

## Cybersécurité Industrielle : Garder une longueur d'avance sur les risques OT



Lundi 17 mars  
18h00 - 20h00

Par webinaire Zoom



**Cybersécurité  
industrielle**  
Garder une longueur d'avance  
sur les risques OT



**Pierre-Marie LORE**  
Directeur cybersécurité Framatome



Organisateurs



Béatrice Laurent



Gérard Peliks



### La convergence de l'OT et de l'IT

Les systèmes technologiques opérationnels dits « **OT** : Operational Technology » utilisent des composants logiciels et matériels pour contrôler les processus industriels. Et ces systèmes intègrent aujourd'hui des systèmes informatiques (**IT**) centrés sur les données.

La convergence IT/OT vise à intégrer les équipements et appareils physiques (OT) dans le domaine numérique (IT). L'Internet des Objets (IoT) prend toute sa place pour piloter les processus industriels. Cela améliore en particulier la maintenance et la disponibilité des équipements.

Mais comment protéger les sites industriels sensibles des agressions de plus en plus nombreuses, et très sophistiquées en particulier grâce à (ou plutôt à cause de) l'Intelligence Artificielle ? Utiliser l'IA pour connaître à l'avance ces menaces ? Utiliser le OTrust ? Prévoir une cyber résilience efficace des installations ?

Ces questions sont fondamentales car les sites industriels sont connectés et pour beaucoup de ces sites, agression réussie : catastrophe assurée. Que pense l'intervenant de cette **Industrie 4.0** qui représente des machines et des processus de fabrication intelligemment mis en réseau à l'aide des technologies de l'information ?

## Je donne la plume à l'intervenant Pierre-Marie LORE



La cybersécurité industrielle est devenue un pilier essentiel pour protéger les infrastructures critiques face à des menaces en constante évolution. Dans un contexte où la digitalisation transforme profondément les systèmes industriels, l'enjeu est de garantir la sûreté et la résilience des installations tout en répondant aux exigences de performance et d'innovation. Les environnements industriels intègrent désormais des technologies connectées (IoT, systèmes de contrôle-commande, réseaux OT/IT convergents), qui ouvrent la porte à des cybermenaces de plus en plus sophistiquées, capables de perturber, voire de stopper des opérations vitales pour l'économie et la société.

Anticiper ces risques nécessite une stratégie de cybersécurité proactive, intégrant des solutions avancées et adaptées aux spécificités des systèmes industriels. Une approche complète et structurée s'impose, combinant gouvernance, évaluation de risques, et renforcement des systèmes par un design sécurisé et une gestion dynamique des vulnérabilités. La surveillance en temps réel et les capacités de détection et de réponse aux incidents permettent de limiter l'impact des cyberattaques. À cela s'ajoute l'importance de maintenir les systèmes en conditions de sécurité grâce à des audits réguliers, des tests d'intrusion, et une amélioration continue, garantissant que les dispositifs restent protégés face aux nouvelles menaces.

Face à une réglementation de plus en plus exigeante, notamment en Europe avec la directive NIS 2 et la mise en conformité LPM, la cybersécurité industrielle n'est plus une option, mais une nécessité stratégique pour les entreprises. Garder une longueur d'avance sur les risques, c'est protéger l'avenir des infrastructures essentielles en intégrant des pratiques de cybersécurité robustes et en adoptant une culture de sécurité à tous les niveaux de l'organisation. Une cybersécurité forte garantit non seulement la continuité des opérations, mais aussi la confiance des partenaires, clients, et du public envers les infrastructures industrielles modernes.

## Je reprends la plume

### Qui est Pierre-Marie LORE ?



**Pierre-Marie Lore**, / Promotion 2015/2016 du MBA Management de la Cybersécurité de l'Institut Léonard de Vinci, Officier de marine, est le **Directeur cybersécurité de Framatome I&C**

Il a cofondé ICON-ONG - <https://icon.ngo/fr/> - Association internationale rassemblant une communauté autour des questions cyber et IA en Europe.

Ancien responsable de la sécurité des systèmes d'information du groupe RATP, il est ingénieur diplômé de l'Ecole Navale.

## Demande d'inscription pour le Lundi de la cybersécurité du mois de mars 2025

**Lundi 17 mars, par visio-conférence Zoom à partir de 18 h 00.**



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien vers la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à Béatrice Laurent :

[beatricelaurent.CDE@gmail.com](mailto:beatricelaurent.CDE@gmail.com)

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail ([gerard.peliks@arcsi.fr](mailto:gerard.peliks@arcsi.fr)).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 17 mars, dès 18 h 00**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00**.

## Quelques minutes avec Charles Blanc-Rolin

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Cette séquence du Lundi de février sera animée par **Charles Blanc-Rolin**.

**Charles Blanc-Rolin** VP de l'APSSIS, et nouveau membre de l'ARCSI, écrit et partage depuis plusieurs années des règles de détection de menaces sur les réseaux pour le moteur Suricata. Ces règles sont donc aussi bien compatibles avec les solutions open source que les sondes qualifiées de l'ANSSI, qui elles aussi se basent sur le moteur Suricata, Il nous dira ce qu'il est possible de détecter avec, et comment tout ça s'articule avec des outils tels que les EDR.



