Projet SuperviZ - WP6 : Plateformes expérimentales

Contributeurs
Radhouene Azzabi et Philippe Limousin (CEA)
Guillaume Doyen et Fabien Autrel (IMT Atlantique)
Sondos Abuzant et Gregory Blanc (IMT - TSP)
Abdelkader Lahmadi (Loria)
Florent Galtier (LAAS)
Stéphane Mocanu (G-INP)
Matthews José et Jérôme François (INRIA)

Responsable : Stéphane Mocanu

Validation : Ludovic Mé et Hervé Debar

Table des matières

Résumé : L'objectif de ce document est double : d'une part répertorier les moyens expérimentaux mis en commun par le consortium, d'une autre part identifier les futurs développements qui seront réalisés au sein du projet.

1 Introduction

La réalisation d'une plateforme expérimentale globale accueillant les prototypes et démonstrateurs issus des avancées scientifiques du projet SuperviZ est l'objectif du lot 6. Physiquement la plateforme sera distribuée sur les sites des partenaires permettant la mutualisation du matériel et cas d'usage en priorité aux partenaires du projet mais aussi aux membres de la communauté académique nationale et aux industriels intéressés. Ce document présente le catalogue des services et cas d'usage disponibles au début du projet. Il sera enrichi au fil du temps, suivant le rythme des développements. Certaines plateformes permettant l'implémentation de cas d'usage dans plusieurs domaines, la présentation est organisée par partenaire.

2 Synthèse des plates-formes

Nous donnons ici un tableau de synthèse de toutes les plates-formes, reprenant les informations qui sont données dans les tableau de synthèse des diverses section dédiées aux diverses plateformes, puis nous commentons ces informations de synthèse et nous positionnons les diverses plateforme les unes par rapport aux autres.

Partenaire	PoC	Nom	Description succincte	Format des données	Activité normale	Activité malveillante	Accès
CEA	Radhouene Azzabi et Philippe Limousin	COSY	Supervision interactive pour la cybersécurité	La plateforme permet d'aggréger les données quel que soit leur format pour afficher une représentation globale du système. Plusieurs formats ont déjà été connectés à la plateforme de supervision : Logs systèmes (syslog) et réseaux (fichiers pcap transformés en log format Zeek)	Monitoring réseau et mises en oeuvre des mécanismes de sécurité end-to-end (gestionnaire d'identité et d'autorisation, PKI, gestionnaire d'intégrité...) Ce monitoring est réalisé avec des IHM couplées à de l'IA pour visualiser l'ensemble des données et apporter de l'aide à la décision	Testbed de monitoring d'attaque cyber allant de la détection, au suivi de la propagation jusqu'à la remédiation. Plusieurs techniques d'attaque : vulnérabilité RCE, force brute SSH, interception de données (man-in-the-middle), injection de paquets, déni de service	Accès possible sur place mais sur demande avec un accès réseau aux membres du projet

Partenaire	PoC	Nom	Description succincte	Format des données	Activité normale	Activité malveillante	Accès
IMT Atlantique	Fabien Autrel	Plateforme IMT Atlantique	Equipements contrôle/ commande autour des systèmes de simulation de processus industriels	Trace réseau (.pcap)	Supervision industrielle (SCADA)	Exploitation de vulnérabilité sur module réseau TCP modbus. Lecture et écriture dans des registres modbus	Accès uniquement possible sur place à l'heure actuelle
IMT-TSP	Gregory Blanc	VARIoT	Objets IoT smart home	Flux réseaux (pcap, csv)	Communications entre objets connectés et avec le contrôleur smart home	Aucune	Local
IMT-TSP	Sondos Abuzant et Gregory Blanc	CERES	Système CVC	Flux réseaux (pcap, csv)	Communications entre capteurs / actionneurs et système SCADA	Aucune	Local, accès restreint (ZRR)
UL-LORIA	Abdelkader Lahmadi	MICRO-GRID	Plateforme d'un micro-réseau électrique	Flux réseaux (pcap)	Communication normale entre les contrôleurs pour synchroniser d'une façon distribuée un niveau de voltage	Attaques réseau (DoS, MitM) pour désynchroniser les contrôleurs	Local sur place, données publiques

Partenaire	PoC	Nom	Description succincte	Format des données	Activité normale	Activité malveillante	Accès
LAAS-CNRS	Florent Galtier	LAAS-MIRAGE	Plateforme détection intrusion IoT	Logs Mirage au format texte, signaux au format CF32	Communications entre objets connectés avec différents protocoles (BLE, IEEE 802.15.4, WiFi...)	Attaques réseau exécutées par Mirage (MitM, jamming, injection de trames) selon le protocole	En ligne
G-INP	Stéphane Mocanu	G-ICS	Plateforme systèmes industriels	Réseau (pcap)	Plusieurs types (protocoles) de trafic industriel selon maquette. L'activité normale correspond aux échanges de données entre les contrôleurs afin de piloter le processus industriel en régime nominal (conforme aux spécifications d'exploitation).	Attaques orientées processus exploitant les vulnérabilités des protocoles industriels et/ou équipements	Local, ou indirect via portail, données publiques

Partenaire	PoC	Nom	Description succincte	Format des données	Activité normale	Activité malveillante	Accès
INRIA	Matthews José, Jérôme François	Réseaux programmables	Equipements réseaux programmables software et hardware (switch P4, smartNICs)	Logs contrôleur réseau, virtualisation	Défini par l'utilisateur (possible via Trex)	Défini par l'utilisateur (possible via Trex)	Accès partiel en ligne

Les plateformes participant au projet SuperviZ sont dédiées majoritairement aux systèmes industriels (CERES, G-ICS, MICROGRID et IMT Atlantique) aux IoT (VARIoT et Mirage) mais aussi aux réseaux programmables (Inria-Loria) ou à la supervision globale de sécurité (COSY). Les cas d'usage disponibles couvrent la domotique (VARIoT) et l'embarqué (Mirage et MICROGRID), le contrôle/commande industriels (CERES, G-ICS et IMT Atlantique) l'infrastructure (Loria) ou les systèmes complexes (COSY).

Les plateformes IMT Atlantique et G-ICS présentent de nombreuses similarités (maquettes identiques Fishertechnik, cas d'usage contrôle/commande proches). Les autres plateformes sont plutôt complémentaires ; ainsi COSY par exemple fusionne des donnés en provenance des IoT domotiques et cartes embarquées, les briques technologiques et outils développés étant ainsi compatibles avec les technologies étudiées par VARIoT, Mirage et MICROGRID voire même CERES sur le cas d'usage gestion du bâtiment. La plateforme MICROGRID est construite autour d'une architecture de réseau programmable OpenFlow et peut tirer ainsi profit des scénarios étudies sur la plateforme réseaux programmables INRIA-LORIA.

Les développements à venir pourraient concerner la mise-en-place des protocoles d'expérimentation communs entre les plateformes « systèmes industriels » permettant de tester une méthodologie de détection sur plusieurs cas d'usage différents ou de renforcer le rapprochement entre les plateformes complémentaires.

Concernant les développements matériels futurs sur les diverses plateformes un certain nombre des points d'attention peuvent être relevés. En se basant sur l'expérience de développement de la plus ancienne des plateformes (G-ICS démarrée en 2014), on peut lister les enseignements tirés de l'expérience suivants.

Maintenance logicielle : souvent les implémentations d'attaque et les prototypes d'IDS sont réalisés dans la partie expérimentale d'une thèse. Les changements des versions des OS, des compilateurs et des environnements rendent, à terme, inopérables les logiciels. Un supporte en développement continu est indispensable.

Maintenance matérielle : les maquettes et plateformes systèmes industriels sont particulièrement vulnérables à l'absence de maintenance matérielle en raison de la présence du processus physique prône aux défaillances matérielles. Une documentation complète de la partie opérative (physique), de la commande et des interfaces électroniques accompagnées d'un supporte technique compétent et continu est indispensable.

Obsolescence des équipements : malgré la longue période de vie des équipements industriels il arrive que des gammes de produits soit discontinués pour des raisons commerciales. Bien que difficile à réalisé en environnement universitaire, un stock de références est nécessaire afin de prolonger la durée de vie des maquettes.

3 CEA Toulouse Plateforme technologique COSY

3.1 Tableau de synthèse

Partenaire	CEA
Point de contact	Radhouene AZZABI et Philippe LIMOUSIN
Nom/titre	COSY
Description succincte	Supervision interactive pour la cybersécurité
Format des données	La plateforme permet d'aggréger les données quel que soit leur format pour afficher une représentation globale du système. Plusieurs formats ont déjà été connectés à la plateforme de supervision : Logs systèmes (syslog) et réseaux (fichiers pcap transformés en log format Zeek) ;
Activité normale	Monitoring réseau et mises en oeuvre des mécanismes de sécurité end-to-end (gestionnaire d'identité et d'autorisation, PKI, gestionnaire d'intégrité...) Ce monitoring est réalisé avec des IHM couplées à de l'IA pour visualiser l'ensemble des données et apporter de l'aide à la décision
Activité malveillante	Testbed de monitoring d'attaque cyber allant de la détection, au suivi de la propagation jusqu'à la remédiation. Plusieurs techniques d'attaque : vulnérabilité RCE, force brute SSH, interception de données (man-in-the-middle), injection de paquets, déni de service
Accès	Accès possible sur place mais sur demande avec un accès réseau aux membres du projet

3.2 Description libre

La plateforme CEA COSY est un environnement physique et numérique dédié à la conception et à la mise en œuvre de nouvelles solutions logicielles répondant aux défis de la gestion et de la visualisation d'informations massives et complexes. Elle fournit un environnement pour l'expérimentation, le prototypage, l'évaluation et l'innovation. L'équipe travaillant sur cette plateforme est composée d'ingénieur-chercheurs en ingénierie logicielle avec de fortes composantes en IHM, en architecture logicielle et en cybersécurité. Les activités techniques menées se regroupent autour de la supervision interactive et sécurisée de systèmes complexes. Cette mission se décompose en trois axes :

- AXE 1 : Intégration de briques technologiques logicielles et matérielles innovantes issues du CEA ou de ses partenaires académiques ;
- AXE 2 : Développement d'outils innovants en supervision & gestion de crise (civiles, industrielles, cyber) ;
- AXE 3 : Développement de socles numériques permettant l'interopérabilité de solutions logicielles de différents niveaux de maturité (cellule numérique de crise, usine-école).

Ces activités facilitent l'intégration de briques technologiques logicielles et matérielles innovantes issues des laboratoires du CEA et permettent le développement de nouvelles méthodes / outils adaptés aux besoins des utilisateurs finaux. Les développements sont ainsi guidés par une approche centrée sur l'utilisateur et permettent la mise en place de démonstrateurs de bout en bout. Des plateformes logicielles similaires à des jumeaux numériques ont donc été développées pour la gestion de situations

FIGURE 1 – Plateforme COSY avec l'utilisation de différents supports de visualisation & d'interaction avec les données

complexes (gestion de crise civile, industrielle, cybersécurité et pilotage énergétique). Elles permettent la collecte de données (massives, hétérogènes de différentes sources), l'analyse de celles-ci pour l'aide à la décision (IA, simulation, optimisation) associés à des techniques de visualisation et de manipulation des données dédiées aux utilisateurs finaux (IHM innovantes, multi-dispositifs).

3.3 Description technique

3.3.1 Environnement matériel

L'environnement matériel de la plateforme COSY est représenté à travers la figure suivante et va être détaillé par la suite.

FIGURE 2 – Représentation de la plateforme COSY et de l'environnement matériel associé

1. Serveurs de données
   — Espace de stockage 10 To
2. Serveurs de calcul
   — CPU - 6 serveurs PowerEdge
   — GPU - 2 x 2 Tesla K20X
3. Pupitre opérateurs
4. Interface mobile - table tactile
5. Architecture réseau reconfigurable
   — Firewall cisco ASA

— Switch/Routeur Cisco
— Borne Wifi TPLINK (2.4 et 5Ghz)

6. Equipement de supervision
   — Mur d'écran 2x2 SAMSUNG UD55D
   — Tableau blanc interactif
7. Ensemble d'objets IoT
   — Capteurs ZWave MultiSensor6
   — Gateways RPI avec dongle usb Zwave
   — Gateway LoRaWan
   — Capteur Qualité d'air indoor LoRaWan
   — Station Météo - Netatmo NSWS01-WW
   — Contrôleur de conso électrique Voltaware GC-VOLTA
   — Prise connectée - Fibaro FGPWE-102-ZW5

3.3.2 Environnement logiciel

La plateforme COSY est composée de différentes solutions :

— Serveur de virtualisation openStack (réinstallation en cours) ;
— Serveur d'authentification Keycloak ;
— Base de données (InfluxDB, MongoDB, PostreSQL etc...) ;
— Serveur de SIG (Geoserveur) ;
— Splunk SIEM utilisé pour les besoins internes en développement d'applications tiers pour les opérateurs de SOC
— Démonstrateur de honeyPOT – Tpot

3.3.3 Moyens de supervision et de développement

L'environnement logiciel de la plateforme COSY a été développé par plusieurs permanents de l'équipe sur des volets transverses tels que l'IHM, la cybersécurité, l'IoT, l'usine 4.0 ou la gestion de crise. L'ensemble des développements issus de projets doivent s'intégrer à l'environnement logiciel de la plateforme en tant que brique technologique réutilisable et améliorable dans d'autres projets. Un ingénieur-chercheur est dédié au suivi et l'orchestration des solutions au sein de la plateforme et leur intéropérabilité avec des solutions de partenaires extérieurs.Des experts techniques de chaque volet cités précédemment participent également au développement d'une roadmap commune en apportant leurs contraintes et volontés en fonction de leur expertise.

3.3.4 Contraintes d'usage

La plateforme COSY devra intégrer les résultats des autres lots du projet dans un contexte d'évaluation à travers des démonstrateurs de bout en bout. En effet, la plateforme sera composée d'un environnement de développement et d'évaluation des solutions guidées par une approche centrée utilisateur. L'équipe de la plateforme COSY se chargera de développer les interfaces dédiées en collaboration avec les autres partenaires du projet. Les travaux prospectifs permettront, sur la base de scénarios d'usage, de proposer de nouvelles solutions de visualisation et d'interaction. Les travaux menés doivent se faire en étroite collaboration avec les autres plateformes et partenaires du projet. Ceci amène donc une contrainte d'utilisation à étudier en particulier pour l'interconnexion avec les autres plateformes proposant notamment un environnement matériel. En ce qui concerne les accès aux démonstrateurs, le CEA étudiera la possibilité de fournir un accès réseau aux membres du projet.

Dans le but de valoriser les résultats du projet, cette plateforme servira de vitrine pour démontrer les résultats finaux du projet.

3.4 Description des cas d'usage normaux

Voici des exemples concrets de projets réalisés sur la plateforme permettant ainsi de comprendre son fonctionnement qui se base sur des activités normales de systèmes industriels :

- ADViz : Un outil numérique pour la contextualisation et la visualisation de menaces cyber à destination des opérateurs de SOC. L'outil ADViz permet d'aider l'opérateur de SOC à investiguer et contextualiser les menaces cyber. Cette investigation se fait au moyen d'un couplage fort entre des outils dédiés de manipulation et d'affichage 2D/3D de données complexe et des outils en intelligence artificielle permettant la clusterisation et l'identification des menaces cyber sur son système.
- CrizLAB^{TM} : Un middleware, au service de la gestion de crise, qui permet l'interconnexion des différents outils utilisés pendant une crise (main courante, tableau de bord...) et une visualisation de données complexes. Cette solution permet donc (a) la collecte de données massives et hétérogènes (exemples : capteurs hydrométriques, décision d'évacuation d'un quartier), (b) de fournir une représentation de la situation et (c) de proposer des outils d'aide à la décision grâce à des solutions d'IA connectées à CrizLAB^{TM}.
- E-spoc : Supervision 3D d'une infrastructure IoT dans le cadre des villes intelligentes avec déploiement d'un framework de sécurité de bout en bout. Cette supervision représente en 3D des remontées de capteurs (type : capteur de présence) sur une installation et met en avant les résultats des outils de suivi de la sécurité des données et de l'intégrité des capteurs. Le framework de sécurité de bout en bout a consisté à développer un gestionnaire d'identité et d'autorisation, une infrastructure de gestion de clés et de certificats (PKI), un gestionnaire d'intégrité, un système d'anonymisation et pour finir un système d'audit et d'attestation des composants IoT.

