

Cyber Indus — Valise de démonstration de cybersécurité industrielle

Mallette portable reproduisant un environnement industriel réel (PLC, capteurs, réseau OT) pour démontrer des scénarios de cyberattaque et de défense. Projet de groupe (3 étudiants), 16 semaines, Lycée Jules Fil (Carcassonne).

Mon périmètre : « Protocoles & Capteurs industriels »

- Installation matérielle et câblage (alimentation, réseau Ethernet/PROFINET) sur rail DIN
- Configuration de l'automate Siemens S7-1200 sous TIA Portal (programmation Ladder, OB1)
- Intégration du variateur G120, de l'IHM KTP700 et du maître IO-Link AL1304
- Préparation des scénarios de démonstration de cyberattaque
- Réalisation des diagrammes UML/SysML (cas d'utilisation, déploiement, exigences)

Scénarios d'attaque démontrés (labo fermé, matériel dédié)

Scénario	Protocole	Impact démontré
Rejeu PROFINET	PROFINET	Commandes reproductibles sans autorisation
Usurpation (spoofing)	PROFINET / S7comm	Envoi de commandes frauduleuses
Man-in-the-Middle	S7comm / TCP	Altération des données PLC <-> IHM
Déni de service	PROFINET	Redémarrage forcé du PLC
Exploitation PUT/GET	S7comm (TCP 102)	Contrôle total du PLC à distance (CVE-2019-13945)

Ce que j'ai cassé et comment je l'ai réparé

Problème — Le panneau IHM KTP700 (firmware V17) refusait le transfert d'image depuis TIA Portal V16.

Solution — Migration du projet vers TIA Portal V20 (firmware V17 nécessite V20+) — migration automatique sans perte du programme.

Problème — Le maître IO-Link AL1304 affichait un défaut (BF rouge), humidité bloquée à 0.

Solution — Submodule mal configuré (« 2 I Byte » au lieu de « 8 I Byte + PQI »). Correction du submodule et des adresses réelles (%IW68/%IW72).

Problème — Le variateur G120 déclenchait les défauts F0850, F7220 puis F3330.

Solution — Réglage de P0700 (commande = PROFINET) et P2106, puis remplacement du mot d'arrêt 16#0000 (interdit) par 16#047E (arrêt sur rampe).

Problème — Le bouton d'arrêt d'urgence démarrait le moteur au lieu de l'arrêter.

Solution — Logique de contact inversée (NF au lieu de NO) corrigée dans le programme Ladder.

Ce que j'ai appris

Compréhension complète d'un système industriel : câblage rail DIN, programmation Ladder, protocoles PROFINET/IO-Link/S7comm, mise en service d'un variateur. Sensibilisation concrète aux vulnérabilités OT et à l'importance de la protection des infrastructures industrielles.

Technologies : TIA Portal V20 · Siemens S7-1200 · PROFINET · IO-Link · SINAMICS G120 · Python (snap7)
· Wireshark · UML/SysML

Jordan Carrere — Portfolio complet avec schémas interactifs : <https://cvjordan.jordancarrere11.workers.dev/projets/cyber-indus.html>