Il nous présentera son activité sur la détection des menaces, en contrôlant les flux depuis et vers des machines sur lesquelles l'installation d'une solution de lutte contre ces menaces n'est pas toujours possible. Avec plus de 20 000 règles, son projet permet de détecter des vulnérabilités sur les systèmes, des connexions vers des serveurs malveillants connus (ou pas encore), des exfiltrations de données, des outils offensifs, des connexions suspectes, des techniques de mouvements latéraux, etc... »

## Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez , sur le web de l'ARCSI en [https://www.arcsi.fr/evt\\_passes.php](https://www.arcsi.fr/evt_passes.php) tous les détails, slides, parfois aussi les enregistrements et des comptes rendus, écrits par Clarisse Véron, élève du master2 « Cybersécurité et e-Santé » de l'université Paris Cité

Par exemple, pour le Lundi de la Cybersécurité du mois de janvier 2025 :

La lettre d'invitation est [disponible ici](#).

Les slides de la présentation "Mesurer et Distribuer le temps" de Gérard Berry sont [disponibles ici](#).

Les slides de la présentation du CEFYCYS sont [disponibles ici](#).

Le compte-rendu est [disponible ici](#).

La rediffusion est [disponible ici](#).

Les documents pour le Lundi de février suivront. Mais attention, il n'est pas garanti qu'il y aura ces documents pour chacun de nos futurs lundis. Donc il est conseillé d'être connectés pour les suivre par Zoom.

## Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?

Prompt posé à Gemini (l'IA Générative de Google) :

### Comment protéger les infrastructures industrielles critiques face à des cybermenaces en constante évolution

La protection des infrastructures industrielles critiques est devenue un enjeu majeur dans un monde de plus en plus digitalisé. Ces systèmes, autrefois isolés, sont désormais connectés à des réseaux étendus, les rendant vulnérables aux cyberattaques. Voici quelques stratégies clés pour renforcer leur sécurité :

#### 1. Évaluer et gérer les risques spécifiques

- **Identifier les actifs critiques** : Déterminez les systèmes, les données et les processus les plus importants pour votre organisation.
- **Analyser les vulnérabilités** : Effectuez des évaluations régulières pour identifier les failles potentielles.
- **Établir un plan de réponse aux incidents** : Préparez-vous à réagir rapidement et efficacement en cas de cyberattaque.

#### 2. Mettre en œuvre des mesures de sécurité robustes

- **Ségréger les réseaux** : Isolez les réseaux industriels des réseaux administratifs pour limiter la propagation des attaques.
- **Contrôler les accès** : Mettez en place une gestion rigoureuse des accès, en utilisant l'authentification multifactorielle et des privilèges minimums.
- **Mettre à jour régulièrement les systèmes** : Appliquez les correctifs de sécurité dès leur disponibilité.
- **Utiliser des solutions de sécurité spécialisées** : Déployez des firewalls industriels, des systèmes de détection d'intrusion (IDS) et des solutions de sécurité des données.

#### 3. Former et sensibiliser les employés

- **Sensibilisation à la sécurité** : Informez les employés sur les bonnes pratiques de sécurité informatique et les risques liés aux cyberattaques.
- **Formation spécialisée** : Formez les équipes techniques aux outils et aux procédures de sécurité.

#### 4. Collaborer avec des partenaires

- **Partager les informations** : Collaborez avec d'autres organisations pour partager les meilleures pratiques et les informations sur les menaces.

- **Faire appel à des experts** : Faites appel à des experts en cybersécurité pour vous aider à mettre en œuvre et à maintenir vos mesures de sécurité.

## 5. Adopter une approche proactive

- **Surveillance continue** : Surveillez en permanence vos systèmes pour détecter toute activité suspecte.
- **Tests d'intrusion** : Simulez des attaques pour évaluer votre niveau de sécurité.
- **Résilience** : Mettez en place des mécanismes de récupération après sinistre pour minimiser les impacts d'une cyberattaque.

### Technologies clés pour renforcer la sécurité des infrastructures critiques :

- **Intelligence artificielle (IA)** : L'IA peut être utilisée pour détecter les anomalies, analyser les menaces et automatiser certaines tâches de sécurité.
- **Blockchain** : La blockchain peut être utilisée pour assurer l'intégrité des données et renforcer la confiance dans les systèmes.
- **IoT sécurisé** : Les objets connectés doivent être sécurisés pour éviter qu'ils ne deviennent des points d'entrée pour les cyberattaques.

**En conclusion**, la protection des infrastructures industrielles critiques nécessite une approche globale et multidimensionnelle. En combinant des mesures techniques, organisationnelles et humaines, il est possible de renforcer considérablement la sécurité de ces systèmes essentiels.

**Bon, intéressant, mais qu'en pense Pierre-Marie LORE ?** L'interprétation des résultats d'une IA Générative par un expert humain connu et respecté est indispensable pour se faire une opinion. Pierre-Marie Lore nous en dira plus le 10 mars et répondra à nos questions, et nous en discuterons. **Les inscriptions sont ouvertes.**

Gérard Peliks