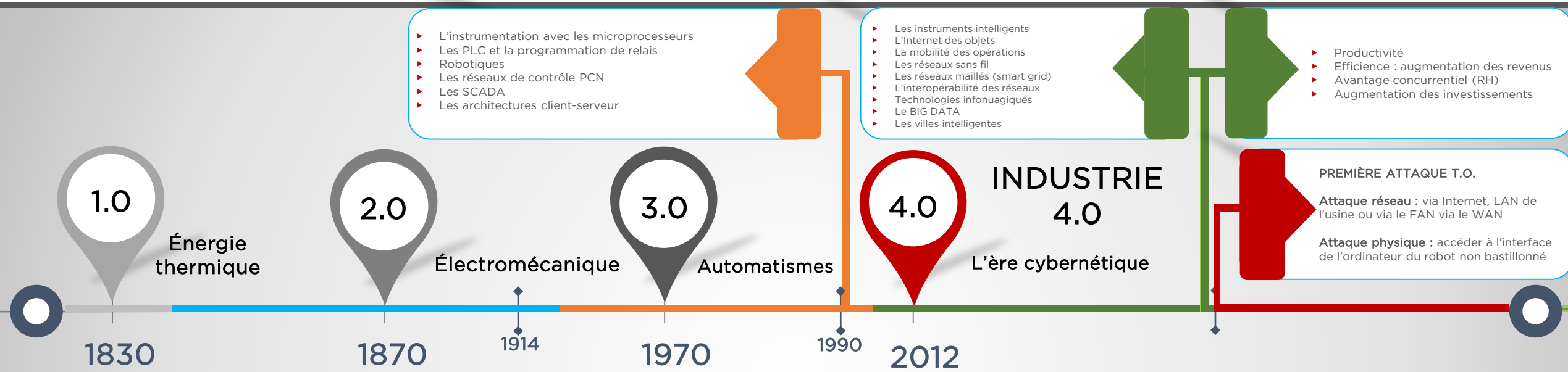
Acronyme : SCADA (*Supervisory Control and Data Acquisition*).

Amalgame de systèmes de contrôles permettant d'automatiser les processus industriels.

