Cyber-Physical Risks: When Data Attacks Meet Physical Safety Stats and Facts – French

FAITS

- **Systèmes de Contrôle Compromis :** Les cyberattaques visant les systèmes de contrôle industriels peuvent altérer le comportement des équipements, entraînant des mouvements dangereux, des défaillances d'arrêt ou des libérations d'énergie incontrôlées.
- **Accès à Distance non Autorisé :** Les intrus qui parviennent à accéder à des équipements connectés ou à des systèmes de sécurité peuvent contourner les commandes et désactiver les protections à l'insu des travailleurs.
- **Manipulation des Capteurs et des Données :** Des données altérées ou erronées provenant des capteurs peuvent induire les opérateurs en erreur, entraînant des décisions dangereuses et un retard dans la détection des dangers.
- **Panne des Systèmes d'Arrêt et de Sécurité :** Les attaques visant les verrouillages de sécurité ou les systèmes d'arrêt d'urgence peuvent empêcher l'activation des protections essentielles lors d'incidents.
- **Réaction Tardive aux Dangers :** La perturbation des systèmes de communication peut ralentir les interventions d'urgence, aggravant ainsi la gravité des incidents.
- **Dépendance vis-à-vis des Systèmes Connectés :** La dépendance accrue vis-à-vis des systèmes numériques signifie que les défaillances ou les violations peuvent avoir un impact direct sur les opérations physiques et la sécurité des travailleurs.
- **Erreur humaine sous l'effet du stress cybernétique :** La confusion lors d'incidents cybernétiques peut conduire à des actions inappropriées, augmentant ainsi le risque de blessures physiques.

STATISTIQUES

- Aux États-Unis, environ 32 % des entreprises industrielles ont signalé des incidents de cybersécurité touchant leurs systèmes de technologie opérationnelle (OT), ce qui accroît le risque de répercussions sur la sécurité physique (rapports d'IBM Security et du secteur, 2023–2024).
- Les données américaines montrent que plus de 40 % des cyberattaques visant des infrastructures critiques impliquent des tentatives de perturbation des opérations physiques, notamment dans les secteurs de l'énergie, de la fabrication et des services publics (rapports de la CISA et du DHS, 2022–2024).
- En Amérique du Nord, environ 25 % des organisations ont signalé que les

incidents de cybersécurité avaient eu des conséquences directes sur le plan opérationnel ou en matière de sécurité, notamment des arrêts d’équipement ou des conditions dangereuses (SANS Institute, 2023).

- Des rapports américains indiquent que plus de 50 % des incidents de cybersécurité industrielle impliquent des systèmes de contrôle compromis, ce qui peut affecter directement la sécurité des machines et des travailleurs (Rapport Dragos sur la cybersécurité industrielle, 2023–2024).
- Au Canada, environ 30 % des organisations gérant des infrastructures critiques ont signalé des incidents de cybersécurité ayant eu un impact sur leurs opérations, y compris des perturbations pouvant affecter la sécurité des travailleurs (Sécurité publique Canada, 2022–2024).
- Les données américaines montrent que les attaques par rançongiciel représentaient plus de 20 % des incidents de cybersécurité dans les secteurs industriels, provoquant souvent des arrêts de production et des conditions d’exploitation dangereuses (Rapport IC3 du FBI, 2023).