ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité »
Lundi 17 Mars 2025

Cybersécurité des systèmes industriels : garder une longueur d'avance sur les risques OT

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 2 Cybersécurité et E-santé

SOMMAIRE

Introduction *3*
I. Pourquoi parler de cybersécurité industrielle ? *4*
II. De quoi doit-on se défendre ? *5*
III. Que doit-on protéger ? *6*
IV. Des solutions pour prévenir et réagir *8*
V. Orchestrer pour garder une longueur d'avance *9*
VI. Intervention de Charles Blanc-Rolin *10*
VII. Questions / Réponses *11*

Introduction

Le **Lundi de la cybersécurité** du 17 mars 2025 s'est intéressé à un sujet crucial mais encore trop souvent négligé : la **cybersécurité des systèmes industriels**, également appelés systèmes OT (Operational Technology). À l'heure où les infrastructures critiques deviennent des cibles privilégiées, comprendre les risques spécifiques à ces environnements techniques et comment y répondre est devenu une nécessité stratégique.

Deux experts sont intervenus pour éclairer cette problématique sous des angles complémentaires :

- **Pierre-Marie Lore**, Directeur des services Framatome Cybersecurity, fort d'un parcours riche mêlant défense, gouvernance publique et industrie nucléaire. Son intervention a apporté une vision globale, stratégique et structurée de la cybersécurité dans les environnements industriels complexes.
- **Charles Blanc-Rolin**, expert en supervision réseau, a présenté un retour d'expérience opérationnel autour de la détection de menaces réseau sans agent, en s'appuyant sur des outils open source comme Suricata et le projet communautaire **pawpatrules**, qu'il contribue à développer.

Ensemble, ils ont livré une conférence dense et éclairante sur les défis contemporains liés à la protection des systèmes industriels, les outils disponibles et les stratégies à adopter pour conserver une longueur d'avance sur les menaces.

I. Pourquoi parler de cybersécurité industrielle ?

Pierre-Marie Lore introduit son intervention en rappelant que les systèmes industriels, longtemps considérés comme isolés ou trop spécifiques pour être exposés aux menaces cyber, sont aujourd'hui pleinement intégrés dans un environnement numérique interconnecté — et donc vulnérable. Il pose d'emblée plusieurs questions clés : ces systèmes sont-ils réellement non connectés ? Leur ultra-spécificité les protège-t-elle ? Et surtout, faut-il prioriser la sûreté ou la sécurité ?

L'intervenant insiste sur le fait que la cybersécurité est encore trop souvent perçue comme un **centre de coûts** ou une responsabilité cantonnée à quelques spécialistes. Cette vision, selon lui, n'est plus tenable face à l'évolution des menaces, de plus en plus hybrides, ciblées et sophistiquées.

Pour Pierre-Marie Lore, il ne s'agit plus seulement de protéger les systèmes industriels, mais bien de **garder une longueur d'avance** sur les attaquants. Cela passe par une prise de conscience collective, une meilleure orchestration des moyens et une anticipation constante des risques. Il invite ainsi les organisations à intégrer la cybersécurité dès la conception des systèmes (*by design*), à considérer les environnements OT comme des zones critiques à part entière, et à rompre avec l'idée selon laquelle la sécurité serait un frein à l'innovation.

En somme, l'intervenant pose les bases d'une approche proactive, transversale et stratégique de la cybersécurité industrielle.

II. De quoi doit-on se défendre ?

Dans cette seconde partie, Pierre-Marie Lore dresse un panorama détaillé des menaces pesant sur les environnements industriels. Il distingue plusieurs catégories de risques, souvent combinés dans des attaques hybrides.

1. Les menaces logicielles

L'intervenant commence par les maliciels spécifiquement conçus pour les systèmes industriels. Il cite notamment **Stuxnet**, **Triton** ou encore **Industroyer**, qui ciblent directement les automates programmables ou les systèmes de contrôle. À cela s'ajoutent les **ransomwares** orientés OT, comme **LockerGoga** ou **DarkSide**, dont les conséquences peuvent paralyser l'activité industrielle, comme l'ont montré les attaques contre Norsk Hydro ou Colonial Pipeline.

