Introduction à la cybersécurité des systèmes industriels

Culture Sciences de l'Ingénieur

La Revue 3E.I

Édité le 15/02/2024

école normale supérieure paris-saclay

Maxime SECHEHAYE[1], Anthony JUTON[2]

[1] *Etudiant en M2 à l'ENS Paris-Saclay – DER Nikola Tesla*

[2] *Professeur agrégé à l'ENS Paris-Saclay – DER Nikola Tesla*

Cette ressource fait partie du N°111 de La Revue 3EI de janvier 2024.

Cette ressource introduit le dossier sur la cybersécurité en définissant ses objectifs, les principes fondamentaux de la cybersécurité ainsi que ses enjeux.

D'après le dictionnaire *Le Robert*, la cybersécurité désigne « l'ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un État, d'une entreprise, etc. ». Aborder la cybersécurité dans son ensemble est donc une tâche colossale qui nécessite des connaissances et des compétences dans de très nombreux domaines : économie, diplomatie, droit, sociologie, renseignement, etc. Se former en cybersécurité, ce n'est donc pas uniquement apprendre de bonnes pratiques en informatique, le champ d'application est bien plus vaste.

Cette ressource définit donc les limites de ce dossier qui ne se veut pas exhaustif, puis précise le public visé, avant de présenter quelques attaques récentes liées à des problématiques de cybersécurité pour commencer à sensibiliser le lecteur.

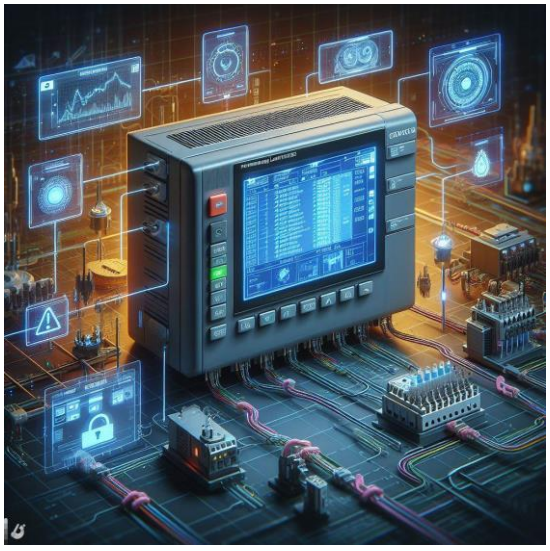

Figure 1 : Cybersécurité des systèmes automatisés industriels, vue par Microsoft Designer / DALL-E3

1 - Les champs de la cybersécurité couverts par ce dossier

Comme beaucoup des disciplines informatiques, la cybersécurité des systèmes informatiques est un sujet largement traité avec des ressources de qualité accessibles librement et destinées à des informaticiens.

La cybersécurité des systèmes industriels est à l'intersection entre la cybersécurité des systèmes informatiques et le champ disciplinaire nommé en France « informatique industrielle » qui regroupe l'automatisme industriel et l'informatique embarquée. Pour le premier, l'« industrie 4.0 » et pour le second, l'« internet des objets », sont deux expressions (aux contours peu précis) très utilisées qui traduisent la tendance à la « connexion de tout, toujours et partout ». Ceci élargit la surface vulnérable des systèmes industriels et amène à une augmentation du nombre des attaques. Ces systèmes, automatisés, embarqués ou IoT, ont de plus une durée de vie importante allant souvent au-delà de la période couverte par les mises à jour de sécurité (quand elles sont faites...).

Cela implique une meilleure formation des acteurs, notamment ceux issus de l'informatique industrielle, à la cybersécurité, d'où notamment l'évolution du BTS Systèmes Numériques en BTS Cybersécurité, Informatique et réseaux, Électronique (CIEL) et l'introduction de la cybersécurité dans le programme national des BUT GEII et R&T (pour lequel existe désormais un parcours cybersécurité).

Accompagnant ce mouvement, ce dossier vise à proposer aux enseignants d'informatique industrielle des ressources théoriques, des exemples de travaux pratiques et des témoignages d'industriels, organisés en trois domaines, pas complètement indépendants, après une partie introductive :

- Cybersécurité des systèmes automatisés industriels,
- Cybersécurité des objets connectés,
- Cybersécurité des systèmes embarqués (essentiellement automobiles).