3.5 Description des attaques implémentées

L'équipe CoSy a mis en place, dans un contexte de projet interne, un environnement virtuel de test qui simule plusieurs installations industrielles. Le but de cet environnement est de collecter des données réalistes afin de soutenir les travaux sur de nouveaux mécanismes de sécurité et des outils d'analyse post attaques. Le testbed comprend trois sous-réseaux pour la supervision, la commande et les opérations (simulant une activité d'un ensemble d'automates en ModbusTCP et OPCUA), un routeur-firewall qui autorise uniquement le flux entre la commande et la supervision, un analyseur de réseau (Zeek [1]) et un IDS (Suricata [2]). Les journaux collectés sont stockés dans une base de données Elasticsearch [3] et également dans une base de données graphique (Dgraph [4]).

Pour simuler des activités malveillantes, un scénario d'attaque a été mis en place, impliquant le scan de réseaux, l'exploitation d'une vulnérabilité RCE (CVE-2021-42013) sur un serveur web vulnérable, le déplacement latéral depuis le serveur attaqué en lançant une attaque par force brute SSH sur un relais vulnérable, une attaque de l'installation industrielle (OPCUA et ModbusTCP) par interception de données (man-in-the-middle), l'altération de données (injection de paquets) et enfin l'exécution d'un déni de service.

1. https://docs.zeek.org/en/master/logs/index.html
2. https://docs.suricata.io/en/suricata-6.0.0/index.html
3. https://www.elastic.co/fr/elasticsearch
4. https://dgraph.io/docs/dgraph-overview/

Ce scénario d'attaque, bien que complexe, a permis à l'attaquant de perturber l'ensemble de l'infrastructure et de manipuler certains automates. Les compétences acquises dans cette simulation pourront être utilisées pour concevoir des scénarios d'attaque similaires pour le projet SuperviZ ou pour développer des scénarios plus complexes.

3.6 Lien avec les datasets

La plateforme COSY ne génère actuellement pas de jeu de données pour le projet SuperviZ mais utilise des datasets existantes listées ci-dessous afin de développer, évaluer et tester ses principales briques technologiques (IHM dédiées à la visualisation de données massives ; détection, suivi, remédiation d'attaques à base d'IA) :

- Jeu de données interne CEA (COSY-ICS : log réseaux en format pcap et Zeek, log IDS 'Suricata", log Firewall en "Syslog")
- Jeu de données interne CEA (Logs DNS et systems)
- Jeu de données public (Splunk/BOTSv1 [5])
- Jeu de données public (OPCUADataset [6])
- Jeu de données public (CIC-IDS2017 [7])

3.7 Liste de publications commentée

[1] Radhouene Azzabi, Cédric Gouy-Pailler, François Valley, and Hubert Dubois. Visualization and machine learning for interactive cyber threats analysis in critical infrastructures. In *Proceedings of the 2nd Inter-national Conference on Nuclear Security (ICONS 2020)*, Vienna, Austria, February 2020. Présentation d'un outil numérique pour la contextualisation et la visualisation de menaces cyber pour les opérateurs de SOC. L'outil aide les opérateurs dans l'investigation des attaques en combinant des techniques de visualisation de données en 3D et de l'IA. pour la clusterisation et l'identification des menaces.

[2] Laurence Boudet, Jean-Philippe Poli, Louis-Pierre Bergé, and Michel Rodriguez. Situational assessment of wildfires : a fuzzy spatial approach. In *2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI)*, pages 1180–1185, 2020. Cet article propose de coupler un SIG avec un système expert flou capable d'évaluer des règles spatiales floues, c'est-à-dire des règles floues intégrant des relations ou des propriétés spatiales. Celles-ci sont basées sur la morphologie mathématique floue et modélisent des relations métriques ou topologiques de haut niveau telles que "être proche de", "être dans la direction de" ou "être adjacent à". L'approche proposée a été appliquée à l'identification des risques dans le cas des incendies de forêt et pourrait être appliqué à d'autres domaines comme la cybersécurité.

[3] Philippe Limousin, Radhouene Azzabi, Louis-Pierre Bergé, Hubert Dubois, Sébastien Truptil, and Luc Le Gall. How to build dashboards for collecting and sharing relevant informations to the strategic level of crisis management : an industrial use case. In *2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, pages 1–8, 2019. Ce document développe une méthode générique pour créer des tableaux de bord dédiés à la phase de réponse à la gestion de crise. La proposition se concentre spécifiquement sur la méthode utilisée pour concevoir et développer le tableau de bord (Quelles informations doivent être hiérarchisées ? Comment afficher toutes les informations pertinentes ?) Cette approche est illustrée par un cas d'utilisation sur un site industriel.

5. https://github.com/splunk/botsv3
6. https://digi2-feup.github.io/OPCUADataset/
7. https://www.unb.ca/cic/datasets/ids-2017.html

[4] Georgios Palaiokrassas, Petros Skoufis, Orfefs Voutyras, Takafumi Kawasaki, Mathieu Gallissot, Radhouene Azzabi, Akira Tsuge, Antonios Litke, Tadashi Okoshi, Jin Nakazawa, and Theodora Varvarigou. Combining blockchains, smart contracts, and complex sensors management platform for hyper-connected smartcities : An iot data marketplace use case. *Computers*, 10 :133, 10 2021. Cette article combine la technologie Blockchain avec des objets IoT et des frameworks de securité. Les données proviennent ainsi de multiples sources utilisant des systèmes indépendants pour la collecte, le stockage et l'utilisation des données. Nous retrouvons dans cette article les principes d'interopérabilité, d'efficacité et de protection des données qui ont été intégrés dans la plateforme COSY .

[5] Sébastien Truptil, Philippe Limousin, Louis-Pierre Bergé, Radhouene Azzabi, and Hubert Dubois. Towards a unified approach of interoperability to facilitate the transfer from research to industry : Application to crisis management. In Martin Zelm, Bob Young, Guy Doumeingts, Hedi Karray, and Linda Elmhadbhi, editors, *Proceedings of Interoperability for Enterprise Systems and Applications Workshops co-located with 10th International Conference on Interoperability for Enterprise Systems and Applications (I-ESA 2020), Tarbes, France, November 17-19, 2020*, volume 2900 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2020. Ce projet vise à combler le fossé entre la recherche et les parties prenantes de la gestion de crise. Ce fossé est essentiellement dû à un manque de maturité et à un problème d'interopérabilité des résultats des projets de recherche et développement. Par conséquent, cet article présente l'architecture logicielle de CrizLAB^{TM}, un logiciel intermédiaire basé sur une architecture pilotée par des événements (EDA) qui propose une approche unifiée de l'interopérabilité et aide à utiliser les résultats des projets de R&D dans des situations pertinentes afin d'accroître leur maturité et de faciliter ainsi les démonstrations.

4 IMT Atlantique Rennes Plateforme technologique systèmes industriels

Cette plateforme réunit plusieurs types d'équipements contrôle/commande autour des systèmes de simulation de processus industriels.

4.1 Tableau de synthèse

Partenaire	IMT Atlantique
Point de contact	Guillaume Doyen et Fabien Autrel
Nom/titre	Plateforme IMT Atlantique
Description succincte	équipements contrôle/commande autour des systèmes de simulation de processus industriels
Format des données	Logs systèmes et réseaux
Activité normale	Supervision industrielle (SCADA)
Activité malveillante	Exploitation de vulnérabilité sur module réseau TCP modbus. Lecture et écriture dans des registres modbus
Accès	Accès uniquement possible sur place à l'heure actuelle

4.2 Description libre

La plateforme de l'IMT Atlantique sur le site de Rennes est construite autour de modèles réduits de processus industriels et des simulations de tels processus. Le pilotage des maquettes et simulations se fait à l'aide de différents automates. Le but de cette plateforme est l'implémentation de systèmes d'information spécifiques au contexte industriel couplés aux maquettes et simulations pilotées par les automates. Ces implémentations permettent entre autre la génération de datasets et le test de composants de sécurité développés à IMT Atlantique ou chez les partenaires de l'école.

4.3 Description technique

Les maquettes de processus industriels utilisés sur la plateforme de IMT Atlantique sont des modèles réduits fabriqués par l'entreprise Fischertechnik. Ils ont la particularité de pouvoir être contrôlés par n'importe quel automate industriel. Ainsi il est possible d'utiliser différents automates et les protocoles qui leurs sont propres dans des expérimentations. D'autre part, des malettes de simulation de l'entreprise Diateam, des valises d'entrainement Siemens et des bancs de chauffage de la marque Schneider sont utilisés. Il est à noter que les malettes Siemens et les bancs Schneider ne sont pas initialement conçus spécifiquement pour l'intégration à des plateformes de recherche en cybersécurité mais plutôt pour de la formation à l'automatisme.

4.3.1 Environnement matériel

Implémentations basées sur les modèles Fischertechnik :

— Chaine d'usinage (figure 3). Maquette composée de 4 modèles assemblés pour former une chaîne d'usinage en boucle fermée : une pièce traitée par la chaîne est ensuite repositionnée au début de la chaîne, ce qui permet de faire fonctionner le système en continu sans intervention humaine.

Cette maquette est pilotée par 3 automates Crouzet comprenant un module TCP/modbus. Les automates sont connectés à la maquette via 4 cartes d'entrées/sorties, à savoir une carte par modèle. Cette maquette est fonctionnelle.

— Usine Fischertechnik (figure 4). Maquette comprenant une zone de stockage, une ligne de tri avec capteur de couleur, une simulation de four et un bras de manipulation des pièces à traiter. Cette maquette est actuellement partiellement piloté par 3 automates industrial shields. Pour un usage complet, il reste à compléter la programmation des automates. Il est à savoir que la société Siemens fourni les programmes pour les automates S7 1500 de chez Siemens mais certains modules d'entrée/sortie spécifiques doivent être utilisés.

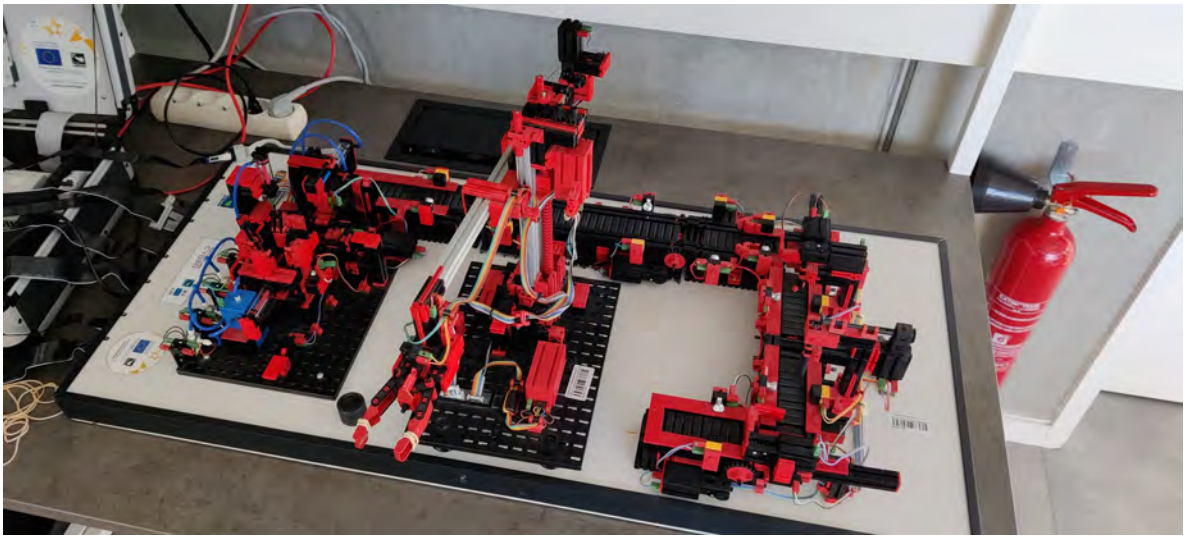

FIGURE 3 – Chaine d'usinage Fischertechnik composée de 4 modèles assemblés

Valises d'entraînement Siemens SIMATIC S7 Training Case S7-1500 : Chaque valise est composée d'un automate S7-1500 (figure 5). Elles sont à l'origine destinée à former des personnes aux outils Siemens, elles sont utilisées pour piloter des maquettes Fishertechnik (en cours d'intégration). 5 exemplaires sont disponibles.

Chaque valise comprend les composants suivants :

— PLC SIMATIC CPU 1513F-1 PN avec PM1507, entrées/sorties analogues et numériques
— ET 200SP avec IM 155-6 PN, entrées/sorties analogues et numériques. Le module ET 200SP communique avec le PLC via un bus PROFINET
— Panneau tactile TP700

Pour l'instant une partie des capteurs et actionneurs tout ou rien des maquettes Fischertechnik IIOT4 sont connectés au S7-1500.

Bancs de chauffage Schneider MD1AE 895 P A l'origine destiné à former des personnes aux outils Schneider et à l'automatisme (figure 6). A été utilisé en TP avec les élèves ingénieurs pour les sensibiliser sur l'absence de mécanismes de sécurité dans le protocole modbus. 5 exemplaires sont disponibles. Un banc est constitué comme suit :

— Partie opérative : la partie opérative représente une installation de chauffage central à eau chaude. Elle est constituée de :

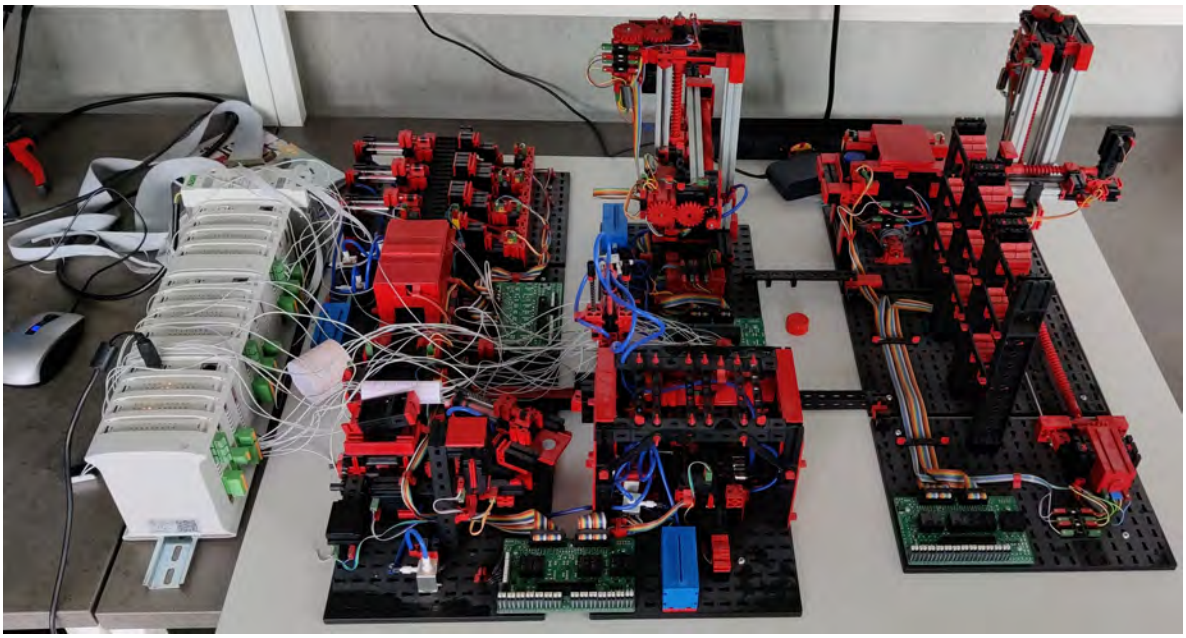

FIGURE 4 – Chaine de traitement Fischertechnik

FIGURE 5 – Valise Siemens SIMATIC S7 Training Case S7-1500

- Un chauffe-eau à accumulation
- Un bloc sécurité associé à un vase d'expansion
- Une vanne proportionnelle motorisée 3 voies actionnée par l'automate pour assurer la régulation de la température dans le circuit
- Un circulateur électrique pour forcer la circulation de l'eau
- Un radiateur simple panneau qui assure la dissipation de la chaleur
- Placé sous le radiateur, un groupe de trois ventilateurs assure une convection forcée de l'air autour du radiateur et provoque ainsi une perturbation contrôlée du système

— Partie commande : au dos de la partie opérative se trouve la partie commande :
- Un terminal de dialogue homme-machine Magélis à écran graphique et tactile qui assure la supervision et la commande du système
- Un automate Premium qui assure le contrôle de l'ensemble de la partie opérative. Il est constitué de :
  - Un processeur 1024 entrées / sorties TOR, 80 entrées / sorties analogiques, 1 connexion Ethernet TCP/IP
  - Un module 8 entrées analogiques
  - Un module 8 sorties analogiques
  - Un module 16 entrées TOR
  - Un module 8 sorties TOR
- Les sondes installées sur le système sont les suivantes :
  - Température d'eau chaude en entrée du radiateur
  - Température d'eau froide en sortie du radiateur
  - Température d'eau froide en retour sur la vanne trois voies
  - Température d'air chaud sortie de radiateur
  - Température d'air ambiant

Valises Diateam SCADAVIRT Ces valises intègrent deux automates : un M251 Schneider et un 1211C Siemens (figure 7). Les automates pilotent respectivement une simulation de production de crème et de traitement d'eau (figure 8). Un scénario d'usage en sécurité montre qu'il est possible de perturber le fonctionnement de la simulation d'usine de production de crème via des commandes modbus.