2. Les menaces réseau

Pierre-Marie Lore alerte ensuite sur la vulnérabilité des protocoles industriels souvent dépourvus de mécanismes de sécurité natifs. Les attaques de type **Man-in-the-Middle**, le **rejeu de trames** ou l'**injection de fausses commandes** sont autant de techniques utilisées pour interférer avec les communications entre les équipements. Il souligne également le risque de **déni de service**, qui peut compromettre tout un processus industriel.

3. Les menaces physiques

Contrairement aux idées reçues, les menaces physiques restent une réalité bien présente. L'accès non autorisé aux **baies réseau**, aux **automates** ou aux **salles de contrôle** représente un point d'entrée critique pour un attaquant. À cela s'ajoutent les **attaques électromagnétiques**, comme celles de type TEMPEST, permettant l'espionnage ou la perturbation des signaux, ainsi que le **sabotage matériel**.

4. L'ingénierie sociale

Enfin, Pierre-Marie Lore rappelle que l'humain reste souvent le maillon faible de la chaîne de sécurité. Techniques d'**élicitation**, **phishing** ou **vishing** visent à obtenir des informations confidentielles ou à compromettre des accès légitimes.

III. Que doit-on protéger ?

Après avoir dressé le panorama des menaces, Pierre-Marie Lore s'attache à cartographier les actifs à protéger dans un environnement industriel. Il s'appuie sur le **modèle en couches** (inspiré du modèle Purdue) pour illustrer la complexité et la diversité des systèmes OT.

L'intervenant identifie six niveaux, allant du plus technique et physique au plus organisationnel :

- **Niveau 0 – Le processus**

  Ce niveau regroupe les **capteurs** et **actionneurs** directement connectés aux processus industriels. Ces équipements sont souvent très exposés et peu protégés.

- **Niveau 1 – Contrôle de base**

  On y retrouve les **automates programmables** (PLC), les **systèmes de contrôle distribués** (DCS) et les **unités distantes** (RTU), qui exécutent les commandes envoyées aux machines.

- **Niveau 2 – Supervision**

  Ce niveau centralise la supervision avec des **systèmes SCADA**, des **interfaces homme-machine (IHM)** et des **passerelles de communication**.

- **Niveau 3 – Gestion des opérations**

  Il regroupe les systèmes qui assurent la gestion industrielle quotidienne : **MES (Manufacturing Execution Systems)**, serveurs de logs, systèmes d'authentification, **SIEM**, etc.

- **Niveau 3.5 – Zone tampon (DMZ)**

  Cette zone intermédiaire permet d'assurer une sécurité renforcée pour les accès distants, via des **proxies**, **pare-feux**, **antivirus**, etc.

- **Niveau 4 – Systèmes IT de l'entreprise**

  On y retrouve les éléments classiques du SI : **messagerie**, **applications**, **web**, etc., souvent plus matures en termes de sécurité mais interdépendants des couches OT.

Pour illustrer ces niveaux, Pierre-Marie Lore cite des exemples d'équipements industriels concrets : **PLC Modicon**, **SCADA iFIX**, **Historian Honeywell**, **capteurs VEGA**, **RTU Emerson**, ou encore des actionneurs **Thomson**.

Cette cartographie permet de comprendre que la cybersécurité industrielle ne peut pas se limiter à une simple approche technique. Il s'agit de **protéger une chaîne complète**, où chaque niveau, chaque équipement, chaque protocole, peut devenir un point d'entrée pour un attaquant.

IV. Des solutions pour prévenir et réagir

Dans cette partie, Pierre-Marie Lore propose une démarche structurée pour faire face aux menaces pesant sur les environnements industriels. Il insiste sur la nécessité d'articuler prévention et capacité de réaction, tout en s'appuyant sur une approche globale combinant organisation, technique et culture de sécurité.

