Opportunités et limites de la technologie moderne dans le contrôle-commande des remontées mécaniques

Avril 2016

Opportunities and limitations of modern technologies in control systems for ropeways

Accès à distance et sécurité des données associées

Avril 2016

Remote access and associated data security

Fabrice JACQUIER
Directeur Technique
Technical Director

Avril 2016

SEMER
INGÉNIERIE ÉLECTRIQUE

Sommaire

La sécurité des systèmes industriels (1/4)

La sécurité des systèmes industriels peut être décomposée en 3 points

- Sécurité physique (gestion des accès)
  - Poste de garde
  - Accès par badge, clef…

- Sécurité fonctionnelle (sûreté de fonctionnement) ISO 12100
  - Analyse de risques
  - Analyse des défaillances

- Sécurité des systèmes d'informations (cybersecurité) ISO 27000
  - Au niveau OT : Operational Techonology
  - Au niveau IT : Information Technology

La sécurité des systèmes industriels (2/4)

- Appliquer les notions de sûreté de fonctionnement aux systèmes d'information
  - Evaluer le niveau de risque d'une installation
  - Prévoir les barrières technologiques et d'utilisation visant à réduire le risque
  - Maintenir un niveau de risque acceptable dans le temps

La sécurité des systèmes industriels (3/4)

Sécurité fonctionnelle

ISO 12100 CEI 61508 ISO 13849	Cycle en V	Choix du système	Choix de composants certifiés (SIL)	Maintien en condition
		• Fonctions de sécurité	**S**afety **I**ntegrity **L**evel	• Plan de maintenance • Obsolescence • Choix personnel

Cybersécurité

ISO 27000 ISO 27001/2 CEI 62443	Cycle en V	Choix du système	Choix de composants éprouvés (CSPN)	Maintien en condition
		• Architecture système	**C**ertificat **S**écurité **P**remier **N**iveau	• Plan de maintenance • Obsolescence • Choix personnel

La sécurité des systèmes industriels (4/4)

- En sécurité fonctionnelle, la méthodologie est portée par :
  - Analyse Préliminaire de Risque (APR), HAZard OPerability (HAZOP)
  - Analyse des Modes de Défaillance de leur Effets et de leur Criticité (AMDEC)
  - …
- En cybersécurité, le méthodologie est portée par :
  - MEHARI : méthodologie d'analyse, d'évaluation et de gestion des risques liés à l'information et à son utilisation.
  - EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité
  - …

La cybersécurité des systèmes industriels (1/10)

- Domaines industriels :
  - Production d'électricité
  - Chimie
  - Gestion de l'eau
  - Alimentation
  - Communications électroniques, audiovisuel et information
  - Manufacture,
  - Transports : Ferré, Aviation, … Transport par câble

Dans la suite de cette présentation, cette couleur bleue permettra d'identifier comment sont appliqués les différents principes, règles ou méthodes au domaine du transport par câble (installations équipées d'architecture de contrôle-commande dites modernes).

Dans tous ces domaines, certains systèmes sont particulièrement importants (fort impact en cas d'interruption de service). Ils sont appelés **SIIV** : **S**ystèmes d'**I**nformation d'**I**mportance **V**itale. C'est rarement le cas des installations de transport par câble.

La cybersécurité des systèmes industriels (2/10)

- Quelques notions

  - Les critères de sécurité sont au nombre de 4 : la disponibilité, l'intégrité, la confidentialité et la traçabilité
    - Pour le transport par câble on peut définir un ordre d'importance pour ces critères :

    1- Intégrité, 2- Disponibilité, 3- Traçabilité, 4- Confidentialité

  - Biens essentiels : processus portés par le système industriel étudié dont l'affectation pourrait impliquer des dommages pour les personnes, l'environnement ou engendrer des gênes importantes suite à l'interruption de service
    - Pour le transport par câble : maitrise de la traction, maitrise du freinage, …, desservir une zone isolée, …

La cybersécurité des systèmes industriels (3/10)

- Quelques notions
  - Biens supports : les composants, les sous-systèmes du système étudié
    - Pour le transport par câble