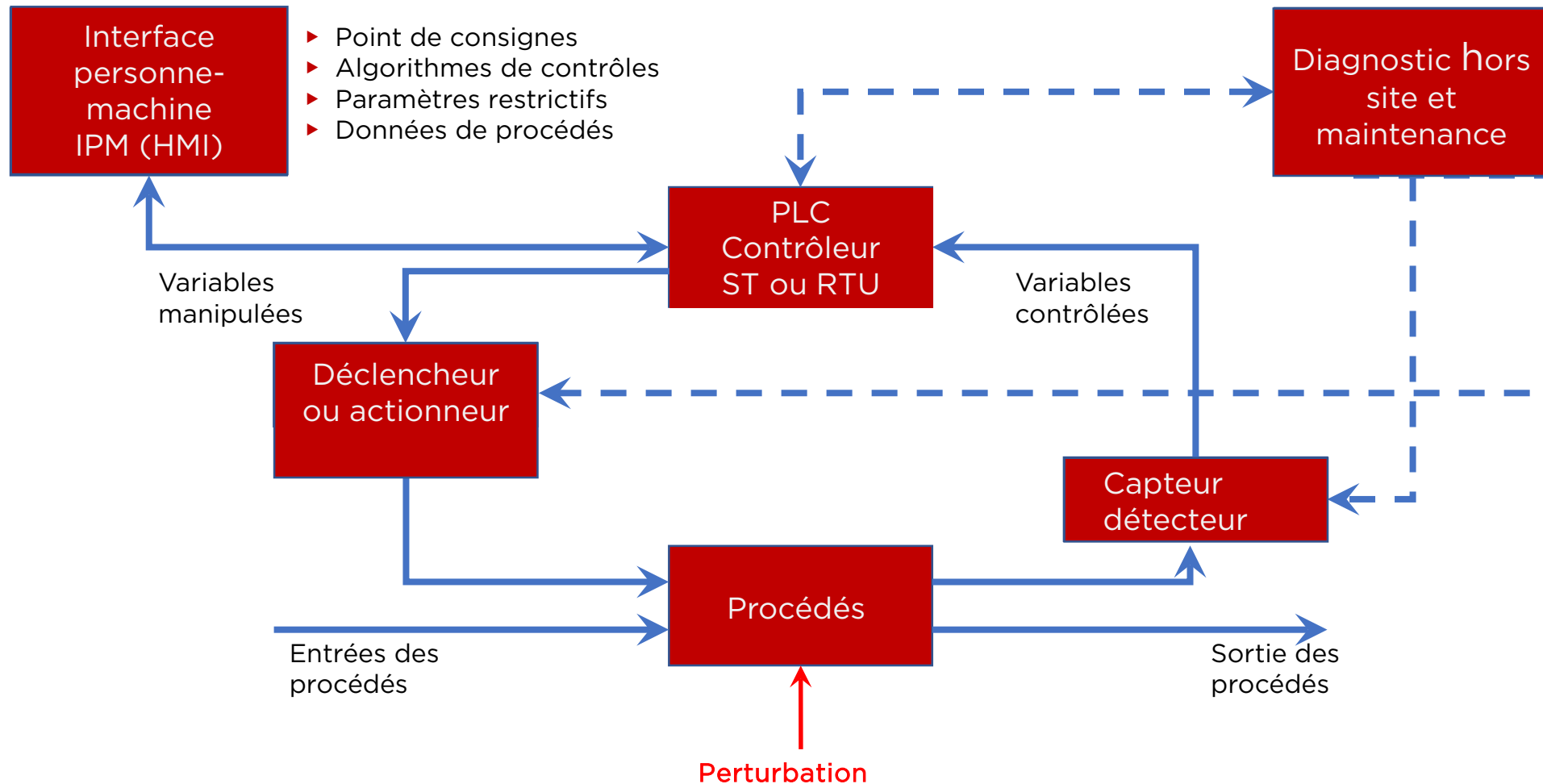
- ▶ SCADA : Système de contrôle et d'acquisition de données automatisées
- ▶ DCS : Systèmes de commandes réparties
- ▶ PLC : Contrôleurs logiques programmables
- ▶ HMI : Interfaces personne-machine
- ▶ IED : Équipement électronique intelligent (IEC 61850) – bientôt des services web
- ▶ Protocoles : DNP3, Modbus, Fieldbus, Controlnet, Devicenet, DH+ et Profinet
- ▶ Et autres configurations de systèmes de commandes de moindre envergure



ÉVOLUTION DE LA RÉVOLUTION INDUSTRIELLE



ENJEUX DES TECHNOLOGIES OPÉRATIONNELLES





MOTIVATIONS POUR **ATTAQUER LES T.O.**

- ▶ Altération ou sabotage des résultats de production;
- ▶ Rançongiciels attaquent les produits modifiés;
- ▶ Dommages physiques;
- ▶ Vol de données sensibles;
- ▶ Hacktivisme.