L'intervenant commence par rappeler un certain nombre de bonnes pratiques fondamentales. Il évoque notamment l'importance d'un contrôle rigoureux des accès, une gestion encadrée des interventions, ainsi qu'une politique de sauvegarde fiable et régulièrement testée. La question des mots de passe est également abordée, avec la recommandation de privilégier des mots de passe robustes et uniques, associés à une authentification forte, plutôt qu'un renouvellement systématique. Pierre-Marie Lore souligne également la nécessité de réaliser un inventaire complet des actifs, de mener des actions de sensibilisation régulières auprès des équipes, et de mieux encadrer l'utilisation des périphériques amovibles, souvent négligés mais pourtant critiques. La protection de l'information, notamment à travers le chiffrement, ainsi que la sécurisation des communications sans fil, font aussi partie des éléments à ne pas sous-estimer.

Il insiste ensuite sur la notion de sécurité « by design ». Selon lui, la cybersécurité ne doit pas être pensée après coup, mais intégrée dès la conception des systèmes. Cela implique de faire les bons choix techniques dès le départ, qu'il s'agisse de composants matériels comme les CPU, GPU ou FPGA, ou encore de pratiques telles que le durcissement des configurations ou la mise en place de mécanismes de type whitelisting. Il plaide pour une réflexion approfondie sur les architectures et la segmentation des réseaux industriels afin de limiter les surfaces d'attaque.

Pierre-Marie Lore passe ensuite en revue les différentes solutions techniques à mettre en œuvre dans les environnements OT. Il évoque les pare-feux industriels, les bastions d'administration sécurisés, les sondes de détection réseau, les solutions antivirus compatibles avec les contraintes OT, ou encore les infrastructures à clé publique et les VPN. Il rappelle que ces outils doivent être intégrés dans une stratégie globale cohérente, et régulièrement réévalués au travers d'audits.

Enfin, l'intervenant insiste sur la nécessité de mettre en place une surveillance continue à plusieurs niveaux. Cela passe par une surveillance physique des infrastructures (via des scellés, de la vidéosurveillance ou des détecteurs d'ouverture), mais aussi par une surveillance réseau s'appuyant à la fois sur des signatures, des comportements et des données opérationnelles. La couche applicative n'est pas en reste, avec l'usage d'outils de type HIDS, HIPS ou EDR adaptés aux systèmes industriels.

Pour conclure cette section, Pierre-Marie Lore rappelle qu'il n'existe pas de solution miracle. Ce qui compte, c'est la cohérence de la stratégie déployée et la capacité des organisations à identifier clairement les responsabilités, à tous les niveaux, afin de construire une cybersécurité industrielle résiliente et adaptée à la réalité du terrain.

V. Orchestrer pour garder une longueur d'avance

Pour conclure son intervention, Pierre-Marie Lore insiste sur la nécessité d'une approche orchestrée, structurée et durable de la cybersécurité industrielle. Il ne suffit pas de déployer des solutions techniques ou de réagir ponctuellement aux incidents. L'enjeu est de construire dans le temps une posture de sécurité capable de s'adapter à l'évolution constante des menaces.

L'intervenant insiste d'abord sur l'importance d'une gouvernance claire et d'un pilotage rigoureux. Cela commence par une gestion de projet bien définie, intégrant les aspects sécurité dès les phases de spécification et de conception. Il évoque la nécessité de formaliser une stratégie d'homologation, de rédiger des procédures et des guides de configuration, et de documenter précisément les architectures en place à travers des plans d'audit, des matrices de durcissement ou encore des listes de composants.