Pour chacun de ces ensembles de systèmes, le dossier s'intéresse essentiellement aux vulnérabilités et protections au niveau réseau, en restant dans le cadre des compétences attendues d'un technicien ou ingénieur en GEII.

En complément, une dernière partie présentera une introduction à la cybersécurité au niveau matériel des systèmes informatiques, problématique commune à tous les domaines de l'informatique.

2 - À qui s'adresse ce dossier ?

Ce dossier s'adresse à la fois aux enseignants, aux techniciens et aux ingénieurs en ingénierie électrique ou en informatique embarquée.

Par sa grande complexité, abordée dans le paragraphe introductif, la cybersécurité est un domaine d'experts. Ce dossier n'a pas vocation à former des experts en cybersécurité. Il se propose au contraire de sensibiliser les acteurs travaillant dans des domaines concernés par la cybersécurité pour qu'ils puissent prendre en compte ces problématiques lors de la conception de systèmes.

En effet, la prise en compte des problématiques de cybersécurité dès la phase de conception d'un système avec l'application des bonnes pratiques et des solutions existantes est le plus souvent suffisante pour se protéger des attaques classiques réalisées par des individus malveillants isolés.

3 - Exemples d'attaques liées à des problématiques de cybersécurité

Cette partie présente trois exemples, issus des fiches d'incidents [1] publiées périodiquement par le Clusif, association française de promotion de la cybersécurité.

3.1 - Systèmes automatisés – Prise de contrôle du système de production d'une aciérie

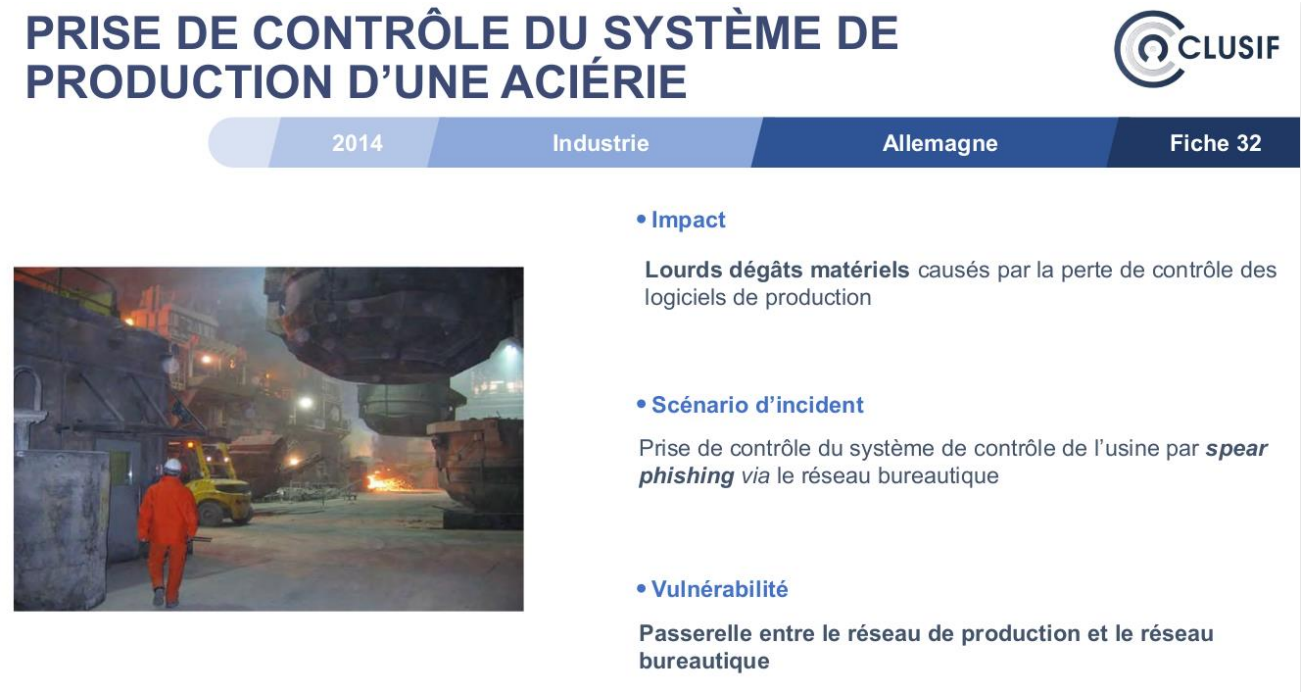

Figure 2 : fiche 32 [1] : Prise de contrôle du système de production d'une aciérie