Une valise est constituée comme suit :

— Composants :
- Afficheur tactile Proface SP5500
- Automate Schneider M251 (référence TM251MESC)
- Automate Siemens S7-1200 CPU 1211C
  - Référence CPU : 6ES7 211-1HE40-0XB0
  - Référence module de communication : 6ES7 241-1CH30-1XB0

— Les PLCs sont configurés comme tel :
- Schneider M251 :
  - 2 ports Ethernet en série
  - Serveur FTP (activé par défaut)
  - Serveur web (activé par défaut)
  - Liaison série Modbus RTU (native)
  - Serveur Modbus TCP
  - Serveur soMachine (protocole propriétaire)
- Siemens S7-1200 CPU1211C :
  - Serveur FTP (non activé par défaut)

FIGURE 6 – Banc de chauffage Schneider MD1AE 895 P

FIGURE 7 – Valise Diateam SCADAVIRT

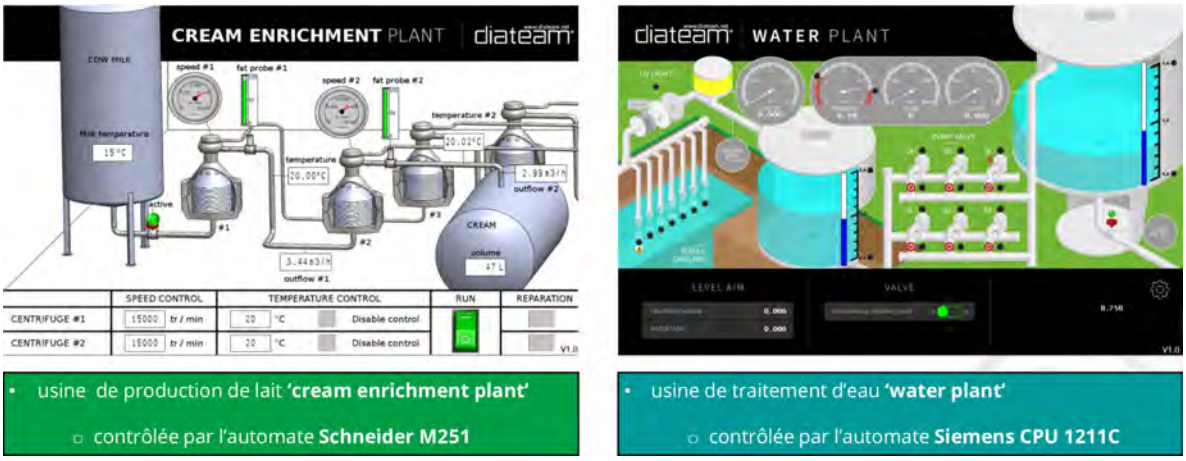

FIGURE 8 – Simulations des usines d'enrichissement de crême et de traitement d'eau

— Serveur web (non activé par défaut)
— Liaison série Modbus RTU (extension)
— Communication S7

4.3.2 Environnement logiciel

Les outils spécifiques à chaque constructeur d'automate sont utilisés pour les programmer. La seule exception concerne les automates industrialshields qui sont basés sur des contrôleurs arduino. Pour ces automates, il est possible d'utiliser tous les outils compatibles avec les contrôleurs arduino. En l'occurence l'outil embrio a été utilisé (https://www.embrio.io).

Concernant la chaine d'usinage (figure 3), les automates Crouzet qui la pilotent sont connectés à un système d'information virtualisé constitué de 2 machines virtuelles :

— La première machine est une machine de supervision sur laquelle est exécuté une interface graphique développée en interne en Java. Cette interface de supervision communique avec les automates via le protocole modbus/TCP pour récupérer certaines variables d'état du processus industriel pour afficher son état courant.
— La deuxième machine est une machine Linux Kali utilisée pour attaquer les automates.

4.3.3 Moyens de supervision et de développement

Actuellement seule la chaine d'usinage (figure 3) est équipée d'une instance de wireshark pour capturer le traffic entre les machines virtuelles et les automates.

4.3.4 Contraintes d'usage

Les maquettes ne sont pas connectées à Internet. Elles ne peuvent pas être utilisées à distance car elles nécessitent la présence d'un opérateur. Les valises Diateam peuvent éventuellement être mises en ligne, mais la réinitialisation de certaines variables d'état des simulation nécessite l'intervention d'une personne physique.

4.4 Description des cas d'usage normaux

L'activité normale des systèmes industriels implémentés par les maquettes correspond au fonctionnement normal du processus industriel. Dans ce mode de fonctionnement, le traffic réseau pouvant être capturé sur la maquette de chaine d'usinage (figure 3) correspond au traffic modbus entre l'interface de supervision et les automates.

4.5 Description des attaques implémentées

Deux attaques sont implémentées sur la maquette de chaine d'usinage (figure 3) :

— La première attaque consiste à exploiter une vulnérabilité découverte sur les modules réseau des automates Crouzet. Nous avons identifié une vulnérabilité dans l'implémentation du protocole modbus/TCP dans ces modules. Cette vulnérabilité a été découverte en utilisant un outil de fuzzing modbus. A l'éxécution de l'outil, il apparaît une impossiblité à communiquer avec les modules réseau Crouzet. Le paquet modbus déclenchant le redémarrage des modules a été identifié et un un script python permettant de rejouer l'attaque a été développé.

  Une attaque de type déni de service sur la supervision est implémentée en exploitant cette vulnérabilité, un script qui envoie en continu le paquet permettant de redémarrer les modules réseaux a été développé. Cette attaque n'influence pas l'exécution du processus industriel car le

module réseau contient un microcontrôleur indépendant de celui qui exécute le programme de l'automate.

— La seconde attaque consiste à exploiter le fait que certains registres modbus des automates sont accessibles en écriture, ce qui permet de modifier le comportement de la chaine pour stopper son fonctionnement et faire lâcher une pièce en cours de traitement par le bras robot. Une fois le processus industriel en cours dexécution, un script python permet de générer les commandes modbus pour modifier deux variables d'état des automates : la première variable d'état permet d'arrêter complétement la chaine, et la deuxième permet d'ouvrir la pince du bras robot à n'importe quel moment.

4.6 Lien avec les datasets

Le traffic d'attaque correspondant au déni de service détaillé dans la section précédente a été capturé sous la forme d'un fichier pcap.

.

4.7 Liste de publications commentée

[1] Simon N. Foley, Fabien Autrel, Edwin Bourget, Thomas Cledel, Stephane Grunenwald, Jose Rubio Hernan, Alexandre Kabil, Raphael Larsen, Vivien M. Rooney, and Kirsten Vanhulst. Science hackathons for cyberphysical system security research : Putting cps testbed platforms to good use. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, CPS-SPC '18, page 102–107, New York, NY, USA, 2018. Association for Computing Machinery. La maquette de chaine d'usinage FisherTechnik a été utilisée dans le cadre d'un hackathon regroupant plusieurs doctorants de la chaire cyber CNI.

5 Télécom SudParis Evry Plateforme VARIoT

Partenaire	IMT-TSP
Point de contact	Gregory Blanc
Nom/Titre	VARIoT
Description succinte	Plateforme smart home
Format des données	Réseau (pcap, csv)
Activité normale	Communications entre objets connectés (WiFi, Zigbee, Z-Wave) et avec un contrôleur smart home (MQTT)
Activité malveillante	Aucune
Accès	Local (scénario ou script d'interaction à fournir)

5.1 Description libre

La plateforme VARIoT vise à reproduire un environnement de type smart home où des objets connectés interagissent avec leur environnement de manière intelligente. Dans un premier temps, VARIoT permet de monitorer les activités des objets déployés dans différentes pièces. Les interactions originellement humaines sont graduellement remplacées par des interactions automatisées et les données sont collectés au niveau réseau et système. Les données produites par les objets connectés pourront servir de données d'entraînement à un détecteur d'anomalies. Plus tard, seront définis plusieurs scénarios d'attaque afin d'évaluer les capacités de détection.

5.2 Description technique

La plateforme VARIoT étend les fonctionnalités d'une plateforme de contrôle d'objets connectés telles que OpenRemote[8]. Elle enrichit une telle plateforme avec des outils permettant d'interagir avec les objets et de réaliser des tests spécifiques sur ces objets. La plateforme VARIoT est constituée de 3 composants : les objets connectés (IoT), la plateforme IoT OpenRemote, et une suite d'outils, dénommée IBPS, développée à Télécom SudParis par le département Informatique. Pour le moment, elle permet de réaliser des tests de performance sur les objets connectés et de stocker des résultats plus détaillés de ces tests afin de comparer différents objets, permettant aux usagers de prendre une décision éclairée sur l'objet le plus adapté. À l'heure actuelle, les 3 composants communiquent en utilisant le protocole MQTT.

5.2.1 Environnement matériel

En tout, 30 objets sont déployés dans 4 salles distinctes au troisième étage du bâtiment ETOILE à Télécom SudParis, qui sont nommés comme suit : l'`IoT Lab` lui-même divisé en trois espaces (`OpenSpace`, `Kitchen` et `Server`), le `Working space` et le `PhD office`. L'ensemble des objets communiquent selon 3 protocoles sans fil (WiFi, Zigbee et Z-wave). Les objets WiFi sont connectés via un router Netgear Orbi RBR350. Le route WiFi supporte les standards sans-fil 802.11ac et 802.11ax. De plus, un Raspberry Pi4B est déployé comme relais WiFi et capture le trafic entre le router WiFi et les objets communiquant sur ce protocole. Les objets Zigbee sont connectés à un hub WiFi Philips Hue Bridge, lui-même connecté au réseau via le Raspberry Pi4B. Le Rapsberry Pi4B opère un système

8. OpenRemote — The 100% Open Source IoT Platform. Lien : https://openremote.io/

OpenWRT pour router le trafic. Le trafic Zigbee entre le Bridge et les objets Zigbee peut aussi être observé en utilisant un dongle USB Zigbee. Enfin, le trafic des objets Z-wave est directement capturé par le serveur d'administration de la plateforme via un dongle USB Z-wave, Z-Stick Gen5, auquel est connecté les objets communiquant sur ce protocole. Ci-dessous se trouve une liste détaillée des objets de la plateforme. Certains n'utilisent qu'un des 3 protocoles cités ci-dessus (17 WiFi, 7 Zigbee, 6 Z-wave) et d'autres utilisent en plus d'autres protocoles filaire (Ethernet) et radio (Bluetooth, BLE) :

- 1 assistant vocal Amazon Echo Dot 3 (WiFi, Bluetooth)
- 1 assistant vocal Amazon Echo Show 5 (WiFi)
- 1 assistant vocal Google Home (WiFi, Bluetooth)
- 1 assistant vocal Google Home Mini (WiFi, BLE)
- 1 caméra D-Link DCS-8300LH-30B0 (WiFi, BLE)
- 2 caméras Google Nest Camera (WiFi, BLE)
- 1 thermostat Google Nest Learning Thermostat 3rd Gen (WiFi)
- 1 ampoule Philips Hue Go (Zigbee, Bluetooth)
- 4 ampoules Philips Hue A60 (Zigbee, Bluetooth)
- 1 ampoule TP-Link LB120 (WiFi)
- 1 prise Philips Hue Smart Plug (Zigbee, Bluetooth)
- 1 prise TP-Link HS110 Smart Plug (WiFi)
- 1 prise Logicom Pluggy (WiFi)
- 1 multi-prise Logicom Smart Strip (WiFi)
- 2 multi-prises Maxcio Smart Strip (WiFi)
- 2 sondes AEOTEC Multisensor 6 (Z-wave)
- 2 sondes de température Fibaro Door/Window Sensor 2 (Z-wave)
- 2 sondes Zipato Multisensor Quad (Z-wave)
- 1 détecteur de présence ESP32+ ToF distance sensor (WiFi)
- 1 détecteur de présence Philips Hue Motion Sensor (Zigbee)
- 1 tablette Samsung Tablet (WiFi)
- 1 téléviseur Sony KD-43XH8096 (WiFi)

La Figure 9 représente les connexions réseau entre objets déployés.

5.2.2 Environnement logiciel

OpenRemote permet de connecter les objets IoT et de les contrôler, notamment via des échanges de données. La plateforme OpenRemote emploie le protocole MQTT et un script Python afin d'établir des connexions avec les objets. Le script permet d'envoyer des commandes aux objets et de recevoir des données depuis ces objets. L'usage de cette plateforme permet de monitorer l'état des objets, de suivre leur historique et de définir des règles conditionnelles de fonctionnement.

Certains objets exposent des APIs directement accessibles par OpenRemote. Pour les objets Z-wave, l'API Domoticz [9] a été employée. Une seconde catégorie d'objets ne pouvant être directement accessibles via OpenRemote. Les outils IBPS ont permis de s'interfacer avec ceux-ci pour les contrôler.

Les outils IBPS sont conçus pour réaliser des tests d'évaluation. Ils se connectent à chaque objet et lancent une batterie de tests dont les résultats sont collectés, analysés et renvoyés à OpenRemote où ils sont interprétés et affichés à l'utilisateur.