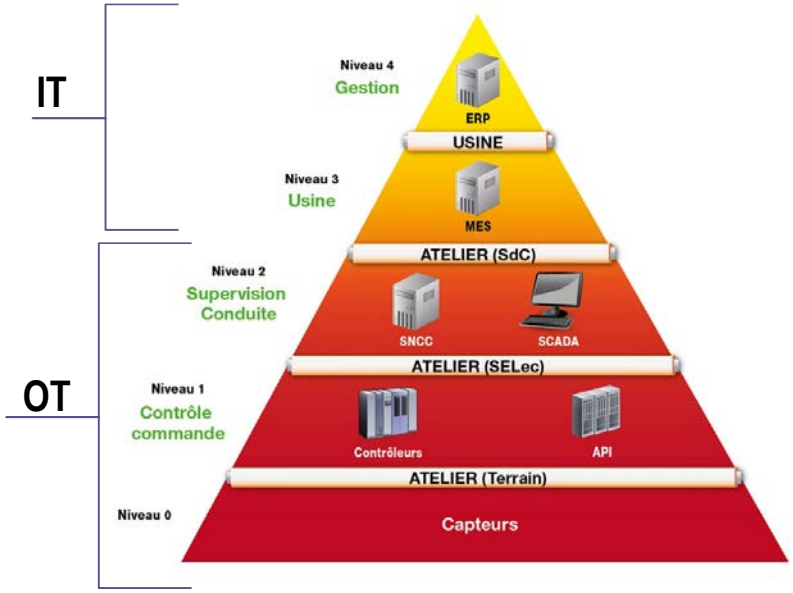
      - Les architectures de contrôle-commande : automates, pupitres, consoles de programmation…

      - Le télé-service regroupant sous une même dénomination : télémaintenance, télédiagnostic, télégestion…

      - Les systèmes de communication sans fil avec les véhicules

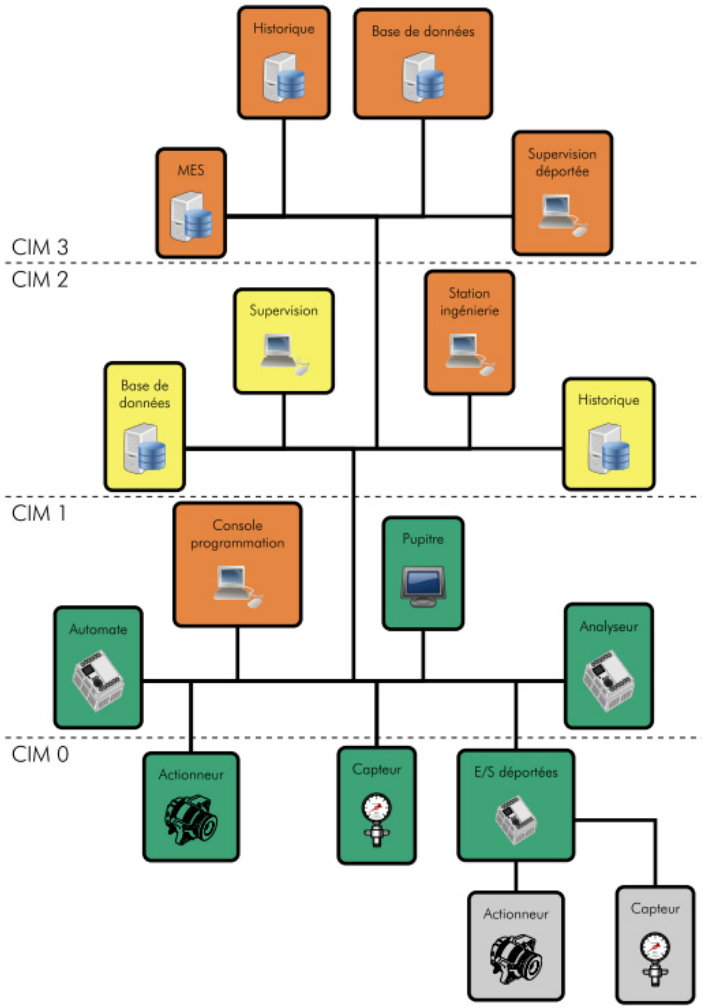
La cybersécurité des systèmes industriels (4/10)