Cette fiche a été choisie car représentative des risques en cybersécurité des systèmes industriels et des conséquences importantes. L'intrusion a eu lieu par une campagne de mails frauduleux (*phishing*) et a permis de s'introduire sur le réseau de bureautique. De ce réseau bureautique, les hackers ont eu accès au réseau industriel pour prendre les commandes des systèmes de production et désactiver les mises en sécurité d'un haut fourneau jusqu'à provoquer de lourds dégâts.

La fiche rédigée par le Clusif à propos de cet incident propose les contre-mesures suivantes :

- Sensibilisation des agents aux méthodes d'attaque par *spear phishing* ;
- Restriction des droits accordés aux profils d'agent sur le réseau et les systèmes, de façon à détecter, voire empêcher toute action suspecte (prise de contrôle de systèmes, de terminaux…) ;
- Cloisonnement des réseaux de bureautique exposés aux attaques et aux intrusions, et des réseaux de contrôle des systèmes de production ;
- Mise en place de mécanismes de sûreté indépendants du système de conduite.

Parmi les fiches Clusif, un nombre important relate des attaques sur des systèmes industriels (exemple : empoisonnement de l'eau dans une usine de production d'eau, fiche 19) ou énergétiques (exemple : Black Energy, fiche 4 – coupure de l'électricité en Ukraine). La majeure partie pourrait être évitée par une bonne application des règles de cybersécurité abordées dans la partie 1 du dossier, consacrée aux systèmes automatisés industriels.

Quelques attaques sont le résultat d'un affrontement entre puissances étrangères, notamment l'attaque Stuxnet (fiche 36) qui a permis en 2010 aux services secrets israéliens de saboter les centrifugeuses iraniennes enrichissant l'uranium.

L'attaque Stuxnet en 2010 a révélé la vulnérabilité des systèmes automatisés et permis de prendre conscience des risques encourus et de la nécessité de mettre en œuvre une politique de cybersécurité pour les systèmes industriels également. Les nombreuses attaques qui ont suivi, comme celle présentée ici, mettent en évidence la lente formation des automaticiens à la cybersécurité et la longue marche vers la sécurisation de tous les équipements, pour certains en fonctionnement depuis longtemps.

3.2 - Objets connectés – Attaque sur une pompe à insuline

Quelques fiches s'intéressent aux objets connectés, notamment la fiche 41 qui présente la prise de contrôle à distance d'une pompe à insuline.

