

## CYBERMOIS 2026

# Cyber, risques industriels & climat

*Quand le risque numérique rencontre le risque opérationnel et environnemental*

*Note de sensibilisation – MKL Engineering,*

*Pôle Ingénierie, Risques & Expertise | MKL OIL*



## 01 — LE CYBER NE S'ARRÊTE PAS À L'INFORMATIQUE

En environnement industriel, une cyberattaque ne touche pas seulement les ordinateurs et les données. Les systèmes OT (Operational Technology) pilotent et surveillent directement les procédés : automates, SCADA, systèmes de contrôle-commande, systèmes instrumentés de sécurité (SIS).

Lorsque l'un d'eux est compromis, les conséquences sortent du périmètre informatique :



Comme le rappelle l'ANSSI, ces systèmes ont une action directe sur le monde physique : leur compromission peut donc avoir des conséquences sur les personnes, les biens ou l'environnement. Un incident cyber peut ainsi devenir un incident opérationnel.

## 02 — CE N'EST PAS UN SCÉNARIO THÉORIQUE

En 2017, le logiciel malveillant Triton a ciblé les systèmes instrumentés de sécurité d'un site pétrochimique au Moyen-Orient, qui constituent une barrière essentielle dans la prévention des situations dangereuses.

En mai 2021, une attaque par rançongiciel sur le système informatique de Colonial Pipeline a conduit l'exploitant à arrêter son oléoduc par précaution, perturbant l'approvisionnement en carburant de l'est des États-Unis.

**Deux attaques, deux chemins différents : dans le premier cas, la sécurité du procédé était directement ciblée ; dans le second, l'attaque IT a conduit à une interruption préventive des opérations.**



## 03 — LE CYBER, FACTEUR INITIATEUR D'UN RISQUE INDUSTRIEL ?

Selon le procédé et le scénario considérés, une compromission peut :

- rendre indisponible un système critique ;
- modifier ou interrompre des fonctions de contrôle ou de sécurité ;
- imposer un fonctionnement en mode dégradé ;
- contribuer à une perte de maîtrise du procédé ;
- entraîner des conséquences sur la sécurité des personnes ou l'environnement.

Les scénarios cyber ont donc leur place dans les démarches de maîtrise des risques, les plans d'urgence et les exercices de crise.

## 04 — DU RISQUE CYBER À L'ÉTUDE DE DANGERS

Il ne s'agit pas de transformer une étude de dangers en étude de cybersécurité, mais de poser une question simple : le cyber peut-il contribuer à un scénario accidentel ?

**MENACE CYBER → SYSTÈME INDUSTRIEL → FONCTION CRITIQUE  
→ PROCÉDÉ → ÉVÉNEMENT REDOUTÉ → CONSÉQUENCES**

Cette lecture fait apparaître les dépendances entre technologies, procédés, organisation et barrières de sécurité, en particulier lorsque des barrières reposent sur des systèmes numériques. L'INERIS souligne d'ailleurs que l'analyse des risques cyber des systèmes de conduite et de sécurité vient compléter l'analyse des risques accidentels menée dans l'étude de dangers.

## 05 — ET L'ENVIRONNEMENT ?

Une défaillance cyber n'entraîne pas automatiquement un impact environnemental. En revanche, selon les scénarios, la perte de maîtrise d'un procédé qu'elle provoque peut, elle, en avoir :

**CYBERATTAQUE → PERTURBATION DU PROCÉDÉ → FONCTIONNEMENT DÉGRADÉ  
→ DÉRIVE / INCIDENT / ARRÊT → CONSÉQUENCE ENVIRONNEMENTALE POTENTIELLE**