- Fonctionnalité : classification coïncidant essentiellement avec les différentes couches habituellement utilisées dans le modèle de «production intégrée par ordinateur» (CIM)
  - CIM 4 planification, gestion des ressources (ERP)
  - CIM 3 système d'exécution des fabrications (MES)
  - CIM 2 supervision (SCADA)
  - CIM 1 automates (PLC) et analyseurs
  - CIM 0 capteurs et actionneurs non communicants



OT : **O**perational **T**echonology
IT : **I**nformation **T**echnology

La cybersécurité des systèmes industriels (5/10)



Fonctionnalité 3 :
Système de suivi d'exploitation et de maintenance

Fonctionnalité 2 :
Supervision globale du parc d'installations

Fonctionnalité 1 :
Contrôle commande de l'installation
y compris l'Interface Homme Machine locale

La cybersécurité des systèmes industriels (6/10)

Fonctionnalité 1 :
Contrôle commande de l'installation
y compris l'Interface Homme Machine locale

Hier …

Une évolution importante des architectures au fil des années …

Aujourd'hui …

La cybersécurité des systèmes industriels (7/10)

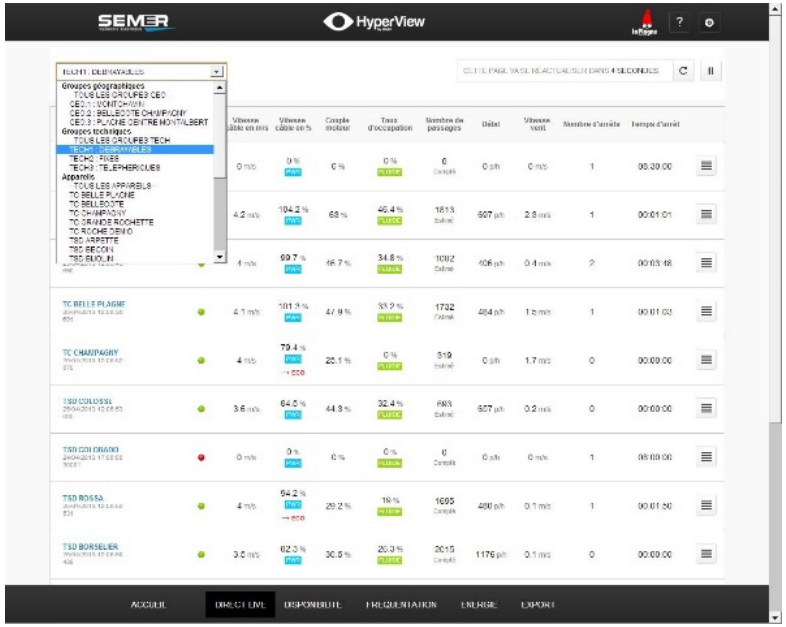
Fonctionnalité 2 :

Supervision globale du parc d'installations

Une nécessité pour les opérateurs …

Fonctionnalité 3 :

Système de suivi d'exploitation et de maintenance



LA base de TOUTES les données !

La cybersécurité des systèmes industriels (8/10)

- Connectivité :
  - Connectivité 1 : Système industriel isolé
  - Connectivité 2 : Système industriel connecté à un système d'information de gestion
  - Connectivité 3 : Système industriel utilisant de la technologie sans fil
  - Connectivité 4 : Système industriel distribué avec infrastructure privée ou permettant des opérations depuis l'extérieur (Virtual Private Network)
  - Connectivité 5 : Système industriel distribué avec infrastructure publique

La cybersécurité des systèmes industriels (9/10)