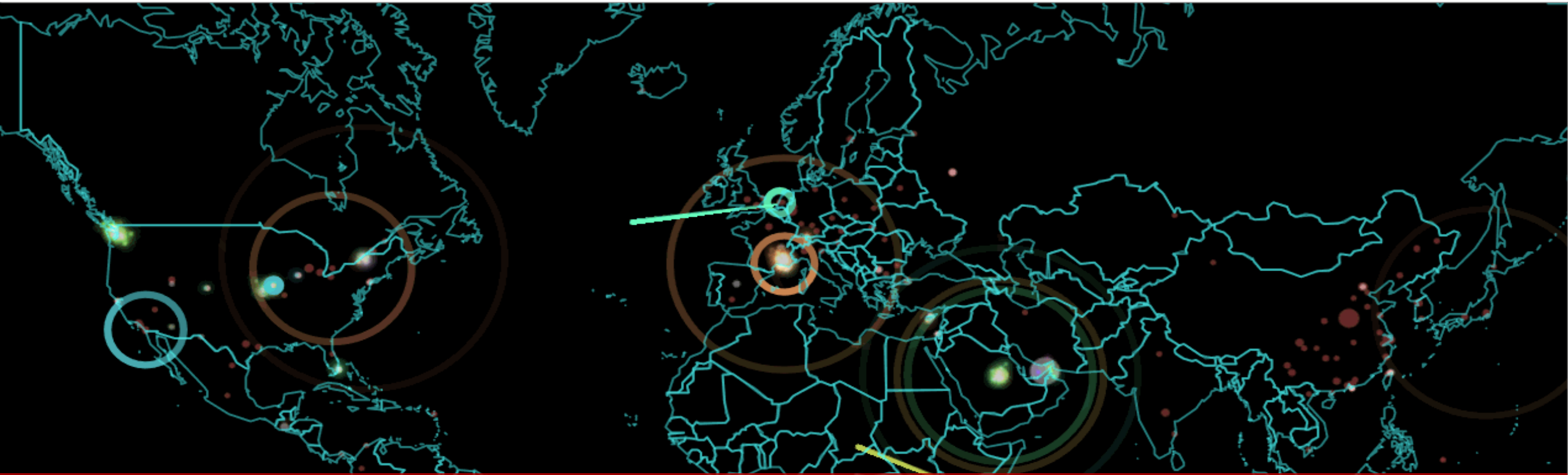


QUESTIONS FACE AUX RISQUES?

- ▶ Que pouvons-nous faire en cas d'incident?
- ▶ Que pourrions-nous faire en cas de perte d'opérations stratégiques?
- ▶ Aurions-nous pu éviter l'incident?
- ▶ Comment catégoriser et traiter les risques?
- ▶ Comment classifier les systèmes?



VULNÉRABILITÉS EN 2017



Depuis janvier 2017, plus de 64 vulnérabilités ont été découvertes dans les systèmes de contrôles impliquant plusieurs manufacturiers reconnus.

TYPES D'ATTAQUES

Classe d'attaque et description	Effet	Impact
Modification du paramètre de contrôle L'attaquant émet des nouvelles consignes qui modifient le comportement du système de contrôle. Exemple : changement de vitesse.	Produits altérés ou défectueux	Sécurité Intégrité Précision
Manipulation des paramètres d'étalonnage L'attaquant change l'étalonnage de façon à donner des résultats inattendus. Exemple : changement de la signalisation.	Robot endommagé	Sécurité Intégrité Précision
Manipulation de la séquence de production L'attaquant manipule le programme d'un des composants de la chaîne de montage afin de produire un défaut de fabrication. Exemple : circuit électronique, carte mère, contrôle pour la vitesse.	Produits altérés ou défectueux	Sécurité Intégrité Précision
Perception erronée des résultats inattendus L'attaquant manipule l'information sur l'état du système de contrôle afin que l'opérateur ne soit pas conscient de son état réel. Exemple : changement du dosage chimique du traitement de l'eau.	Santé de la population	Sécurité Réputation
Altération de l'état du système de contrôle L'attaquant manipule le véritable statut du robot afin que l'opérateur perde son contrôle ou puisse être blessé. Exemple : train sur une mauvaise voie	Blessures corporelles	Sécurité