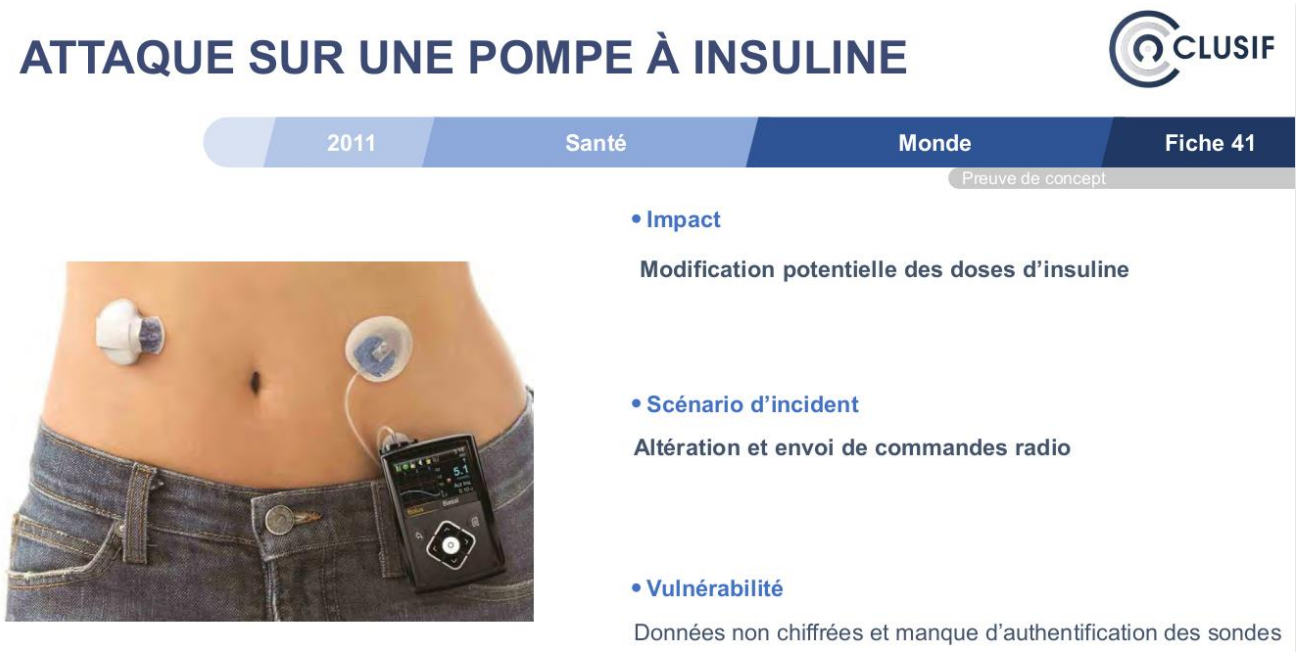

Figure 3 : Fiche 41 [1] : Attaque sur une pompe à insuline

Après l'analyse de la documentation constructeur (manuel d'utilisation, analyse des brevets, numéro de série de l'appareil…), un chercheur est parvenu à intercepter les communications échangées entre les capteurs et sa pompe à insuline et établir la liste des codes de commande utiles de l'équipement.

Le chercheur a alors imaginé plusieurs scénarios d'attaque : rejeu (l'entité malveillante intercepte puis réitère une transmission de données valide) de valeurs transmises à la pompe par les sondes, envoi de commandes forgées directement à la pompe (accès physique requis pour connaître le numéro de série nécessaire à l'envoi).

La fiche à propos de cet incident propose les contre-mesures suivantes :

- Forcer l'authentification mutuelle des sondes et pompes à insuline ;
- Chiffrer les signaux échangés ;
- En conclusion : intégrer la sécurité dans la phase de conception de ces objets.

Cette attaque met en valeur le manque de mesures de sécurité lors de la conception d'objets connectés. Les objets, parfois d'un coût peu élevé, sont conçus par des électroniciens qui valident le bon fonctionnement sans toujours connaître les attaques que leur dispositif risque d'affronter, parfois dans plusieurs années.

La fiche 22 du Clusif montre comment un adolescent a pu reproduire une télécommande d'aiguillage de Tramway. Martin Hron, chercheur en sécurité chez Avast, a publié pour sa part un article présentant la possibilité d'attaquer une machine à café connectée [3]. Les attaques peuvent porter uniquement sur la machine (dérèglement dangereux de la machine pouvant mener à sa destruction si une rançon n'est pas payée) mais aussi sur le réseau domestique (la machine à café sert de porte d'entrée au réseau).

La prise de contrôle d'objets connectés peu sécurisés (car peu chers et peu dangereux) permet à des hackers de lancer depuis ces milliers d'objets contrôlés des attaques DDoS (Distributed Denial of Service) en saturant un serveur de requêtes. Par exemple, le 21 octobre 2016, le malware Mirai, après avoir infecté des dizaines de millions d'objets connectés (notamment des caméras de surveillance de bébés, ce qui a participé à son succès médiatique) a rendu indisponible le gestionnaire de noms de domaine américain Dyn, ce qui a mis hors connexion les sites de clients importants comme Twitter, Spotify, et PayPal.

Une fois les objets connectés dans les mains de particuliers, non enregistrés et non visés par les attaques, il est très difficile de faire procéder à leur mise à jour, ce qui contribue à expliquer que Mirai refait parfois parler de lui.

La partie 2 du dossier, consacrée aux objets connectés, présente les dispositifs de cybersécurité sur les principaux réseaux IoT et une application pratique Bluetooth vulnérable et sa sécurisation.

3.3 - Systèmes embarqués – Prise de contrôle d'un véhicule automobile

En 2015, les chercheurs américains Chris Valasek et Charlie Miller ont révélé des failles de sécurité dans des applications embarquées dans un véhicule Jeep [2]. Ces failles concernaient un réseau Wifi disponible en option à l'intérieur du véhicule mais pouvaient aussi être exploitées directement par internet car les véhicules concernés étaient connectés au réseau cellulaire de l'entreprise Sprint.