Une autre composante essentielle de cette orchestration repose sur l'analyse de risques. Celle-ci doit être menée de manière régulière et dynamique, afin de prendre en compte l'apparition de nouvelles vulnérabilités, de nouveaux équipements ou de nouvelles menaces. Pierre-Marie Lore rappelle que la sécurité ne peut rester figée : elle doit s'inscrire dans un cycle d'amélioration continue, avec des réévaluations périodiques, des contrôles récurrents, et un suivi de la conformité réglementaire.

Il souligne également la nécessité de se préparer à la gestion de crise. Cela implique de définir des échelles de gravité, de prévoir des scénarios de réponse, de conduire des exercices réguliers, et surtout, d'impliquer tous les niveaux de l'entreprise. Cette coordination élargie permet de mieux réagir en cas d'incident, mais aussi d'anticiper les failles organisationnelles qui peuvent freiner une réponse efficace.

Pierre-Marie Lore insiste enfin sur les enjeux liés à la fin de vie des systèmes industriels. La sécurisation des cycles de décommissionnement est trop souvent négligée, alors qu'elle constitue un point critique. Il recommande la mise en place de procédures spécifiques pour la neutralisation matérielle, l'effacement sécurisé des données, la désactivation des firmwares, la destruction physique des composants sensibles, et la traçabilité post-déploiement.

À travers cette dernière partie, l'intervenant transmet un message fort : la cybersécurité industrielle ne peut reposer sur une logique d'outils ou d'urgence. Elle requiert un **effort continu**, une organisation transversale, et une capacité à planifier dans le temps long, afin de rester toujours un coup d'avance sur la menace.

VI. Intervention de Charles Blanc-Rolin

La seconde intervention de la conférence a été assurée par Charles Blanc-Rolin, expert reconnu en supervision réseau et contributeur actif au projet pawpatrules. Son exposé, à la fois technique et pragmatique, portait sur les limites des solutions classiques de cybersécurité dans les environnements industriels, et sur l'importance croissante de la supervision réseau pour pallier ces lacunes.

Charles Blanc-Rolin commence par poser un constat clair : dans de nombreux contextes industriels, il est tout simplement impossible d'installer un agent de sécurité sur chaque machine. Les raisons sont multiples : systèmes d'exploitation obsolètes, contraintes techniques ou réglementaires, équipements critiques non compatibles, ou encore refus des éditeurs. Par ailleurs, même lorsqu'un antivirus ou un EDR est en place, ces outils peuvent être contournés par des techniques sophistiquées comme le Reflective Loading, le Black Out, ou encore l'EDR Sandblast. L'intervenant rappelle également que ces outils sont parfois mal configurés ou ne disposent pas d'une visibilité suffisante sur l'ensemble des activités réseau, notamment lorsque des outils légitimes sont détournés.

Dans ce contexte, la supervision réseau apparaît comme une réponse incontournable. Elle permet d'élargir considérablement le périmètre de détection, sans nécessiter l'installation d'agents sur les postes. Grâce à des technologies comme les IDS (Intrusion Detection System), les NDR (Network Detection and Response) ou les NSM (Network Security Monitoring), il devient possible de détecter un grand nombre de comportements anormaux : communications vers des serveurs de commande et contrôle, shadow IT, vulnérabilités connues, ou encore pratiques inappropriées sur le réseau. L'un des grands avantages de cette approche est qu'elle est difficilement contournable par les attaquants, tout en offrant une vision complémentaire à celle des outils installés sur les hôtes.

Charles Blanc-Rolin a ensuite présenté Suricata, un moteur d'analyse réseau libre, sans interface graphique, développé par l'OISF (Open Information Security Foundation), dont l'ANSSI est membre. Suricata est aujourd'hui utilisé comme base pour les sondes de détection souveraines qualifiées en France. Cet outil est capable de reconnaître de nombreux protocoles réseau, de générer des alertes à partir de règles définies, de produire des traces au format JSON, et même d'exporter les paquets au format PCAP. Il permet également d'analyser les flux TLS (via JA3) et SSH (via hassh), et de calculer la volumétrie échangée.