Les outils IBPS sont écrits en Pythonet leurs principales fonctions incluent :

- inscription d'objets à des *topics* MQTT
- interagit avec les clients MQTT
- initialise et lance des tests de performance

9. domoticz : Open source Home Automation System. Lien : https://www.domoticz.com/

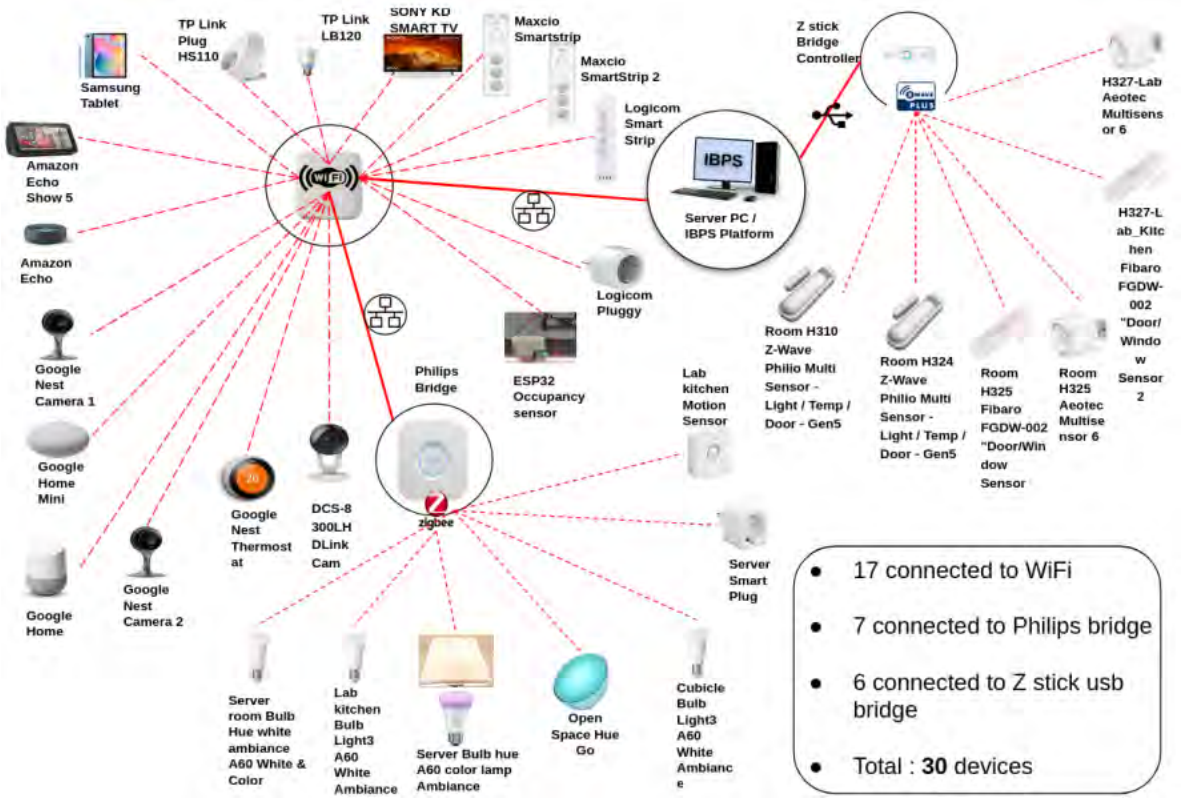

FIGURE 9 – Topologie réseau sans fil des objets déployés dans la plateforme VARIoT.

— collecte et impression d'informations concernant la consommation énergétique moyenne
— collecte et analyse le trafic Zigbee
— calcule la latence en utilisant ICMP
— interagit avec le Raspberry Pi et le serveur d'analyse

Les outils IBPS sont déployés sur différents équipements du réseau : le Raspberry Pi4B qui agit comme un relais WiFi, les dongles USB cc2531 (Zigbee) et Z-Stick Gen5 (Z-wave), permettant ainsi de communiquer avec les différents objets et de lancer les tests de performance.

5.2.3 Moyens de supervision et de développement

La supervision des objets connectés se fait via le contrôleur OpenRemote qui permet de collecter des métriques sur les objets connectés et de lancer des scripts à destination de ceux-ci via le protocole MQTT. Les scripts sont lancés de manière ponctuelle, mais peuvent être également programmés.

OpenRemote expose une interface Web permettant d'injecter des scripts ou de réutiliser des *templates*, afin d'étendre les capacités d'interaction avec les objets. Cependant, OpenRemote ne dispose pas d'interfaces de programmation pour tous les objets.

5.2.4 Contraintes d'usage

La plateforme n'est pour l'instant pas connectée à Internet et n'est donc accessible que physiquement. Elle est déployée à Evry dans la bâtiment ETOILE, au 3e étage. L'accès est limité au personnel de l'école.

Un nombre limité de scénarios d'attaque sont envisagés : capture et altération/rejeu de trafic, déni de service, usurpation d'identité, détournement d'un objet. Ils pourront être rejoués pour générer des données de trafic qui pourront être exportés (pcap, csv) et exploités a posteriori. À terme, les capacités de collecte seront étendues pour permettre de fournir des jeux de données issus de la plateforme aux partenaires et à la communauté plus largement. Puis, il pourra être envisagé que nous déployions des détecteurs fournis par les partenaires du projet SuperviZ afin d'évaluer leur capacité de détection dans cet environnement.

5.3 Description de cas d'usage normaux

Actuellement, la plateforme IBPS implémente des tests de performance sur les objets qui y sont déployés.

Un objet déployé dans la plateforme est accédé par la plateforme OpenRemote qui l'enregistre, assure son monitoring, affiche différents *Insights* –une interface graphique représentant les données métiers sous formes de graphes et de séries temporelles– et collecte un historique au format JSON.Des règles peuvent être créés pour automatiser le fonctionnement de l'objet. OpenRemote envoie des commandes via MQTT et collecte les données depuis les objets IoT.

Dans un second temps, les outils IBPS permettent de lancer des tests sur les objets, de capturer le trafic résultant des tests via les équipements de capture (Raspberry Pi4B pour les objets WiFi, dongle USB cc2531 pour Zigbee et Z-Stick Gen5 pour Z-wave). Les outils collectent les résultats de test via MQTT en plus du trafic capturé. Les résultats sont ensuite parsés afin d'en extraire les métriques à collecter, qui seront ensuite envoyées via MQTT à OpenRemote. OpenRemote permet de contrôler les outils IBPS pour identifier les objets IoT et configurer les tests.

5.4 Description des attaques implémentées

Pour le moment, aucun scénario n'a été défini et aucun logiciel d'attaque n'a été déployé.

5.5 Liens avec les datasets

Durant le projet VARIoT [10], des données ont été générées par interaction manuelle de sujets humains avec les objets connectés. Les interactions le plus souvent quotidiennes ont permis de générer entre quelques Mo à quelques Go de données par mois durant la majeure partie de la durée du projet. À partir des captures réseau (pcap), l'outil CICFlowMeter [11] a été utilisée pour extraire des caractéristiques de flux réseau au format csv. Ces données sont disponibles sur le portail `data.gouv.fr` regroupant 185 archives de captures quotidiennes, collectées entre Septembre 2020 et Décembre 2022 [12]. La version actuelle de la plateforme n'a pas encore produit de données.

5.6 Liste de publications commentée

[1] Houda Jmila, Gregory Blanc, Mustafizur R. Shahid, and Marwan Lazrag. A survey of smart home iot device classification using machine learning-based network traffic analysis. *IEEE Access*, 10 :97117–97141, 2022. Cet artice réalise une étude de l'état de l'art de l'analyse par apprentissage machine de trafic réseau issu d'objets IoT de type Smart Home. Les co-auteurs ont ainsi pu définir une taxonomie afin de classifier les différents travaux en fonction des méthodes d'acquisition de données, d'extraction de caractéristiques d'apprentissage, de méthodes de classification. Les co-auteurs, qui ont contribué eux-mêmes à la génération de données dans la plateforme VARIoT, donnent leur éclairage sur les autres travaux de l'état de l'art.

[2] Marwan Lazrag, Houda Jmila, Gregory Blanc, and Mustafizur R. Shahid. Dataset of legitimate iot data (variot). http://data.europa.eu/88u/dataset/617290e5562ea455d3d3ab0d, October 2021. Jeu de données de trafic légitime issu d'objets IoT déployés dans la plateforme VARIoT. Le jeu de données contient 185 jours de collecte.

[3] Mustafizur R. Shahid, Gregory Blanc, Houda Jmila, Zonghua Zhang, and Hervé Debar. Generative deep learning for internet of things network traffic generation. In *25th IEEE Pacific Rim International Symposium on Dependable Computing, PRDC 2020, Perth, Australia, December 1-4, 2020*, pages 70–79. IEEE, 2020. Cet article démontre la possibilité de générer un trafic synthétique d'objets IoT à partir d'une trace existante en utilisant une approche d'apprentissage générative. Les co-auteurs prennent pour source des échantillons issus du jeu de données collecté sur la plateforme VARIoT, afin de reproduire sur un nombre restreint de caractéristiques d'apprentissage, un trafic capable de confondre un détecteur d'intrusions.

10. Vulnerability and Attack Repository for IoT, projet CEF de la Commission Européenne nr. 28263632. Lien : https://www.variot.eu/.
11. https://github.com/ahlashkari/CICFlowMeter
12. *Dataset of Legitimate IoT data (VARIoT)*. Lien : https://www.data.gouv.fr/fr/datasets/dataset-of-legitimate-iot-data/.

6 Télécom SudParis Palaiseau Plateforme CERES

Partenaire	IMT-TSP
Point de contact	Sondos Abuzant, Gregory Blanc
Nom/Titre	CERES
Description succinte	Plateforme smart building
Format des données	Réseau (pcap, csv)
Activité normale	Trafic de sondes et d'actionneur CVC et communications avec le contrôleur SCADA (Modbus, OPC UA)
Activité malveillante	Aucune
Accès	Local (scénario ou script d'interaction à fournir)

6.1 Description libre

La plateforme CERES vise à émuler un système cyber-physique complexe de type smart building où un bâtiment équipé de sondes et d'actionneurs s'auto-régule. Dans un premier temps, CERES émule un premier sous-système, un système *CVC* (chauffage, ventilation, climatisation). Les données produites par le système CVC sont enregistrées pour servir de données d'entraînement à un jumeau numérique sur lequel seront simulées des attaques et des contre-mesures afin de prédire l'état de sécurité du système CVC.

6.2 Description technique

6.2.1 Environnement matériel

- 1 automate Schneider M580 (avec interface série, module OPC-UA et 4 entrées analogiques)
- 2 sondes d'humidité et de température 4-20 mA
- 2 sondes d'humidité et de température Modbus
- 1 variateur de vitesse ATV320
- 1 boîtier de raccordement Modbus-série
- 1 IPC 19" et logiciel EMSE
- 1 Harmony hub 5 sondes sans fil
- 1 centrale de mesure PowerLogic PM5320

La Figure 10 montre un aperçu des différents composants matériels qui constituent le système CVC déployé à Palaiseau.

6.2.2 Environnement logiciel

L'automate est contrôlable par le logiciel EcoStruxure Control Expert XL : il permet de générer le programme de contrôle exécuté par l'automate M580. Il permet la réception et le traitement des signaux générées par les capteurs (ici, les 8 sondes), la centrale de mesure et le variateur de vitesse. Il génère ensuite des signaux vers les actionneurs, ici le variateur de vitesse. Il traite également les ordre reçus du SCADA.

Le programme est écrit en langage Grafcet, qui représente le fonctionnement du programme en utilisant des états, des transitions et des branches. Chaque étape représente une section de code à l'aide d'un des 4 langages possibles (Function Block Diagram, Structured Text, Ladder, Instruction List).

FIGURE 10 – Aperçu des composants matériels de la plateforme CERES hors de leur boîtier : de g. à d., la connectique, les automates, les sondes, et l'interface homme-machine.

6.2.3 Moyens de supervision et de développement

La plateforme est assemblée et programmée principalement par une ingénieure plateforme. Des prestations de sous-traitance ont permis d'initialiser la programmation de l'automate et de l'outil de contrôle.

L'outil EcoStruxure ControlExpert de Schneider permet de superviser la plateforme et de programmer le programme de contrôle et d'acquisition des données (SCADA). De plus, un écran de contrôle externe permet à un opérateur de visualiser les données remontées par les sondes.

6.2.4 Contraintes d'usage

La plateforme n'est pour l'instant pas connectée à Internet et n'est donc accessible que physiquement. Cet accès est soumis à une autorisation d'accès à la Zone à Régime Restrictif (ZRR) de Télécom Paris à Palaiseau.

Un nombre limité de scénarios d'attaque sont envisagés : comme par exemple, capture et rejeu de trames, déni de service ou détournement de fonctionnement du contrôleur SCADA.Ils pourront être rejoués pour générer des données de trafic qui pourront être exportés (pcap, csv) et exploités dans un jumeau numérique Le jumeau numérique sera développé dans le cadre du projet CERES qui héberge cette plateforme. Eventuellement des contremesures proposées par des partenaires pourront y être déployées pour être évaluées.

6.3 Description de cas d'usage normaux

En fonctionnement nominal, le programme de contrôle est exécuté et collecte les données des capteurs. À intervalle régulier, la valeur en mémoire pour chacun des 8 appareils sont lues et placées dans les 8 tables de réception. Les données sont récupérées par le logiciel SCADA. Ensuite, le programme de contrôle reçoit et traite le retour du logiciel SCADA qui détermine la nouvelle vitesse cible pour le variateur de vitesse.

Ce cycle est répété toutes les 2 secondes.

6.4 Description des attaques implémentées

1 à 2 attaques seront implémentées dans un premier temps, notamment des attaques de rejeu et d'injection dans des protocoles industriels (Modbus, OPC UA), se basant sur la capture et la réémission des trames, altérées ou non.Pour le moment, aucun logiciel d'attaque n'est déployé.

7 Université de Lorraine (Loria) – Plateforme micro-réseaux électriques

7.1 Tableau de synthèse

Partenaire	UL-LORIA
Point de contact	Abdelkader Lahmadi (lahmadi@loria.fr)
Nom/Titre	LORIA-MICROGRID
Description succinte	Plateforme d'un micro-réseau électrique
Format des données	captures PCAP
Activité normale	communication normale entre les contrôleurs pour synchroniser d'une façon distribuée un niveau de voltage à générer
Activité malveillante	attaques réseau (DoS, MitM) pour désynchroniser les contrôleurs
Accès	Local sur place, données publiques

7.2 Description libre

Il s'agit d'une plateforme matérielle pour reproduire le fonctionnement d'un système de contrôle distribué pour un micro-réseau électrique. La plateforme implante des algorithmes de contrôle distribué pour synchroniser un niveau de voltage entre des unités génératrices. Le niveau de voltage est visible grâce à un niveau d'éclairage associé à une ampoule connecté à chaque unité. Les messages de synchronisation sont échangés sur un réseau de communication avec des switches OpenFlow et un contrôleur SDN. La plateforme offre la possibilité d'implanter des attaques de type DoS, MitM ou injection des fausses données pour désynchroniser les unités génératrices et affecter le niveau de l'éclairage. Elle offre également la possibilité d'expérimenter l'usage du protocole OpenFlow et des approches SDN pour appliquer des contre-mesures aux attaques développées.

7.3 Description technique

7.3.1 Environnement matériel

La plateforme comporte 4 unités génératrices. Chacune d'elle est composé de :
- contrôleur primaire : 1 raspberry Pi et 1 Arduino Mega 2560 board
- 2 moteurs pour générer du courant continu
- 1 ampoule pour visualiser la puissance délivrée
- 1 écran pour afficher la consigne de synchronisation en Volt

Elle comporte également 4 switches OpenFlow implantés dans des Raspberry Pi et totalement interconnectés entre eux. Chaque unité de distribution est connecté à un switch dédié. Chaque switch RaspBerry Pi possède également une connexion WiFi vers le contrôleur SDN.

7.3.2 Environnement logiciel

Les Arduino et les Raspberry Pi de chaque unité génératrice embarque le code de contrôle du système de synchronisation. Chaque Arduino comporte le code du contrôleur primaire pour réguler la vitesse du moteur pour générer le voltage souhaitée (la consigne). Le Raspberry Pi embarque le code

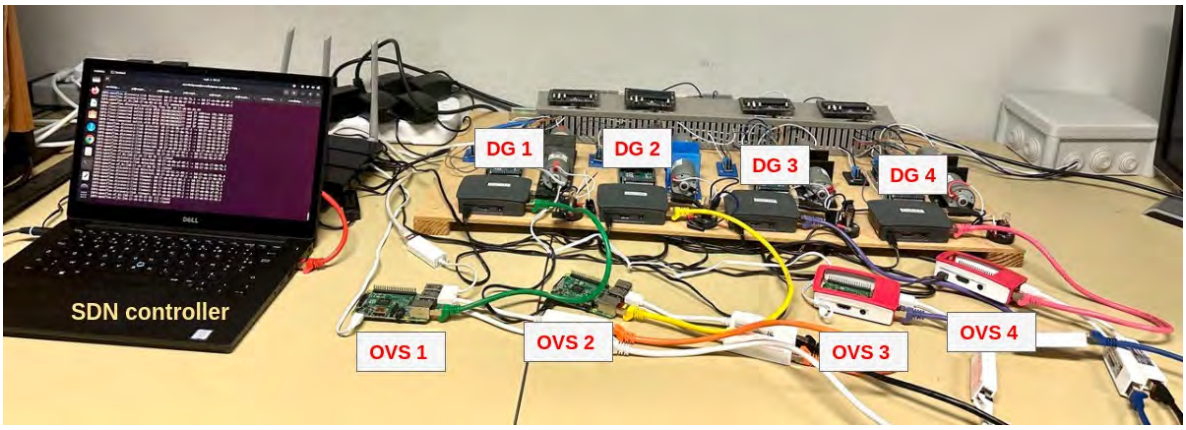

FIGURE 11 – Plateforme matérielle du micro-réseau électrique.

client et serveurs des contrôleurs distribués pour synchroniser les valeurs des mesures et consignes entre les 4 unités. Le switches réseaux basés sur Raspberry PI embarque un switch OVS (OpenFlow).