Il fut alors possible de réaliser des commandes normalement gérées via le tableau de bord : augmentation du volume sonore de la radio, activation de la ventilation, etc. Ce sont de nombreuses commandes qui peuvent surprendre le conducteur et donc mener à des comportements dangereux sur la route.

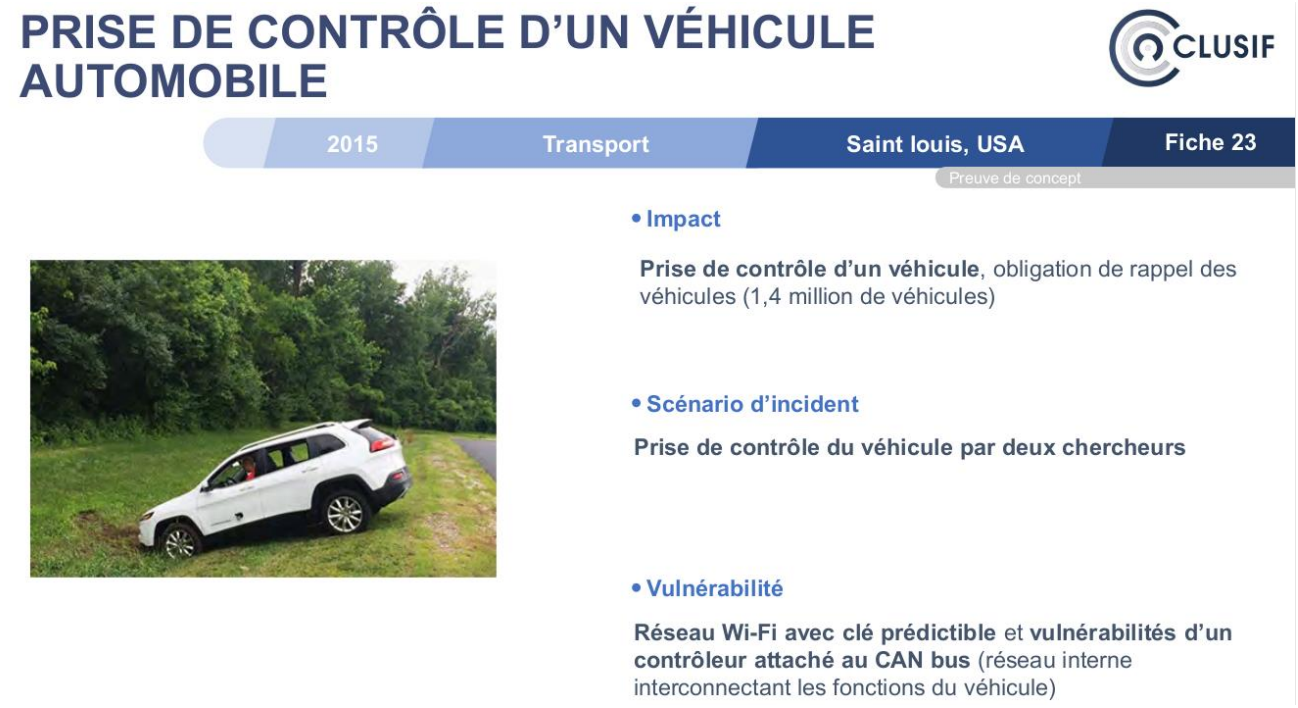

Figure 4 : Fiche 23 [1] Prise de contrôle d'un véhicule automobile

La vulnérabilité la plus dangereuse était la possibilité de modifier le firmware du contrôleur V850 qui, a priori, ne pouvait que lire des informations sur le bus CAN mais ne pouvait pas y envoyer des commandes. Une fois le firmware modifié, les chercheurs ont réussi à envoyer des commandes à distance pour par exemple bloquer le système de freinage ou faire changer le véhicule de direction.

La fiche à propos de cet incident propose les contre-mesures suivantes :

- Utilisation d'un algorithme assurant une génération de clé non prédictible ;
- Mise en place d'un mécanisme empêchant la mise à jour du Firmware du contrôleur V850 par un code non signé ;
- Filtrage des communications entre le contrôleur V850 et le bus CAN

Cette attaque a fait l'effet d'un électrochoc dans l'industrie automobile en 2015 et a abouti au rappel de plus d'un million de véhicules. Ici, l'attaque est d'une complexité très élevée et a pris plusieurs années pour être conçue par les deux chercheurs. Elle souligne toutefois qu'avec l'augmentation de la connectivité, la cybersécurité est devenue un axe de travail important pour l'industrie automobile.