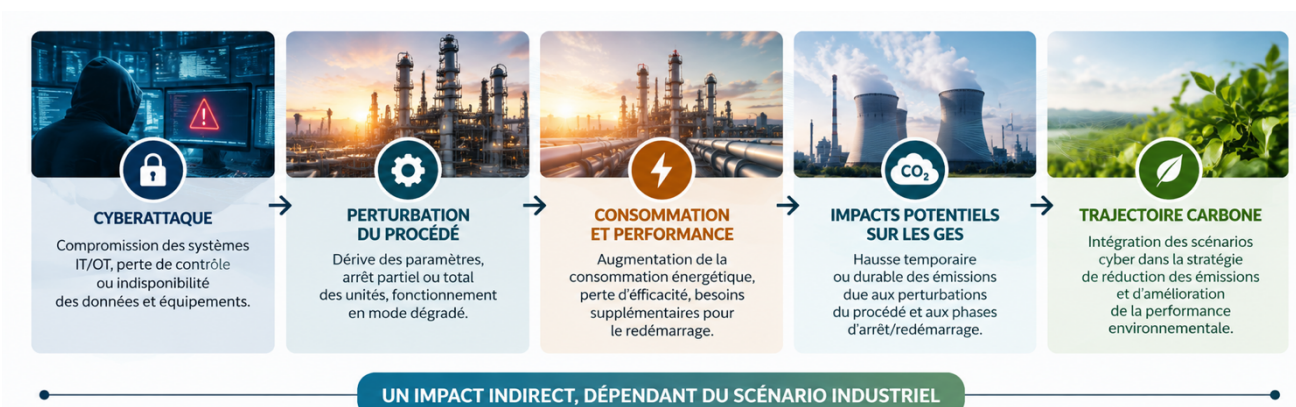
Ce lien doit être analysé à partir des scénarios réels du site, pas de manière générique.

## 06 — ET LA TRAJECTOIRE CARBONE ?

Le cyber n'est pas un poste d'émission en soi. Le lien éventuel est indirect : il passe par les conséquences opérationnelles d'un scénario cyber sur le procédé.

Selon le procédé et le scénario considérés, une perturbation peut ainsi affecter les consommations énergétiques, l'efficacité des procédés, les phases d'arrêt et de redémarrage ou certaines émissions.

Pour un exploitant engagé dans une trajectoire de réduction des GES, ces scénarios peuvent donc mériter d'être identifiés et évalués, comme une conséquence potentielle du risque industriel.



## 07 — UNE APPROCHE INTÉGRÉE DES RISQUES

Le risque cyber doit être analysé en lien avec les risques opérationnels, industriels, environnementaux et de continuité.



## 08 — ET SI VOUS TESTIEZ VOTRE RÉILIENCE ?

Si un système critique devenait indisponible demain, saurions-nous quelles en seraient les conséquences sur la sécurité, la production, l'environnement et la continuité de nos activités ? Cinq questions pour commencer :

- ☐ Avons-nous identifié nos systèmes industriels critiques ?
- ☐ Avons-nous identifié les conséquences d'une indisponibilité de ces systèmes ?
- ☐ Nos scénarios cyber sont-ils intégrés à notre analyse des risques ?
- ☐ Avons-nous défini nos capacités de fonctionnement en mode dégradé ?
- ☐ Avons-nous testé notre capacité de reprise ?

## 09 — L'APPROCHE MKL ENGINEERING

Pour MKL Engineering, la cybersécurité est une composante de la maîtrise globale des risques, en particulier dans les environnements industriels à enjeux critiques. Nous accompagnons les exploitants sur :



## CONCLUSION

La cybersécurité industrielle ne peut plus être pensée comme une simple question informatique. Le risque cyber peut devenir un risque opérationnel, un facteur de risque industriel, un enjeu de continuité et, selon les scénarios, une source de conséquences environnementales et climatiques.



La bonne question n'est donc pas seulement « *Sommes-nous protégés contre une cyberattaque ?* », mais aussi « **Sommes-nous capables d'en comprendre les conséquences et de maintenir nos fonctions critiques si elle survient ?** »

# ANTICIPER • PRÉVENIR • RÉSISTER • REPRENDRE

*Parce que la cybersécurité est aussi une question de maîtrise des risques industriels.*

## MKL ENGINEERING PEUT VOUS ACCOMPAGNER

Diagnostic • Analyse des risques • IT/OT • Étude des scénarios • Continuité • Résilience •  
Environnement & GES



### CYBER

Protéger  
les systèmes  
IT/OT



### PROCÉDÉ

Assurer  
la continuité  
des opérations



### RISQUE

Limitier  
les impacts  
industriels



### ENVIRONNEMENT

Maîtriser  
les conséquences  
sur les GES



### RÉSILIENCE

Maintenir  
et rétablir  
les fonctions  
critiques



## MKL ENGINEERING

Pôle Ingénierie, Risques & Expertise – MKL OIL

Pour échanger sur vos enjeux :

- [engineering@mkl-oil.fr](mailto:engineering@mkl-oil.fr)
- [info@mkl-oil.fr](mailto:info@mkl-oil.fr)