7.3.3 Moyens de supervision et de développement

Des accès SSH sont disponibles sur les différents Raspberry Pi pour lancer les contrôleurs, avoir accès aux switches OpenFlow et lancer des captures PCAP avec tcpdump.

7.3.4 Contraintes d'usage

L'accès à la plateforme est seulement local en physique pour mener les expérimentations et collecter des mesures et PCAP.

7.4 Description des cas d'usage normaux

En fonctionnement normal, un programme Python envoie une consigne de voltage avec une des unités génératrices qui la propage ensuite vers les 3 autres via le réseau de communication. La propagation vers les unités s'effectue sur un arbre de synchronisation programmé dans le code Python de chaque contrôleurs. Par exemple, la consigne est envoyé initialement vers DG1 qui la transmet ensuite à DG2 et DG3. Ensuite le DG3 transmet la consigne au DG4.

7.5 Description des attaques implémentées

Actuellement la plateforme implante deux types d'attaques

— une attaque MitM avec un attaquant qui s'intercale entre deux unités génératrices (DGs) pour remplacer la valeur de la consigne par la valeur de la mesure. Dans cette attaque, les DG communiquent avec le protocole TCP et les messages ne sont pas chiffrés. La machine d'attaque est connectée sur le même réseau que celui des DGs. L'outil d'attaque développé utilise la bibliothèque *Scapy* pour capturer les paquets et les injecter. Dans une première phase, l'outil applique de l'empoisonnement ARP pour que la source et la destination envoient leurs paquets à la machine d'attaque. Ensuite, les paquets sont capturés et modifiés à la volée pour échanger la valeur de la consigne avec celle de la mesure.

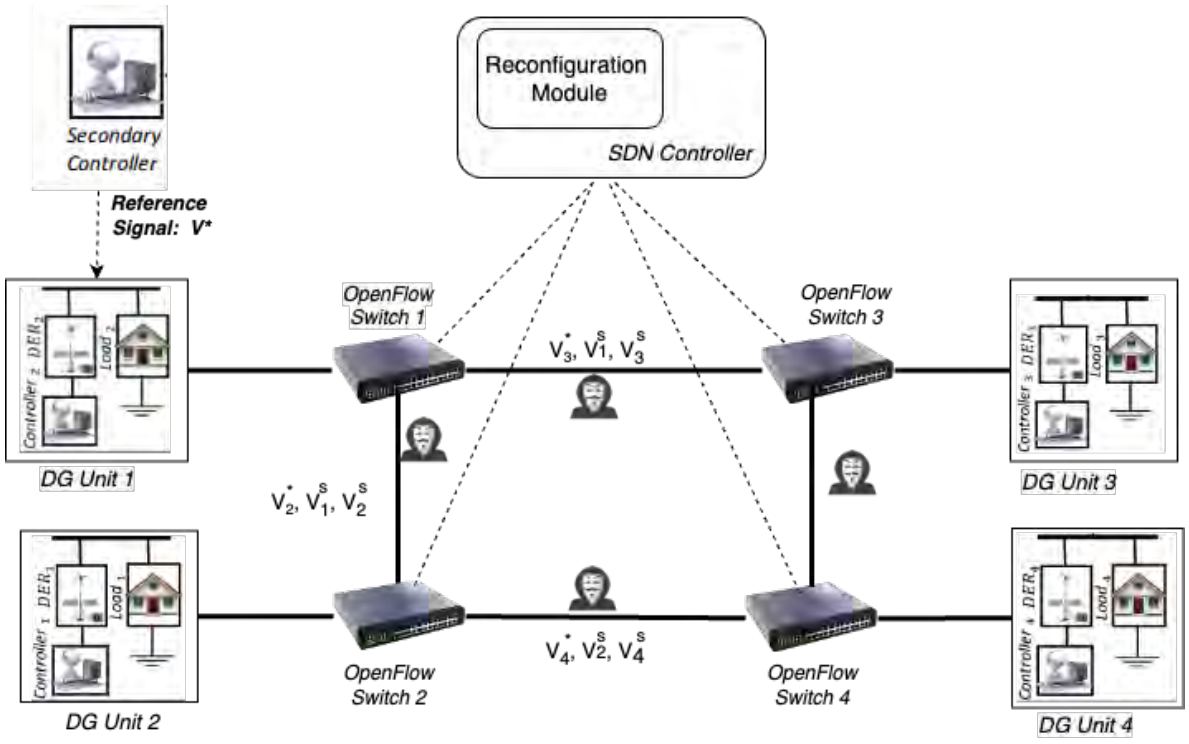

FIGURE 12 – Switches OpenFlow et contrôleur SDN du micro-réseau électrique.

— une attaque d'injection des délais pour perturber la synchronisation entre les DGs. Dans cette attaque, on utilise l'outil *saboteur* pour injecter des délais lors de l'échange des informations de synchronisation par un DG. L'outil s'exécute sur un DG pour retarder les paquets de synchronisation selon une distribution gaussienne avec une moyenne de 2s et une variance de 1500ms.

7.6 Liste de publications commentée

[1] Mingxiao Ma. *Attack Modelling and Detection in Distributed and Cooperative Controlled Microgrid Systems*. Theses, Université de Lorraine, April 2021. Cette thèse se base sur la platerforme de test de micro-réseaux électriques afin de démontrer et valider la mise en pratique d'attaques sur ce type d'infrastructures ainsi que des mécanismes de détection en utilisant des algorithmes d'apprentissage automatique.

[2] Mingxiao Ma, Abdelkader Lahmadi, and Isabelle Chrisment. Demonstration of Synchronization Attacks on Distributed and Cooperative Control in Microgrids. In *IM 2019 - The 16th IFIP/IEEE Symposium on Integrated Network and Service Management*, Washington DC, United States, April 2019. La plateforme de test de micro-réseaux électriques est composée de Raspberry Pi et Arduino pour contrôler des moteurs générateurs et vérifier la puissance délivrée par d'autres en plus d'ampoules pour une visualisation rapide. Cette plateforme a permis de tester en pratique une attaque où des valeurs de mesure erronées sont injectées dans un contrôleur afin de perturber l'ensemble du système de génération synchronisé. En effet, cette perturbation se diffuse aux autres contrôleurs sains.

8 Centre Inria de l'Université de Lorraine - Loria – Réseaux programmables

8.1 Tableau de synthèse

Partenaire	INRIA
Point de contact	Matthews José matthews.jose@inria.fr, responsable technique Jérôme François jerome.francois@inria.fr, responsable scientifique
Nom/titre	Réseaux programmables
Description succincte	PF permettant d'expérimenter des réseaux programmables sofwtare et hardware (switch P4, smartNICs)
Format des données	Interface de configuration
Activité normale	Aucune (l'utilisateur spécifie ses propres scénarios)
Activité malveillante	Aucune (l'utilisateur spécifie ses propres scénarios)
Accès	Accès partiel en ligne + local (certaines manipulations peuvent demander un recablage physique)

8.2 Description libre

La plateforme est conçue pour expérimenter en priorité des réseaux programmables de type P4. P4 est à la fois un langage et une architecture permettant de programmer le plan de données d'un réseau. La PF comporte différentes types d'équipements et en particulier des switch compatibles P4 de type Tofino ainsi que des cartes réseaux programmables ou SmartNICs également compatibles avec P4. La PF est complétée avec plusieurs serveurs traditionnels permettant l'hébergement de VM. Ainsi, un programme P4 peut être déployé de façon distribué sur différentes type de hardware et software (dans des VMs). Cette configuration en font sa spécificité. De plus, les capacités de la PF intègrent également la possibilité d'expérimenter des réseaux programmables de type OpenFlow de façon software (via les VM) et/ou hardware grâce à des switchs compatibles OpenFlow. La PF permet donc d'expérimenter des réseaux SDNs. Son avantage réside dans la présence de switchs hardwares dont les performances outrepassent les versions softwares utilisées dans le monde académique (par exemple avec bmv2 et mininet). De plus grâce aux multiples switches, des programmes distribués peuvent être testés en créant une infrastructure d'un petit réseau (comme décrit sur la figure 13) sur lesquels des hôtes peuvent être instanciées sous forme de VMs et contenir différents services que ce soit purement pour du réseau (par exemple un contrôleur SDN, un générateur de trafic) ou pour générer une charge applicative. La PF permet donc de vérifier de façon fonctionnelle une solution basée sur les réseaux programmables mais aussi d'en tester ses performances de façon réaliste. Dans le cas de Superviz, la PF peut être utilisée pour déployer des algorithmes de détection ou réaction qualifié de « in-network » en étant embarqué sur les switches mais les possibles domaines d'applications vont bien au-delà (test des nouveaux algorithmes pour le QoS, le routage, etc.).

8.3 Description technique

La PF est configurée avec différents réseaux comme ci-dessous :

— Blue network : The blue network a dedicated networks used for VM management, network storage, cluster sync and network provision and management. It has a band-with configuration :

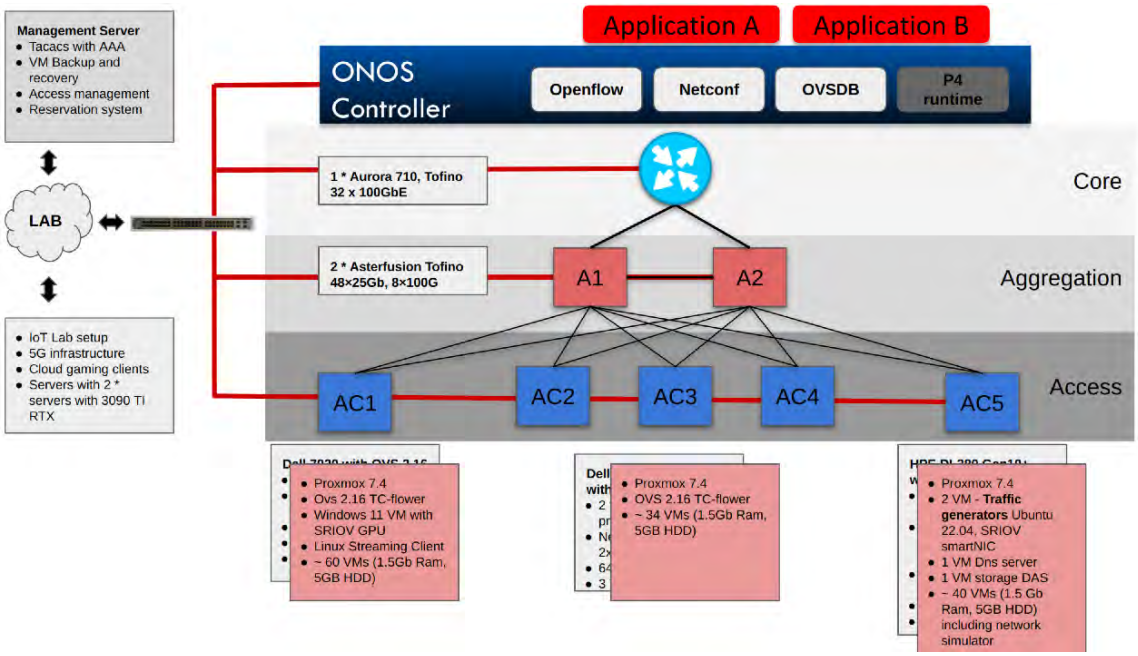

FIGURE 13 – PF réseaux programmables

- 16 x 10G MikroTik CRS317-1G-16S+RM running routerOS
- 4 x 1G D-Link DES-1024D switch
- A dedicated 10g 10Gtek Network Card for each of the 8 servers connected to the MikroTik Router
- A dedicated 1g backup Network Card for each of the 8 servers connected to the D-link switch. This link is cofigured with as a bonded interface with the 10G interfaces mentioned before. They have LACP running on it with active-backup mode and act as a backup interface.
- The server Nantes has DHCP, DNS, the PF wiki and OpenLdap, Nat VM ,the PBS backup server and the master ONOS SDN controller running on it.
- A Ceph cluster between the server nodes Lyon, Marseilles and Toulouse
- All the services on this network except the PBS server has HA backup configured between Nantes and Lyon server nodes

— Black network : This network is completely intended for research and is isolated on a hardware level from the rest of the equipment. The VMs connected to this network as assigned a specific VLAN provided during creation of the PF. The Black network consists of the following equipment :

- 2 x Mellanox ConnectX-5 Dual-Port 100GbE / Mellanox ConnectX-5 Dual-Port 25GbE as a part of the montpellier server node for primarily traffic generation
- 2 x Netronomoe agilio 40g / 2 x Netronomoe agilio 2 x 40g on the server nodes Lyon, Marseilles, Paris and Toulose. These are primarily used various research setups. The cards support P4, eBFP and DPDK.
- Intel Ethernet Controller 10-Gigabit X540-AT2 These are primarily used various research setups. The cards support P4, eBFP and DPDK.
- 3 x Tofino Programmable switches

- Each of the 8 servers can be connected to the black network using a network card that is of atleast 10Gbps bandwidth(details are in the appendix).
- Red network : The primary function of the red network is to make the PF accessible via the local research network. The Red network consists of the following equipment :
  - a dedicated 1g backup Network Card for each of the 8 servers connected to the D-link switch.
  - access to the PF GUI, that enables VM management via the GUI.
  - a shadow process used to recovery in case the Blue network malfunctions.
  - a DMZ VM that is used to bridge the Blue and Red network as needed
  - a specific VLAN dmz-MADYNES configured. We have 29 available public IP addresses (DNS names can be configured upon request) that can be assigned to VMs on the Bordeaux and Toulose server nodes with the Vlan tag 46. External users will need to pass through the bastion loria.loria.fr for SSH to this DMZ.