Deux autres fiches (exemples : 26, 27) montrent que les voitures modernes avec des logiciels de plus en plus complexes et des connectivités (wifi, 4G/5G, Bluetooth) importantes, notamment des interactions avec des applications smartphone, ont une surface vulnérable aux attaques plus importantes et deviennent des cibles de choix pour les hackers. Comme dans l'industrie, les mises à jour régulières et le cloisonnement du réseau multimédia et du réseau de terrain sont les premiers éléments mis en avant.

Enfin, la fiche 39 présente un exemple de leurre d'un récepteur GPS, menace prise très au sérieux, en particulier par les équipes travaillant sur les véhicules autonomes.

La partie 3 de ce dossier présente des vulnérabilités dans l'automobile et les travaux actuels des industriels pour renforcer la cybersécurité dans l'automobile.

4 - Plan du dossier

Après avoir défini la cybersécurité et le cadre de ce dossier, ces quelques exemples ont permis de souligner les problématiques de cybersécurité pour les systèmes industriels, dont une partie concernent des aspects réseaux : authentification, confidentialité, intégrité, non répudiation, disponibilité. C'est l'objet de la ressource « Fondamentaux de la sécurité réseau » [6], ce qui amène à introduire le plan prévu pour ce dossier :

Introduction à la cybersécurité des systèmes industriels

Fondamentaux de la sécurité réseau [6]

Cybersécurité des systèmes automatisés industriels

Cybersécurité des systèmes automatisés industriels [7]

Mise en œuvre du protocole sécurisé OPC-UA (à paraitre)

La Cybersécurité chez Eiffage Energie Systèmes [8]

Cybersécurité des objets connectés

Sécurité du protocole Bluetooth Low Energy (à paraitre)

Création d'une application Bluetooth Low Energy sur STM32WB (à paraitre)

Analyse de la sécurité d'une application Bluetooth Low Energy (à paraitre)

Sécurité du protocole LoraWan (à paraitre)

Sécurité du protocole Zigbee (à paraitre)

Wattsense - Siemens, une entreprise pour une GTB sécurisée [9]

Cybersécurité des systèmes embarqués (automobile)

(à paraitre)

Cybersécurité matérielle / les attaques par canaux auxiliaires

Mise en œuvre de la carte ChipWhisperer (à paraitre)

Références

[1]: *Fiches incidents cyber SI industriels – Fiche 22*, Clusif, 2022
https://clusif.fr/publications/fiches-incidents-cyber-si-industriels/
[2]: *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, Andy Greenberg, WIRED, 2015
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[3]: *The Fresh Smell of ransomed coffee*, Martin Hron, Avast, 2020

https://decoded.avast.io/martinhron/the-fresh-smell-of-ransomed-coffee/

[4]: Essonne : un centre hospitalier visé par une cyberattaque, une rançon de 10 millions de dollars exigée, Le Figaro, 2022

https://www.lefigaro.fr/secteur/high-tech/essonne-un-centre-hospitalier-vise-par-une-cyberattaque-une-rancon-de-10-millions-de-dollars-exigee-20220822

[5]: 10 choses à savoir sur les attaques DDoS massives contre Dyn, Le Monde informatique, 25 Octobre 2016, https://www.lemondeinformatique.fr/actualites/lire-10-choses-a-savoir-sur-les-attaques-ddos-massives-contre-dyn-66325.html

[6]: Fondamentaux de la sécurité réseau, M. Sechehaye, A. Juton, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/fondamentaux-dela-securite-reseau

[7]: Cybersécurité des systèmes automatisés industriels, A. Juton, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/cybersecurite-des-systemes-automatises-industriels

[8]: La Cybersécurité chez Eiffage Energie Systèmes, J. Zindy, F. Le Gall, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/cybersecurite-chez-eiffage-energie-systemes

[9]: Wattsense - Siemens, une entreprise pour une GTB sécurisée, M. Zenadi, M. Sauvergeat, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/wattsense-siemens-une-entreprise-pour-une-gbt-securisee