Enfin, l'intervenant a présenté le projet pawpatrules, une collection de plus de 21 000 règles de détection librement accessibles. Ce projet, initié en 2020 et ouvert au public en 2022, a été intégré à Suricata en 2024. Il peut être mis en œuvre dans n'importe quelle solution de supervision réseau basée sur Suricata. Ce jeu de règles est utilisé par de nombreuses structures : des universités européennes et asiatiques, des centres hospitaliers, des ministères, des entreprises ferroviaires, des services de renseignement ou encore des professionnels de la cybersécurité.

Avec cette présentation, Charles Blanc-Rolin a démontré l'efficacité et la pertinence des approches réseau pour renforcer la détection des menaces, en particulier dans des environnements contraints comme ceux de l'OT. Son message est clair : face aux limites des solutions traditionnelles, la supervision réseau s'impose comme un pilier indispensable d'une cybersécurité industrielle moderne et robuste.

VII. Questions / Réponses

La session s'est conclue par un temps d'échange riche entre les participants et les intervenants, permettant de prolonger la réflexion sur des enjeux concrets, tant techniques qu'organisationnels. Plusieurs questions ont été soulevées via le chat, traduisant les préoccupations actuelles des professionnels face à la montée des exigences réglementaires, aux contraintes industrielles ou encore à la complexité croissante des environnements OT.

L'une des premières questions posées à Pierre-Marie Lore concernait la situation des **PME industrielles peu matures ou dépourvues de RSSI**. L'intervenant a souligné l'importance d'un accompagnement externe pour structurer progressivement une démarche de sécurité. Il a recommandé de commencer par un **inventaire des actifs**, la mise en place de **sauvegardes robustes**, la **gestion des accès**, et surtout, une **gouvernance claire** du sujet, même dans des structures de taille modeste. Pour lui, il est essentiel d'éviter de négliger ces entreprises, car elles représentent souvent le maillon faible d'une chaîne plus vaste.

Une autre question portait sur les **moyens de se conformer aux exigences réglementaires**, en particulier **NIS2** et **IEC 62443**. Pierre-Marie Lore a rappelé qu'il ne s'agit pas seulement de répondre à un cadre légal, mais de bâtir une posture de sécurité pérenne. Il a insisté sur la nécessité de **cartographier les risques**, de **mettre en œuvre une politique de sécurité formalisée** (PSSI), et d'**intégrer progressivement les bonnes pratiques de sécurité** dans les processus métiers.

Catherine Gabay a interrogé les intervenants sur la place des **attaques électromagnétiques** dans le spectre des menaces cyber. Il a été confirmé qu'elles sont bel et bien considérées comme des menaces, notamment dans les référentiels de l'ANSSI. Ces attaques, bien que rarement évoquées dans les médias, peuvent permettre l'espionnage ou la perturbation des signaux critiques dans un environnement industriel sensible.

Une autre intervention a soulevé la question des **solutions de chiffrement dans les systèmes OT**. Charles Blanc-Rolin et d'autres participants ont précisé que des technologies existent désormais pour chiffrer les échanges sans altérer les performances industrielles, notamment par l'utilisation d'**équipements de coupure à base de FPGA**, insérés entre deux assets OT.

Enfin, plusieurs commentaires ont porté sur les **mots de passe**. Il a été rappelé que le **renouvellement systématique** des mots de passe n'est plus recommandé, sauf en cas de suspicion de compromission. L'approche actuelle privilégie l'usage de mots de passe **longs, uniques**, associés à des **mécanismes d'authentification multifactorielle**.

Ces échanges ont mis en lumière la diversité des préoccupations du terrain et l'intérêt croissant pour des solutions concrètes, adaptées aux contraintes industrielles. Ils ont également illustré la richesse de cette édition des Lundis de la Cybersécurité, qui a su faire dialoguer stratégie, retour d'expérience et innovations techniques dans un cadre accessible et interactif.