8.3.1 Environnement matériel

- **Bordeaux (Server)**
  - **Purpose :** VM hosting
  - **Hardware :**
    - CPU : Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz
    - RAM : 256GB DDR4 2400 MHz
    - Storage : Ceph Pools (unrestricted)
  - **Software :**
    - common server software*
  - **Network Cards :** 4 x NetXtreme BCM5720 Gigabit Ethernet PCIe x 1Gb, 2 x Netronome Systems Agilio x 40Gbps.
- **Lyon (Server)**
  - **Purpose :** File Storage and Proxmox VM
  - **Hardware :**
    - CPU(s) : 24 x Intel(R) Xeon(R) CPU E5-2420 v2 @ 2.20GHz (2 Sockets)
    - RAM : 64GB DDR4 3200 MHz
    - Storage : Ceph Pools (unrestricted)
  - **Software :**
    - **ceph :** 17.2.6-pve1+3
    - **ceph-fuse :** 17.2.6-pve1+3
    - **corosync :** 3.1.7-pve3
    - common server software*
  - **Network Cards :** 2x NetXtreme BCM5720 Gigabit Ethernet PCIe, 2 x Netronome Systems Agilio x 40Gbps
- **Marseille (Server)**
  - **Purpose :** File Storage and Proxmox VM
  - **Hardware :**
    - CPU : 32 x Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz (2 Sockets)
    - RAM : 128GB DDR4 2666 MHz
    - Storage : Ceph Pools (unrestricted)
  - **Software :**
    - **ceph :** 17.2.6-pve1+3
    - **ceph-fuse :** 17.2.6-pve1+3
    - **corosync :** 3.1.7-pve3

  - common server software*
  - **Network Cards :** 4 x NetXtreme BCM5720 Gigabit Ethernet PCIe x 1Gb, 4 x Ethernet Controller 10-Gigabit X540-AT2
- **Montpellier (Server)**
  - **Purpose :** Traffic Generator and Proxmox VM
  - **Hardware :**
    - CPU : 64 x Intel(R) Xeon(R) Silver 4314 CPU @ 2.40GHz (2 Sockets)
    - RAM : 128GB 2666 MHz
    - Storage : Ceph Pools (unrestricted)
    - Local Storage : Ceph Pools (unrestricted)
  - **Software :**
    - **Open vSwitch (OVS) :** 3.2.90
    - **ONOS Controller :** 2.7
    - **trex-traffic-generator :** 14.4
    - **DPDK :** 20.11.9
    - common server software*
  - **Network Cards :** 4 x Mellanox ConnectX-5 100Gbps, 4 x Mellanox ConnectX-5 25Gbps
- **Nantes (Server)**
  - **Purpose :** Network Management and Proxmox VM
  - **Hardware :**
    - CPU : 12 x Intel(R) Xeon(R) CPU E5-2420 v2 @ 2.20GHz (1 Socket)
    - RAM : 32GB DDR4 2666 MHz
    - Storage : Ceph Pools (unrestricted)
  - **Software :**
    - **Open vSwitch (OVS) :** 3.2.90
    - **ONOS Controller :** 2.7
    - **DPDK :** 20.11.9
    - **DNS-DHCP :** 14.3
    - **DOKUWIKI :** Hogfather
    - **Proxmox Backup Server :** 2.4
    - common server software*
  - **Network Cards :** 1 x 82599 10 Gigabit Network Connection 10Gbps
- **Paris (Server)**
  - **Purpose :** Proxmox VM
  - **Hardware :**
    - CPU : 32 x Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz (2 Sockets)
    - RAM : 64GB DDR4 2666 MHz
    - Storage : Ceph Pools (unrestricted)
    - Local Storage : 2 Tb HDD
    - GPU : Nvidia 3090 RTX
  - **Software :**
    - **Open vSwitch (OVS) :** 3.2.90
    - **ONOS Controller :** 2.7
    - **trex-traffic-generator :** 14.4
    - **DPDK :** 20.11.9
    - common server software*
  - **Network Cards :** 1 x 82599 10 Gigabit Network Connection 10Gbps, 2 x Netronome Systems Agilio x 40Gbps

- **Toulouse (Server)**
  - **Purpose :** File Storage and Proxmox VM
  - **Hardware :**
    - CPU : 12 x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (1 Socket)
    - RAM : 128GB 2666 MHz
    - Storage : Ceph Pools (unrestricted)
  - **Software :**
    - **ceph :** 17.2.6-pve1+3
    - **ceph-fuse :** 17.2.6-pve1+3
    - **corosync :** 3.1.7-pve3
    - common server software*
  - **Network Cards :** 1 x 82599 10 Gigabit Network Connection 10Gbps, 1 x Netronome Systems Agilio x 40Gbps
- **Asterfusion - 1/ Asterfusion - 2 (Hardware switches)**
  - **Advancing P4 Programmable switch**
  - **Capacity :** 3.3Tbps
  - **Hardware :**
    - **CPU :** 12 x Intel(R) Xeon(R) CPU
    - **RAM :** 32Gb DDR4
    - **Storage :** 1xM.2 NVME SSD 1 TB
    - **Forwarding Plane :** Programmable Barefoot Tofino ASIC-based
  - **Extra Features :**
    - **L4-L7 in-depth data processing capability**
    - **SDK :** Barefoot 9.0 or 11.1
  - **Ports :**
    - **48 x 25Gb SFP28**
    - **8 x 100Gb QSFP28**
  - **Power Supply :**
    - Dual-redundant, load-sharing, hot-swappable PSUs
  - **Cooling :**
    - 4+2 redundant, hot-swappable fan modules
- **Netberg 710** (Hardware Switch)
  - **P4 Programmable switch**
  - **Capacity :** 3.2Tbps
  - **Hardware :**
    - **CPU :** Intel Xeon D-1527 CPU
    - **RAM :** 32Gb DDR4
    - **Storage :** 1xM.2 NVME SSD 1 TB
    - **Forwarding Plane :** Programmable Barefoot Tofino ASIC-based
  - **Extra Features :**
    - **L4-L7 in-depth data processing capability**
    - **OS :** Ubuntu 20.04
    - **SDK :** Barefoot 9.0 or 11.1
  - **Ports :**
    - **32 x 100G Ports**
- **4 x Netronomoe agilio 40g** (SmartNIC)
  - **Processor :** Netronome NFP-4000
  - **Cores :** 40

- **Memory :** 8GB DDR3
- **Connectivity :**
  - **QSFP28 connectors :** 1/2 ports
- **Interfaces :**
  - **2 x 10/25/40/50/100GbE**
  - **PCIe :** Gen3 x16
  - **VAB :** Virtual Acceleration Bridge
  - **Offload :** Hardware-based virtual switch acceleration
- **Offload Capabilities :**
  - **OVS Offload :** Open vSwitch (OVS)
  - **P4 Offload :** P4 based on NTF lib
  - **IPsec Offload**
  - **SR-IOV**
  - **DPI Offload :** Cavium TurboDPI Offload
- **Security Features :**
  - **IPsec**
  - **SSL/TLS**
  - **Hardware-based firewall**
- **Acceleration Features :**
  - **OVS Offload :** Open vSwitch (OVS)
  - **GRE Offload :** Generic Routing Encapsulation (GRE)
  - **VXLAN Offload :** Virtual Extensible LAN (VXLAN)
  - **Stateless Offloads :** Stateless offloads for various protocols

- **2 x Mellanox ConnectX-5 Dual-Port 100GbE / Mellanox ConnectX-5 Dual-Port 25GbE** (SmartNIC)
  - **Adapter Model :** Mellanox ConnectX-5
  - **Ports : Dual-port 100GbE / Dual-port 25GbE**
  - **Data Rate : 100 Gbps per port**
  - **Form Factor :** PCIe 3.0 x16
  - **Connectivity :**
    - **SFP+/QSFP28 connectors :** 2 ports
  - **Virtualization :**
    - **SR-IOV :** Single Root I/O Virtualization (SR-IOV)
    - **NetQueue :** VMware NetQueue and Microsoft Hyper-V VMQ
  - **RoHS Compliant : Yes**
  - **Offload Capabilities :**
    - **RoCE :** RDMA over Converged Ethernet (RoCE)
    - **Stateless Offload :** TCP/IP and UDP/IP stateless offload
    - **Interrupt Coalescence :** Intelligent interrupt coalescence
    - **LRO :** Large receive offload (LRO) and GRO
  - **Security Features :**
    - **Inline Cryptography :** IPsec and TLS inline cryptography
    - **Certificate Support :** Hardware-based X.509 certificate support
  - **Management and Software Support :**
    - **Management Software :** Mellanox NEO management software
    - **Firmware Tools :** Mellanox Firmware Tools (MFT)
    - **OFED :** Mellanox OpenFabrics Enterprise Distribution (OFED)
    - **Drivers :** RoCE and VPI drivers

- **2 x Intel Ethernet Controller 10-Gigabit X540-AT2** (SmartNIC)
  - **Controller Model :** Intel X540-AT2
  - **Ports : Dual-port 10-Gigabit Ethernet**
  - **Data Rate : 10 Gbps per port**
  - **Form Factor :** PCIe 2.1 x8
  - **Connectivity :**
    - **RJ45 connectors :** 2 ports
  - **Virtualization :**
    - **VT-c :** Intel Virtualization Technology for Connectivity (VT-c)
    - **VMDq :** Virtual Machine Device Queues (VMDq)
  - **Offload Capabilities :**
    - **Checksum Offloading :** TCP, UDP, and IP checksum offloading
    - **TSO :** TCP segmentation offload (TSO)
    - **LRO :** Large receive offload (LRO)
    - **DCA :** Direct Cache Access (DCA)
  - **Power Management :**
    - **EEE :** Energy-efficient Ethernet (EEE)
  - **Security Features :**
    - **VT-d :** Intel Data Direct I/O Technology (VT-d)
    - **TXT :** Intel Trusted Execution Technology (TXT)
  - **Management and Software Support :**
    - **PROSet Utility :** Intel PROSet Utility
    - **ANS :** Advanced Network Services (ANS)
    - **iWARP/RDMA :** Intel iWARP/RDMA
    - **BootUtil :** Intel Ethernet Flash Firmware Utility (BootUtil)
- **8 x 10Gtek 10GbE PCIe Network Card for Intel X540-T2** (SmartNIC)
  - **Controller Model :** Intel X540-T2
  - **Ports : Dual-port 10-Gigabit Ethernet**
  - **Data Rate : 10 Gbps per port**
  - **Form Factor :** PCIe 2.1 x8
  - **Connectivity : RJ45 connectors :** 2 ports
  - **Virtualization : VT-c, VMDq**
  - **Offload Capabilities : Checksum offloading, TSO, LRO, DCA**
  - **Security Features : VT-d, TXT**
  - **Management Support : PROSet Utility, ANS, iWARP/RDMA, BootUtil**
- **1 x MikroTik CRS317-1G-16S+RM** (Traditional Switch hardware)
  - **Model :** MikroTik CRS317-1G-16S+RM
  - **Ports : 16 SFP+ ports, 1 Gigabit Ethernet port**
  - **Data Rate : 10 Gbps per SFP+ port**
  - **Connectivity : SFP+ ports :** 16, **Gigabit Ethernet port :** 1
  - **Features : Layer 2 and Layer 3 switching, VLAN support, OVS support**
  - **Management : Web-based interface, CLI, SNMP**
- **2 x D-Link DES-1024D - Hardware Specifications** (Traditional Switch hardware)
  - **Model :** D-Link DES-1024D
  - **Ports :** 24 10/100 Mbps Ethernet ports
  - **Switching Capacity :** 4.8 Gbps
  - **Forwarding Rate :** 3.57 Mpps
  - **MAC Address Table :** 8K entries

— **Buffer Memory :** 2 MB per device

8.3.2 Environnement logiciel

All servers are configured with a unified list of sofwtare components :
— **proxmox-ve :** 8.0.2 (running kernel : 6.2.16-14-pve)
— **pve-manager :** 8.0.4 (running version : 8.0.4/d258a813cfa6b390)
— **pve-kernel-6.2 :** 8.0.5
— **proxmox-kernel-helper :** 8.0.3
— **proxmox-kernel-6.2.16-14-pve :** 6.2.16-14
— **pve-kernel-6.2.16-4-pve :** 6.2.16-5
— **ceph-fuse :** 16.2.11+ds-2
— **corosync :** 3.1.7-pve3
— **criu :** 3.17.1-2
— **glusterfs-client :** 10.3-5
— **ifupdown2 :** 3.2.0-1+pmx4
— **ksm-control-daemon :** 1.4-1
— **libjs-extjs :** 7.0.0-4
— **libknet1 :** 1.25-pve1
— **libproxmox-acme-perl :** 1.4.6
— **libproxmox-backup-qemu0 :** 1.4.0
— **libproxmox-rs-perl :** 0.3.1
— **libpve-access-control :** 8.0.5
— **libpve-apiclient-perl :** 3.3.1
— **libpve-common-perl :** 8.0.8
— **libpve-guest-common-perl :** 5.0.4
— **libpve-http-server-perl :** 5.0.4
— **libpve-rs-perl :** 0.8.5
— **libpve-storage-perl :** 8.0.2
— **libspice-server1 :** 0.15.1-1
— **lvm2 :** 2.03.16-2
— **lxc-pve :** 5.0.2-4
— **lxcfs :** 5.0.3-pve3
— **novnc-pve :** 1.4.0-2
— **proxmox-backup-client :** 3.0.2-1
— **proxmox-backup-file-restore :** 3.0.2-1
— **proxmox-kernel-helper :** 8.0.3
— **proxmox-mail-forward :** 0.2.0
— **proxmox-mini-journalreader :** 1.4.0
— **proxmox-widget-toolkit :** 4.0.6
— **pve-cluster :** 8.0.3
— **pve-container :** 5.0.4
— **pve-docs :** 8.0.4
— **pve-edk2-firmware :** 3.20230228-4
— **pve-firewall :** 5.0.3
— **pve-firmware :** 3.8-2
— **pve-ha-manager :** 4.0.2
— **pve-i18n :** 3.0.7

— **pve-qemu-kvm :** 8.0.2-6
— **pve-xtermjs :** 4.16.0-3
— **qemu-server :** 8.0.7
— **smartmontools :** 7.3-pve1
— **spiceterm :** 3.3.0
— **swtpm :** 0.8.0+pve1
— **vncterm :** 1.8.0
— **zfsutils-linux :** 2.1.12-pve1

In addition, some servers have been extended with the following components :

— **Lyon**
  — **ceph :** 17.2.6-pve1+3
  — **ceph-fuse :** 17.2.6-pve1+3
  — **corosync :** 3.1.7-pve3
  — common server software*
— **Marseille**
  — **ceph :** 17.2.6-pve1+3
  — **ceph-fuse :** 17.2.6-pve1+3
  — **corosync :** 3.1.7-pve3
— **Montpellier**
  — **Open vSwitch (OVS) :** 3.2.90
  — **ONOS Controller :** 2.7
  — **trex-traffic-generator :** 14.4
  — **DPDK :** 20.11.9
— **Nantes**
  — **Open vSwitch (OVS) :** 3.2.90
  — **ONOS Controller :** 2.7
  — **DPDK :** 20.11.9
  — **DNS-DHCP :** 14.3
  — **DOKUWIKI :** Hogfather
  — **Proxmox Backup Server :** 2.4
— **Paris**
  — **Open vSwitch (OVS) :** 3.2.90
  — **ONOS Controller :** 2.7
  — **trex-traffic-generator :** 14.4
  — **DPDK :** 20.11.9
— **Toulouse**
  — **ceph :** 17.2.6-pve1+3
  — **ceph-fuse :** 17.2.6-pve1+3
  — **corosync :** 3.1.7-pve3

8.3.3 Moyens de supervision et de développement

The configurability of a cluster with P4 Tofino switches and optional components like GPU and SmartNICs is highly flexible and can be tailored to meet specific use-cases. Below is an overview of key configurability aspects :

— **Proxmox Cluster Configuration** :
  — We inherit the configurability of a Proxmox cluster. It allows for fine-grained configuration of virtualization and container resources, including CPU, memory, storage, and network

allocation. Proxmox also provides HA clustering for fault tolerance, ensuring uninterrupted service availability by automatically migrating virtual machines in the event of node failures. Additionally, it provides granular user and rights management, allowing administrators to define distinct access levels and permissions for various users, enhancing security and access control. Also, access to a VM backup server and VM repository.

- **Integration with Proxmox** :
  - P4 Tofino switches can be integrated with the Proxmox cluster incase of traffic management cases, we have default P4 programs for that including the SDN controller cofiguration.
- **Optional Components Configuration** :
  - **GPU** :
    - Configure GPU passthrough to virtual machines for GPU-intensive workloads like machine learning and rendering.
  - **SmartNICs** :
    - Configure SmartNICs to offload network processing tasks and support features like SR-IOV for virtual machine acceleration.
- **Storage Configuration** :
  - Configure various storage options, including local storage, and CEPH with the ability to define storage pools and volumes.
- **Custom Scripts and Automation** :
  - Leverage Proxmox's API and CLI for custom scripts and automation, allowing advanced users to customize and automate various aspects of the platform.

The configurable of this setup offers a high degree of flexibility, making it suitable for a wide range of requirements.

The platform can be configured and monitored using the following tools :

- By default : The Platform allows admin users to configure the resources needed, deploy virtual machines, and monitor the resources they use (CPU, memory, GPU, network).
- To control and monitor programmable network elements (virtual and hardware switches) : ONOS controller. Due to hardware resources, this must be done by the platform admin or on request (no direct access for users by default).
- Optionally (user installation) : more specific tools for obtaining network statistics (such as Wireshark) on user VMs.
- Control of the programmable network with a user-installed SDN controller on a virtual machine.
- Ceph cluster (integrated into the Proxmox VE interface).

