# Les jumeaux numériques et physiques, bancs d’essai pour la cyber-résilience industrielle

La convergence IT/OT s’impose aujourd’hui comme un impératif pour l’industrie 4.0. Pourtant, cette ouverture nécessaire des systèmes de production expose les infrastructures critiques à des cybermenaces croissantes.

Face à ce paradoxe, une approche innovante émerge rapidement : l’utilisation de jumeaux numériques et physiques utilisés comme des environnements d’entraînement à la cyber-résilience. Au-delà de la simple modélisation, ces répliques permettent de tester, valider et optimiser les architectures de sécurité, avant leur déploiement en production.

L’architecture Unified Namespace (UNS) constitue par exemple une réponse concrète aux défis de la convergence IT/OT. Contrairement aux approches traditionnelles cloisonnées, l’UNS établit un référentiel unique permettant à l’ensemble des systèmes industriels de communiquer grâce à un langage normalisé. Cette architecture ouverte facilite la circulation bidirectionnelle des données entre les automates programmables, les systèmes Edge, et les infrastructures cloud… Cependant, cette connectivité accrue multiplie mécaniquement la surface d’attaque. Chaque nouveau capteur IoT, chaque connexion supplémentaire représente un vecteur d’intrusion potentiel. La mise en œuvre de l’UNS exige donc une approche cyber-sécuritaire rigoureuse dès la conception, intégrant tout à la fois segmentation réseau, firewalls contextuels, et serveurs d’administration dédiés. L’enjeu consiste donc à préserver l’agilité opérationnelle sans sacrifier la sécurité, un équilibre difficle à trouver, qui

nécessite des tests approfondis.

## Les limites des jumeaux purement numériques

Continuer la lecture de Les jumeaux numériques et physiques, bancs d’essai pour la cyber-résilience industrielle →

Cet article Les jumeaux numériques et physiques, bancs d’essai pour la cyber-résilience industrielle est apparu en premier sur Techniques de l’Ingénieur.