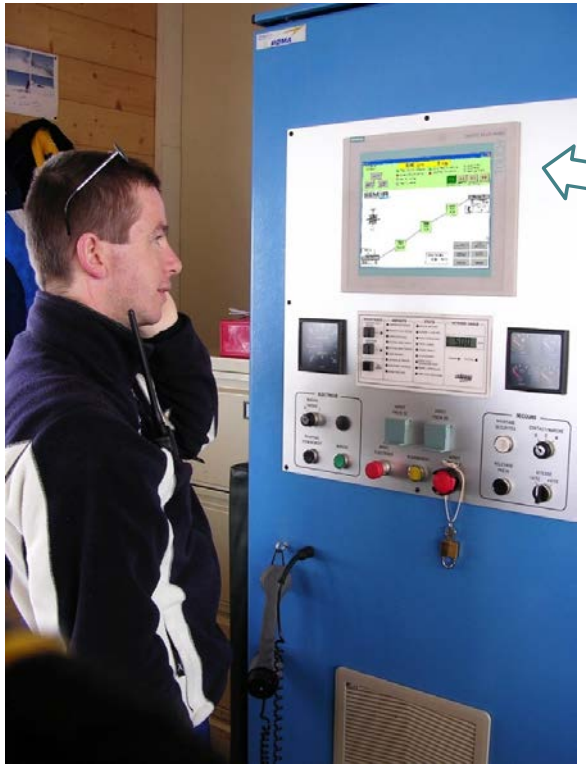
Connectivité 3 : Utilisation de différentes technologies sans fils

Pour de plus en plus de fonctionnalités embarquées

La cybersécurité des systèmes industriels (10/10)

Connectivité 4 :

Utilisation d'un Virtual Private Network (VPN) pour le télé-service

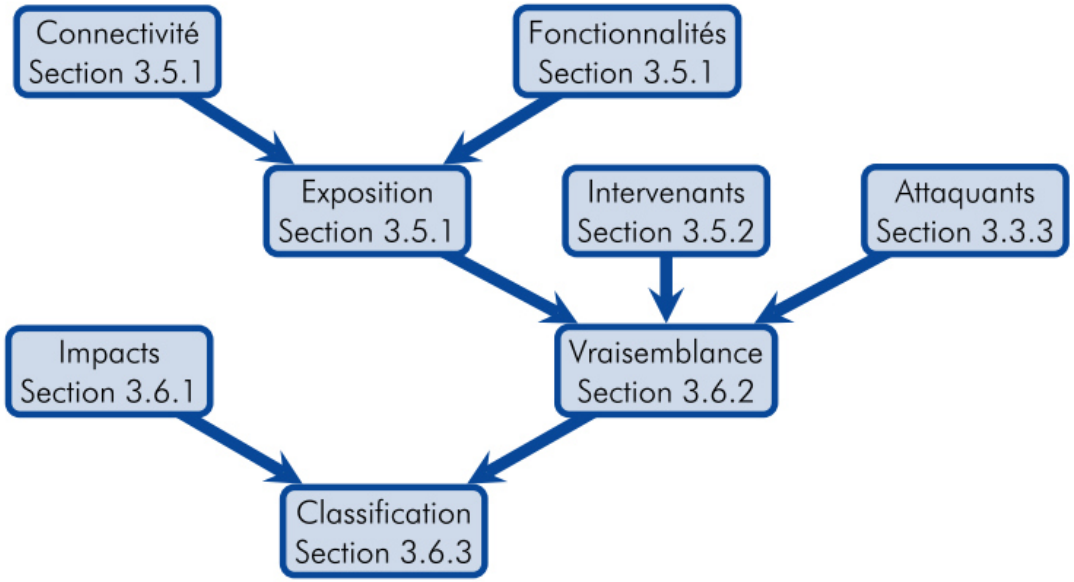


Report d'écran

Pour un support réactif et efficace

Classification d'une installation de transport par câble (1/8)

Méthode de classification et mesures principales
Version 1.0 - Janvier 2014



ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

Classification d'une installation de transport par câble (2/8)

- Exposition : résultante de la fonctionnalité et de la connectivité

F3	Exposition 3	Exposition 3	Exposition 4	Exposition 4	Exposition 5
F2	Exposition 2	Exposition 2	Exposition 3	Exposition 4	Exposition 5
F1	Exposition 1	Exposition 2	Exposition 3	Exposition 4	Exposition 5
Fonct./Conn.	C1	C2	C3	C4	C5

  - Fonctionnalité : niveau pouvant atteindre F3
  - Connectivité : niveau pouvant atteindre C4
  - Le niveau d'exposition maximal résultant est le **niveau 4**

Classification d'une installation de transport par câble (3/8)