8.3.4 Contraintes d'usage

La platforme fournit une flexibilité d'utilisation mais requière une coordination nécessaire avec l'administrateur de la plateforme pour la bonne réalisation des expériences. Plusieurs types de ressources doivent être utilisées en pure isolation par design ou pour éviter un biais dans les performances obtenues. C'est le cas des ressources GPUs et des équipements réseaux programmables hardware (SmartNIC, switch). Dans ces cas là, l'administrateur de la plateforme gérera les accès à ces ressources et associera les droits équivalents dans l'interface de Proxmox. A ce stade, le nombre d'utilisateurs étant restraint, cette gestion peut se faire de façon ad-hoc. Dans le cas où la plateforme serait amener à évoluer vers un nombre plus grands d'utilisateurs, d'autres outils permettant l gestion automatique des demandes et leur réservation pourraient être développés. Il est à noter que néanmoins, le recâblage de certains réseaux nécessiteront toujours l'intervention et donc la coordination avec l'administrateur de la plateforme.

La plateforme est donc accessible à distance mais son utilisation demande une coordination avec

l'administrateur de la plateforme pour le bon partage équilibré des ressources entre utilisateurs. En cas d'abus, ce dernier pourra être amené à supprimer certaines ressources (après avertissement), par exemple des VMs online pendant des temps trop longs. Un formulaire standardisé de demande d'expérimentation est en cours de préparation. Il sera notamment explicitement demandé aux utilisateurs de borner leur expérience dans le temps.

8.4 Description des cas d'usage normaux

La plateforme permet la réalisation de scénarios divers. L'utilisateur définit via ses machines virtuelles les services et programmes qu'il souhaite. Cependant, afin de faciliter certains expérimentations, un serveur est fourni avec une VM intégrant un générateur de trafic TRex. Cet outil permet de générer différents types de traffic (par exemple HTTPS) mais doit être configuré par l'utilisateur lui-même.

8.5 Description des attaques implémentées

De la même façon, la plateforme n'implémente pas d'attaque par défaut. L'utilisateur est libre d'utiliser les ressources à sa disposition. Par exemple, il peut créer des VMs avec des outils d'attaques. Il est à noter que le générateur de trafic TRex peut servir notamment à faire des tests de performance en générant des trafic à fort débit et peut donc être par exemple utilisé pour instancier une attaque de type déni-de-service.

9 CNRS LAAS MIRAGE

9.1 Tableau de synthèse

Partenaire	LAAS-CNRS
Point de contact	Florent Galtier florent.galtier@laas.fr
Nom/Titre	LAAS-MIRAGE
Description succinte	Plateforme détection intrusion IoT
Format des données	Logs Mirage au format texte, signaux au format CF32
Activité normale	Communications entre objets connectés avec différents protocoles (BLE, IEEE 802.15.4, WiFi...)
Activité malveillante	Attaques réseau exécutées par Mirage (MitM, jamming, injection de trames) selon le protocole
Accès	En ligne (spécification des attaques à mener et des objets qui doivent communiquer en JSON)

9.2 Description libre

Mirage est un framework développé en Python et destiné à l'audit des technologies sans fil fréquemment utilisées par les objets connectés. Il supporte plusieurs protocoles sans fil (Bluetooth Low Energy, Enhanced ShockBurst, WiFi, Zigbee, ...) des modules d'analyse et d'attaque et des nombreuses interfaces matérielles (HCI, BTLEJack, Nordic, sniffeurs ButteRFly et Ubertooth). Cette plateforme comprend divers objets connectés et matériels utilisant ces protocoles, contrôlables à l'aide de Mirage pour faciliter l'utilisation d'attaques, ainsi que des sondes radio. Elle permet ainsi de tester des approches de détection dans différentes configurations en contrôlant l'environnement et les attaques qui y sont jouées, en remontant des données depuis les objets, ainsi que des données radio brutes depuis les sondes radio. Une machine est également dédiée pour exécuter des approches de détection centralisées. Il est ainsi possible à un utilisateur de fournir une liste de commandes Mirage à exécuter, à quel moment, pendant combien de temps et sur quel matériel, ainsi que de déployer une sonde sur la machine dédiée, pour ensuite récupérer les logs de Mirage, les logs de son outil, et une capture de l'environnement radio durant l'expérience. La plateforme suit la structure indiquée dans la Figure 14.

9.3 Description technique

9.3.1 Environnement matériel

La plateforme comporte deux raspberry Pi 4, vingt raspberry Pi 3 (plus une pour la gestion d'un réseau WiFi interne), deux prises connectées BLE, une prise connectée WiFi, un thermostat et un contrôle de chauffage en 6LoWPAN, et un ensemble de gateway, ampoule et télécommande Phillips Hue. La machine contrôlant la solution de détection d'intrusion centralisée est reliée à un USRP N210. Les Raspberry Pi 4 sont reliées à des nRF52840, ainsi qu'à des LimeSDR Mini.

9.3.2 Environnement logiciel

Les deux Raspberry Pi 4 et vingt Raspberry Pi 3 embarquent le framework Mirage afin de mener les attaques sur l'environnement. La dernière Raspberry Pi 3 fait office de passerelle WiFi pour le réseau

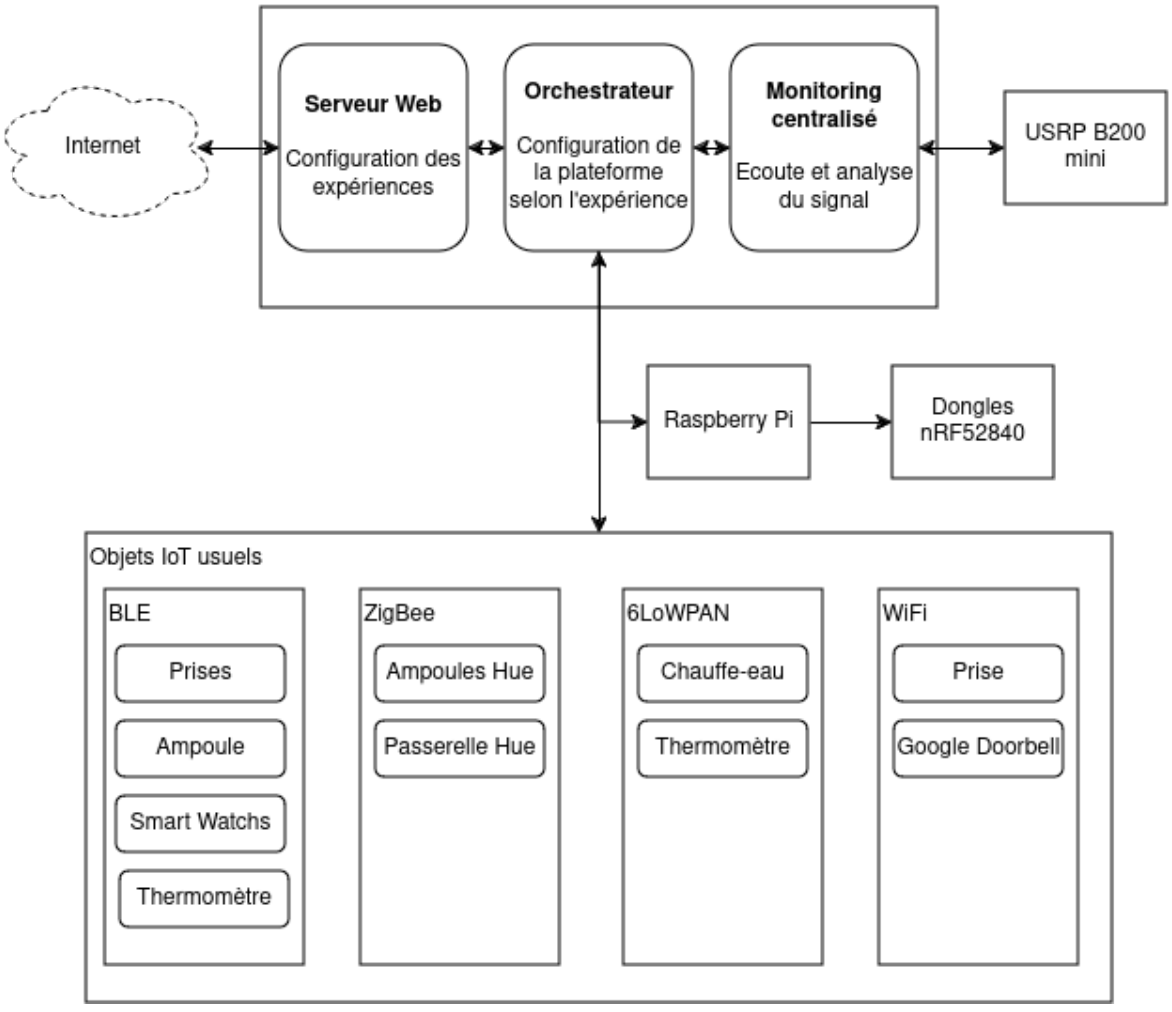

FIGURE 14 – Architecture globale de la plateforme LAAS-MIRAGE

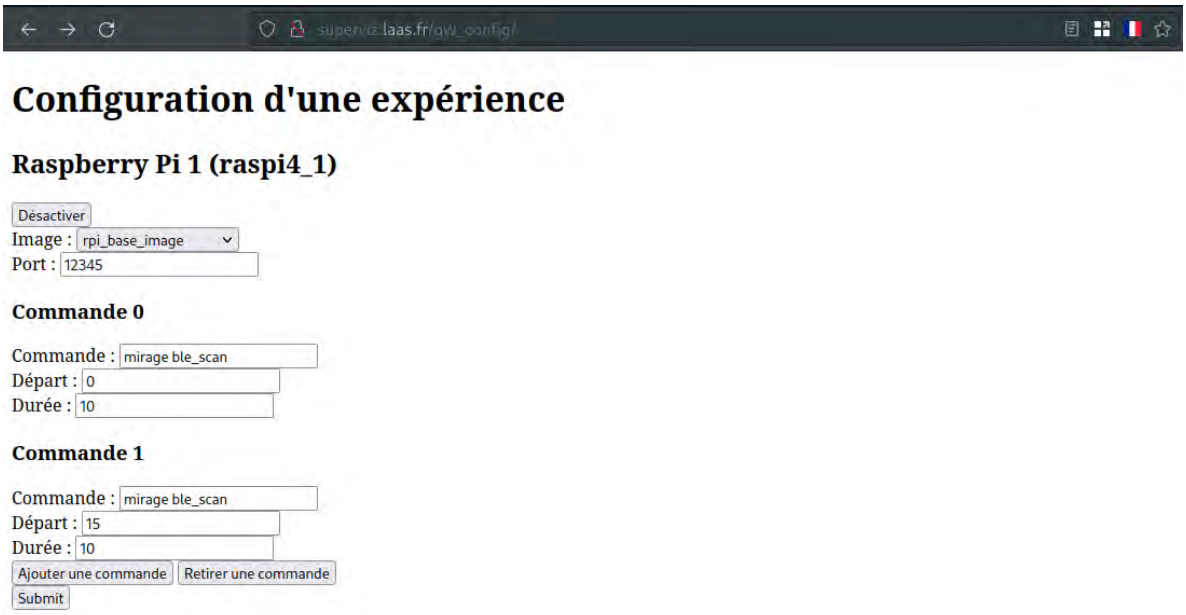

FIGURE 15 – Interface de contrôle de la plateforme

interne de la plateforme. Les autres objets n'ont pas été modifiés, mais seront à terme contrôlables via un relais afin de pouvoir les allumer ou éteindre durant les campagnes de tests.

9.3.3 Moyens de supervision et de développement

La supervision des machines embarquant Mirage, ainsi que la machine contrôlant la solution de détection d'intrusion centralisée, se fait via une interface web (représentée sur la capture d'écran en Figure 15). Celle-ci contient une liste actualisée en temps réel des machines reliées à la plateforme, avec la possibilité de les allumer ou éteindre pour la durée de l'expérience à mener. La solution de détection d'intrusion centralisée doit pour le moment être déployée manuellement au niveau de la plateforme. Les machines embarquant Mirage peuvent être contrôlées en fournissant une liste de commandes à exécuter avec l'instant de lancement de la commande (par rapport au début de l'expérience) ainsi que la durée au bout de laquelle celle-ci doit être interrompue le cas échéant.

La structure modulaire de Mirage, ainsi que l'abstraction du matériel pour les différents protocoles supportés, permet d'ajouter des modules personnalisés pour rajouter des fonctionalités ou des attaques à la plateforme. Mirage supporte également la modification ponctuelle du comportement de certains modules à l'aide de "scenarios", dans lesquels l'utilisateur peut définir des callbacks alternatifs lors de la réception de certaines communications.

9.3.4 Contraintes d'usage

Autorisation d'accès à la ZRR nécessaire pour un accès direct à la plateforme, hébergée au sein du LAAS (à confirmer).

9.4 Description des cas d'usage normaux

L'utilisateur spécifie une série d'exécutions de modules mirages, avec instant de démarrage, durée, et machine exécutant la commande. Ces modulent couvrent différentes actions, légitimes ou non, associées aux différents protocoles supportés par mirage :

Protocole	Fonctions supportées
Bluetooth Low Energy	émission et réception d'advertisements (beacons BLE), connexions entrantes et sortantes, Man-in-the-Middle (BTLEJuice, GATTacker), hijacking (InjectaBLE, BTLEJack), injection de trames dans une connexion en cours (InjectaBLE)
ZigBee	émission et réception de paquets sur un canal, attaque de désauthentification, flood de demandes d'associations
WiFi	scan, attaque de déseauthentification, création d'un point d'accès

Ces modules sont également chaînables entre eux, ou personnalisables via les "scenarios" Mirage (voir 9.3.3). Ainsi, il est possible de jouer des scénarios où des objets se connectent entre eux et communiquent, ou d'intégrer des attaquants dans l'environnement menant différentes attaques sur d'autres objets jouant le rôle d'acteurs légitimes.

9.5 Description des attaques implémentées

Les attaques sont menées sur la plateforme conformément à la configuration demandée par l'utilisateur (types d'attaques à mener, depuis quelle machine, quand) et les logs sont remontés dans une archive accessible à l'utilisateur après la fin de l'expérience.

Les attaques supportées à l'heure actuelle sont le Man-in-the-Middle en BLE, l'injection de trames en ZigBee ou BLE (y compris en cours de connexion), des attaques de hijacking en BLE, des attaques de désauthentification en ZigBee et WiFi, et du flood de demandes d'association ZigBee.

9.6 Liste de publications commentée

[1] Romain Cayre, Florent Galtier, Guillaume Auriol, Vincent Nicomette, Mohamed Kaâniche, and Géraldine Marconato. Injectable : Injecting malicious traffic into established bluetooth low energy connections. In *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 388–399. IEEE, 2021.

[2] Romain Cayre, Florent Galtier, Guillaume Auriol, Vincent Nicomette, Mohamed Kaâniche, and Géraldine Marconato. Injectable : injection de trafic malveillant dans une connexion bluetooth low energy. In *Symposium sur la sécurité des technologies de l'information et des communications (SSTIC 2021)*, 2021. InjectaBLE est une attaque en BLE développée au LAAS, permettant d'injecter à la volée des trames dans des communications BLE établies. Elle est intégrée à Mirage.

[3] Romain Cayre, Vincent Nicomette, Guillaume Auriol, Eric Alata, Mohamed Kaaniche, and Geraldine Marconato. Mirage : towards a metasploit-like framework for iot. In *2019 IEEE 30th International Symposium on Software Reliability Engineering (ISSRE)*, pages 261–270. IEEE, 2019.

[4] Romain Cayre, Jonathan Roux, Eric Alata, Vincent Nicomette, and Guillaume Auriol. Mirage : un framework offensif pour l'audit du bluetooth low energy. In *Symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC 2019)*, pages 229–258, 2019. Mirage

est un framework permettant de contrôler des communications dans différents protocoles de l'IoT (BLE, ZigBee, WiFi...), ainsi que différentes attaques de l'état de l'art sur ces derniers. Il sert de base au contrôle de la plateforme.