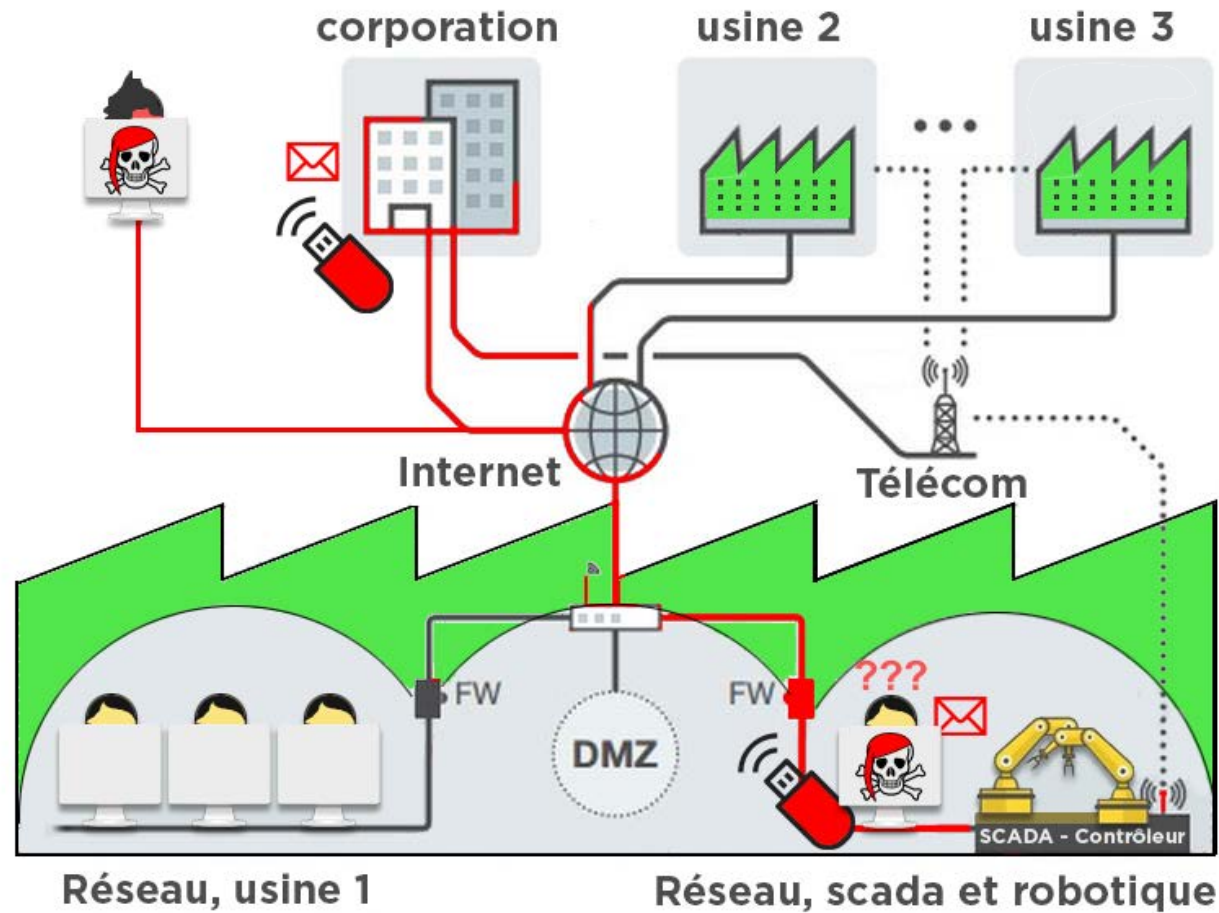
EXEMPLES D'ATTAQUES

Exemple no 1

ICSA-17-129-01 : mise hors service des usines / installations utilisant les produits Siemens communiquant en PROFINET (DCP).

Exemple no 2

ICSA-17-094-04 : prise de contrôle ou infection à distance des routeurs industriels Rockwell Automation Stratix 5900.



COMMENT MITIGER LES RISQUES?

- ▶ La prévention a un ROI plus élevé que la réaction à la suite d'un incident majeur.
- ▶ Collaborer avec les fabricants et les fournisseurs pour s'assurer que la sécurité de base est bien intégrée.
- ▶ Évaluer le niveau de risques avec des normes reconnues.
- ▶ Auditer la sécurité et l'architecture industrielle de cyberdéfense.
- ▶ Déployer une architecture de défense intégrée (ICDA) contre les attaques avancées de type APT, rançongiciels.
- ▶ Valider fréquemment le niveau de sécurité par des tests d'intrusion.



COMMENT MITIGER LES RISQUES?

- ▶ Renforcer l'authentification avec une solution multi-facteurs.
- ▶ Obscurcir au besoin les zones critiques.
- ▶ Être impliqué dans les communautés dédiées à la cybersécurité partageant l'information en temps réel sur les menaces.
- ▶ Auditer l'efficiency et l'efficacité des contrôles de sécurité et les ajuster selon les déficiences trouvées.
- ▶ Être préparé aux cyberattaques parrainées par des organisations avec des budgets illimités.



The background of the slide is a grayscale photograph of a renewable energy facility. In the foreground, there are several rows of solar panels tilted at an angle. In the background, several wind turbines are visible against a dark sky.

MERCI

Questions?

Nous sommes ici pour VOUS!

PM▲SCADA
CYBERSÉCURITÉ