- Intervenant : personnel habilité ou non ayant une interaction avec le système
  - Intervenants 1 : autorisés, habilités et contrôlés. Une intervention non-autorisée n'est pas possible
  - Intervenants 2 : autorisés et habilités. Une intervention non-autorisée n'est pas possible
  - Intervenants 3 : autorisés Il n'y a pas d'exigence particulière sur les intervenants autorisés mais une intervention non-autorisée n'est pas possible.
  - Intervenants 4 : non-autorisés Cette catégorie contient tous les systèmes industriels dans lesquels une intervention non-autorisée est possible

Classification d'une installation de transport par câble (4/8)

- Attaquant : personne ou entité réalisant une intrusion dans le système

Niveau	Qualificatif	Description / Exemple
1	Non ciblé	Virus, robots
2	Hobbyiste	Personnes avec des moyens très limités, pas nécessairement de volonté de nuire
3	Attaquant Isolé ***(niveau recommandé par l'ANSSI)***	Personne ou organisme avec des moyens limités mais avec une certaine détermination (employé licencié, par exemple).
4	Organisation privée	Organisme aux moyens conséquents (terrorisme, concurrence déloyale, par exemple)
5	Organisation étatique	Organisme aux moyens illimités et à la détermination très forte

Attaques non ciblées (Virus)

Hobbyiste

Attaquant niveau étatique

Attaquant isolé

Organisation privée

Classification d'une installation de transport par câble (5/8)

- Vraisemblance : Estimation de la possibilité qu'un scénario de menace ou un risque, se produise

  où V est la vraisemblance, E l'exposition, I les intervenants
  et A le niveau de l'attaquant.
  L'opérateur mathématique [.] dénote la partie entière supérieure

$$V = E + \left\lceil \frac{A + I - 2}{2} \right\rceil$$

- Dans le cas d'une installation de transport par câble :
  - Exposition E = 4
  - Attaquant A = 3
  - Intervenant I = 3

La vraisemblance d'une attaque est donc de : 6

Classification d'une installation de transport par câble (6/8)

- Une fois la vraisemblance quantifiée, il faut estimer l'impact pour au final déterminer la classe
- Gravité : impacts humains, environnementaux, consécutif à l'arrêt du service

Niveau	Qualificatif
1	Faible
2	Mineur
3	Modéré
4	Majeur
5	Catastrophique

Classification d'une installation de transport par câble (7/8)

- Gravité : impacts humains, environnementaux, consécutif à l'arrêt du service
  - Compte tenu de la technologie, l'impact humain sera très probablement faible :

    - Nombre important de Fonctions de Sécurité Fondamentales gérées par un automate *Failsafe*,

    - Accès au frein de sécurité toujours possible pour l'opérateur via une chaine en logique câblée et/ou une vanne hydraulique (dispositifs indépendants de l'automate)
  - Compte tenu du caractère propre du transport par câble, l'impact environnemental sera là-aussi faible.
  - Compte tenu du niveau de service requis (loisirs ou possibilité de rejoindre la zone desservie via un autre mode de transport), l'impact consécutif à l'arrêt du service sera également relativement faible.
- **Le niveau retenu est donc de : 1**

Classification d'une installation de transport par câble (8/8)

- Classes de cybersécurité

5+	Classe 2	Classe 2	Classe 3	Classe 3
4	Classe 2	Classe 2	Classe 2	Classe 3
3	Classe 1	Classe 2	Classe 2	Classe 2
2	Classe 1	Classe 1	Classe 2	Classe 2
1	Classe 1	Classe 1	Classe 1	Classe 1
Impact/Vraisemblance	1	2	3	4+

Dans le cas d'une installation de transport par câble, où la vraisemblance est forte (6) mais l'impact faible (1), la classe de cybersécurité est donc la **classe 1** .

- *Classe 1 : systèmes industriels pour lesquels le risque ou l'impact d'une attaque est faible*
- *Classe 2 : systèmes industriels pour lesquels le risque ou l'impact d'une attaque est significatif*
- *Classe 3 : systèmes industriels pour lesquels le risque ou l'impact d'une attaque est critique. Ce sont les OIV Opérateur d'Importance Vitale (ex : EDF, RATP)*

Quelles mesures pour une installation de transport par câble? (1/4)

Liste des bonnes pratiques (recommandations vu que Classe 1) :

- BP01 : Contrôle d'accès physique aux équipements et aux bus de terrain
- BP02 : Cloisonnement des réseaux
- BP03: Gestion des médias amovibles
- BP04 : Gestion des comptes (accès logique, authentification)
- BP05 : Durcissement des configurations
- BP06 : Gestion des journaux d'événements et d'alarmes
- BP07 : Gestion des configurations

Quelles mesures pour une installation de transport par câble? (2/4)

Suite et fin des bonnes pratiques (recommandations vu que Classe 1) :

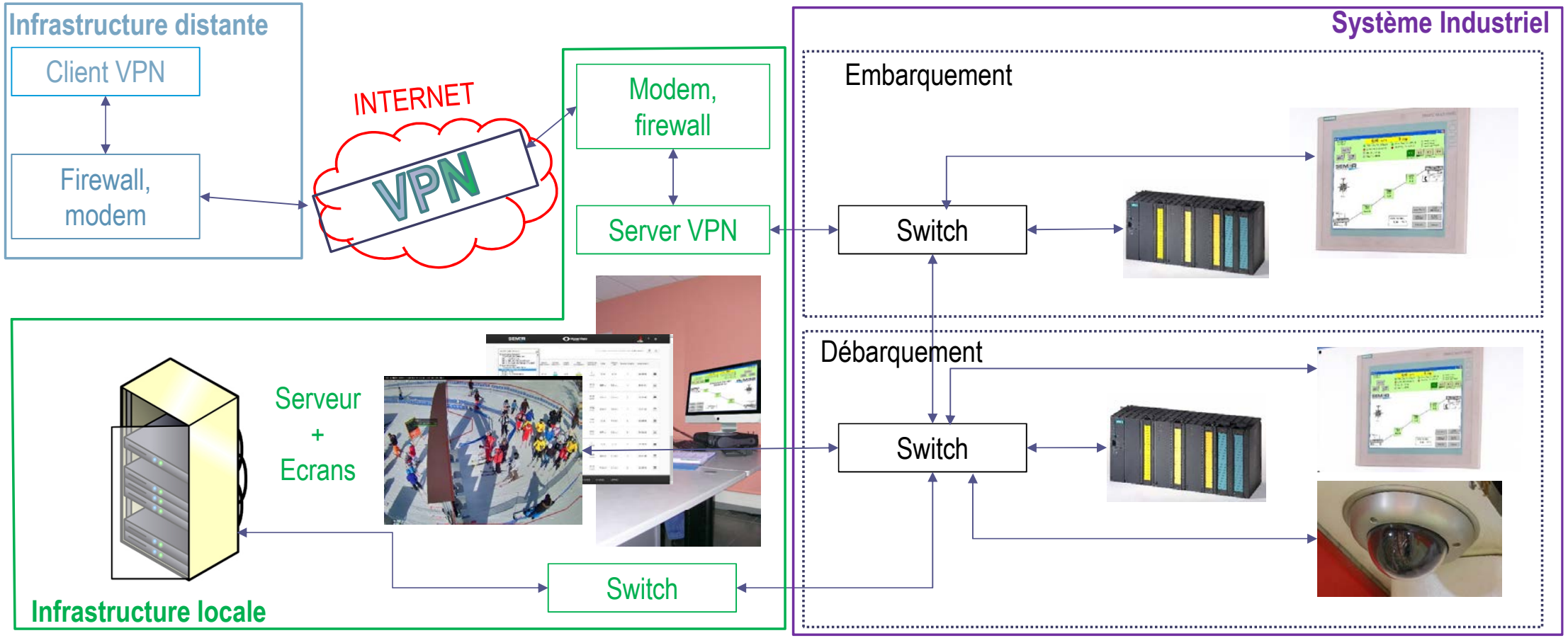
- BP08 : Sauvegardes / restaurations
- BP09 : Documentation
- BP10 : Protection antivirale (antivirus, whitelisting)
- BP11 : Mise à jour des correctifs (planification)
- BP12 : Protection des automates (PLC)
- BP13 : Stations d'ingénierie, postes de développement

Quelles mesures pour une installation de transport par câble? (3/4)

- En tant que Constructeur, notre contribution concerne la partie technique, avec :
  - L'utilisation de produits éprouvés :
    - SIEMENS met à disposition un suivi des vulnérabilités pour ses produits (informations importantes à destination des intégrateurs et des opérateurs)
    - SIEMENS participe activement aux groupes de travail de l'ANSSI (agence très active sur les sujets liés à la cybersécurité des systèmes industriels)
  - L'utilisation d'outils de programmation dédiés maintenus régulièrement à jour au niveau :
    - De la couche Windows : antivirus, ...
    - De l'atelier de programmation : STEP7 ou TIA Portal (compilateurs intégrés), …

Quelles mesures pour une installation de transport par câble? (4/4)

- Notre contribution concerne également la partie organisationnelle, avec :
  - L'utilisation systématique d'un VPN pour les connexions à distance



A retenir (1/3)

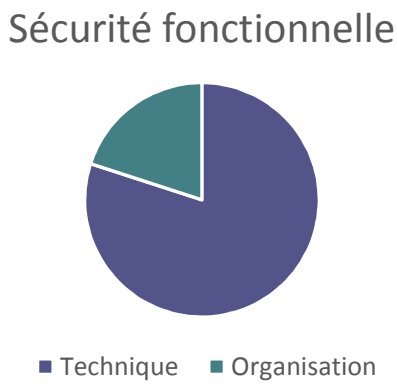
- Les installations contemporaines sont définitivement plus exposées que les anciennes, compte tenu :

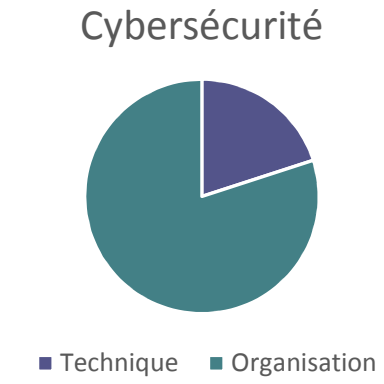
- De leur plus grande connectivité
- Du spectre toujours plus large de leurs fonctionnalités

A retenir (2/3)

- Les moyens de lutte et de prévention restent proches de ceux connus en sécurité fonctionnelle, cependant la répartition n'est pas la même.
  - En sécurité fonctionnelle, les risques engendrés par la machine sont couverts essentiellement par des barrières technologiques

  - En cybersécurité, les risques engendrés par malveillance (externe ou interne) sont couverts essentiellement par des mesures organisationnelles : défense en profondeur, entité dédiée, …





A retenir (3/3)

- La sécurité fonctionnelle peut toutefois constituer un élément de défense contre les cyber-attaques, si elle s'appuie sur une approche diversitaire :
  - Logique programmée + Logique câblée pour les fonctions de sécurité fondamentales,
  - Présence continue d'un opérateur en lien physique avec le système industriel.
- Sur une installation de transport par câble, une accélération incontrôlée / incontrôlable (suite par exemple à une attaque type Stuxnet …) aurait très probablement conduit à une réaction de l'opérateur (réaction restée efficace grâce à la chaine en logique câblée) et/ou au déclenchement d'une survitesse mécanique …

Libération MONDE

POLITIQUE SOCIÉTÉ MONDE ÉCONOMIE CULTURE NEXT IDÉES VIDÉO PHOTO

Un ver informatique dans le nucléaire iranien

DELPHINE MATTHIEUSSENT JÉRUSALEM, DE NOTRE CORRESPONDANTE ET JEAN-PIERRE PERRIN 29 SEPTEMBRE 2010 À 00:00

Des installations sur le site iranien gazier de South Pars en juillet 2010. (© AFP Atta Kenare)

Le virus Stuxnet a infesté un nombre important d'ordinateurs contrôlant des infrastructures du pays, notamment le centre de recherche atomique de Natanz. Téhéran soupçonne les Etats-Unis et Israël.

Merci de votre attention

Thank you for your attention

Fabrice JACQUIER
Directeur Technique
Technical Director

Avril 2016

SEMER
INGÉNIERIE ÉLECTRIQUE