10 Grenoble-INP – G-ICS

Partenaire	GINP
Point de contact	Stéphane Mocanu
Nom/Titre	G-ICS
Description succincte	Plateforme systèmes industriels
Format des données	Réseau (pcap)
Activité normale	Plusieurs types (protocoles) de trafic industriel selon maquette. L'activité normale correspond aux échanges de données entre les contrôleurs afin de piloter le processus industriel en régime nominal (conforme aux spécifications d'exploitation).
Activité malveillante	Attaques orientées processus exploitant les vulnérabilités des protocoles industriels et/ou équipements
Accès	Local, ou indirect via portail, données publiques

10.1 Description libre

GreEn-ER Industrial Control systems Sandbox (G-ICS) est une plateforme d'enseignement et de recherche qui réunit une centaine d'équipements de contrôle-commande et de supervision industriels multi-protocole et multi-constructeur qui peuvent être couplés de manière flexible avec un système de simulation matérielle (hardware-in-the-loop). La simulation logicielle des procédés peut être réalisée avec des simulateurs commerciaux (Matlab/Simulink, Dymola) ou libre (Scilab ou Modelica) ainsi qu'avec des environnements de virtualisation (Factory I/O ou Home I/O). On peut ainsi réaliser des architectures de système couvrant des domaines industriels allant de domotique et distribution électrique de bâtiment jusqu'à l'industrie manufacturière et smartgrids.

10.2 Description technique

10.2.1 Environnement matériel

La plateforme est constituée de plusieurs maquette distinctes. Les sections suivantes détaillent les principaux cas d'usage. Un plus des maquettes décrites une importante quantité de matériel d'automatisme est disponible pour la réalisation des expériences sur mesure.

Maquettes Robots 2D Trois maquettes pédagogiques Schneider MD1ADAX2M Machines 2 Axes comprenant deux axes industrielles, un automate M340, deux variateurs de vitesses et une IHM. Protocoles mis-en-oeuvre : CANOpen et Modbus/TCP

Maquettes FisherTechnik Processus physiques à échelle réduite : 6 valises Fischertechnik simulateur d'usine [13]. Capteurs/actionneurs interfaces avec des unités E/S déportées TM3BCEIP (Figure 17). Communication basée sur Modbus/TCP.

13. https://www.fischertechnik.de/en/products/simulating/training-models/554868-sim-training-factory-industry-4-0-24v

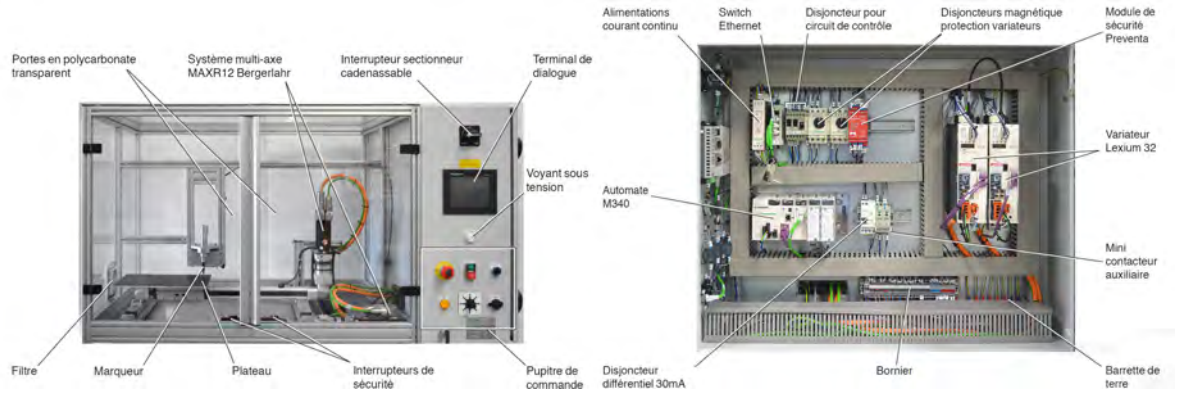

FIGURE 16 – Maquette Robots Schneider

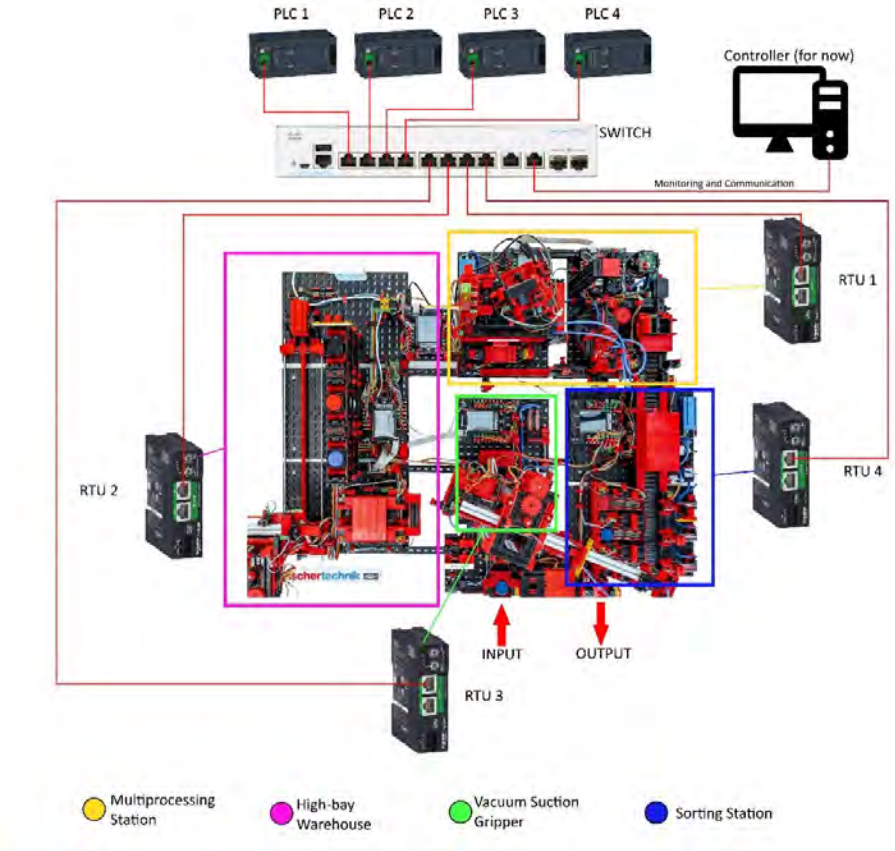

FIGURE 17 – Maquette Fischer Technik / Schneider

Maquettes Hardware-in-the-Loop Une cinquantaine d'automates programmables gammes Schneider, Siemens, Wago et ABB reliées à des interfaces électroniques permettant le couplage avec des simulateurs de processus. Licences simulateur Home I/O, Factory I/O disponibles ou interfaçage avec Matlab/Simulink, Modelica, etc .. Le principe est présenté dans la Figure 18

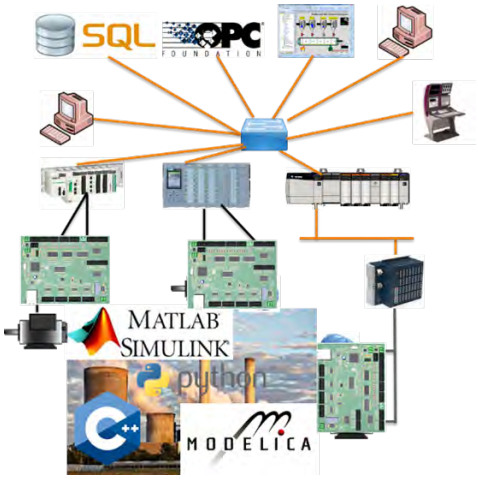

FIGURE 18 – Maquette Hardware-in-the-Loop

Maquettes multiprotocole Maquettes multi protocoles : un modèle de « valise SCADA » réalisation interne est disponible (10 exemplaires - Figure 19). La maquette permet d'étudier et réaliser des attaques sur des architectures hiérarchiques et distribuées multi protocole (Modbus TCP, CANOpen, OPC UA, Modbus RTU).

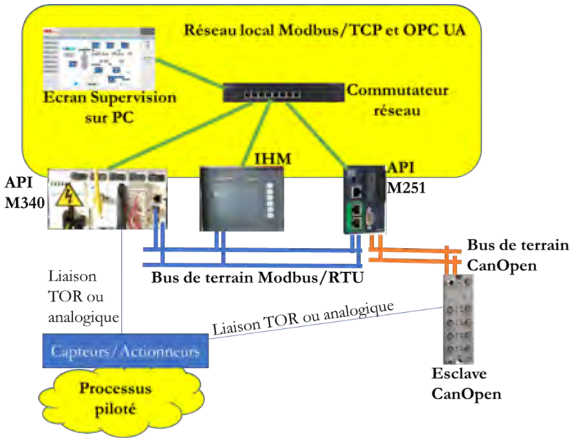

FIGURE 19 – Maquette Multiprotocole

Plateforme smart-grid IEC 61850 Environ 30 relais de protection et unités de mesure des courant et tension sont disponible pour la réalisation des maquettes des infrastructures de protection et control

des réseaux électriques basés sur les protocoles de communication IEC 61850 ainsi que les réseaux redondants HSR et PRP. Une des maquettes constituée de plusieurs unités de mesure autonomes (Stant Alone Measurement Unit -SAMU) et relais de protection (Intelligent Electronic Device - IED) est présentée dans la Figure 20. Le réseau redondant est accessible pour la capture des trames et le deployement des attaques via une Redondancy Box (RedBox).

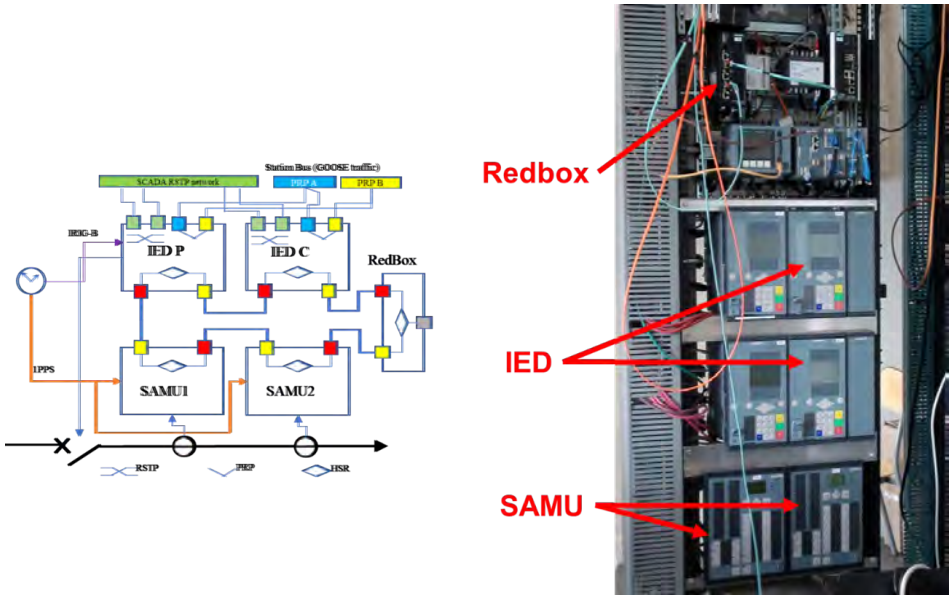

FIGURE 20 – Maquette Smart-Grid

Maquette automatisme de sécurité Trois maquettes complètes (capteurs, actionneurs et automates programmables) de la marque PILZ ainsi que plusieurs automates de sécurité Schneider et Siemens sont disponibles pour la réalisation des démonstrateurs d'attaques sur les fonctions de commande de sécurité (Figure 21).

FIGURE 21 – Maquette Automates de sécurité

10.2.2 Environnement logiciel

— environnements de programmation des composants de contrôle/commande (Schneider, Siemens, Pilz, ABB, Kepware)
— logiciels de supervision industrielle : PCVues, WinCC
— serveurs OPC Kepware et Matrikon

10.2.3 Moyens de supervision et de développement

Wireshark disponible sur tous les postes avec un dissecteur partiel UMAS local, accès en admin aux commutateurs et possibilité de configuration des ports supplémentaires en monitoring. Instances snort et zeek.

10.2.4 Contraintes d'usage

La plateforme est connectée avec les PC d'une salle d'enseignement de Grenoble-INP. Bien qu'il soit possible de déconnecter temporairement les PC, par sécurité, le déploiement des ransomware et virus auto-replicant ne sera pas possible. Des attaques DoS possibles sous certaines conditions : les ordinateurs de la salle étant connectés au réseaux des maquettes et au réseau de Grenoble-INP, afin d'éviter des perturbations sur le réseau d'établissement il est nécessaire, en préalable, déconnecter physiquement les ordinateurs de la salle. Des ordinateurs dédiés (et non-gérés par l'établissement) doivent être utiliser pour les attaques de type DoS afin d'éviter les remontées des alertes par les EDR de Grenoble-INP.

Afin de garantir la sécurité du matériel pas des attaques destructives (chargement des firmwares corrompus).

Pas de contraintes d'accès physique, la plateformes est hors ZRR.

10.3 Description des cas d'usage normaux

S'agissant des systèmes industriels l'activité normale correspond au fonctionnement normal du processus physique. La trafic correspond à la communication entre les contrôleurs industriels ou avec les capteurs/actionneurs ou encore avec la supervision industrielle.

10.4 Description des attaques implémentées

Les attaque implémentées sont des forçages des valeurs d'entrée (capteurs), de sortie (actionneurs) ou des variables internes des contrôleurs. Les protocoles réseaux supportés actuellement sont Modbus/TCP, UMAS (partiellement), CANOpen, GOOSE et SV (version 61850-9-2LE)

Attaques Modbus/TCP Ce type d'attaque se situes au niveau du réseau de communication entre la supervision industrielle et les automates programmables et utilise des écritures dans les variables internes des automates programmables via des clients Modbus/TCP (logiciels libres sur Internet ou Metasploit). Les attaques utilisent des commandes "légitimes" (par exemple l'ouverture d'une vanne ou l'arrêt d'un moteur) dans des contextes ou l'action peut endommager le processus physique. Des exemples concrets d'attaque sur Modbus/TCP sont détaillés en [6, 5, 4, 1]. Une parties des attaques ont été protées sur UMAS (requêtes Modbus propriétaires de Schneider).

Attaques CANOpen Ce type d'attaque vise directement le trafic entre les automates programmables et les contrôleurs des boucles locales. Il est implémenté actuellement uniquement sur la maquette "Robots 2D". L'attaque consiste dans l'injection de commandes sur le bus CAN qui vont, par exemple, mettre en défaut un variateurs de vitesse ou changer son mode de fonctionnement, modifier ou arrêter les déplacements en cours, effectuer des déplacement interdit ou avec des vitesses trop élevée, injecter de fausses valeurs des capteurs ou désynchroniser les mouvements des deux axes. En tout 17 types d'attaques sont implémentées et décrites en [1].

Attaques GOOSE Le protocoles GOOSE et un protocole multicast Ethernet utilisé pour la transmission des évènements dans un poste électrique IEC 61850. Essentiellement il s'agit de déclenchement des disjoncteurs (trip). Le trames GOOSE sont identifier à l'aide des deux compteurs (un pour les trames l'autre pour les changements d'état-évènements). L'attaque consiste a usurper la séquence légitime des trames GOOSE en injectant des trames qui provoquent un déclenchement du disjoncteur (une seule trame est suffisante). L'implémentation et la détection ont été présentés en [2].

attaque SMV Le protocole SMV est un multicast Ethernet utilisé pour la remontées des échantillons des mesures de courent et tension dans les postes IEC 61850. Les trames SMV sont identifiées par des compteurs. Deux types d'attaques sont disponibles : injection des fausses mesures et flood Ethernet. L'injection des fausses mesures consiste a usurper le flot des SMV légitime et, donc, injecter un flot avec de fausses mesures. Le flood Ethernet vise les réseaux haute disponibilité HSR et PRP. En particulier, les réseaux "double anneau" HSR son très vulnérables face aux floods Ethernet. Les attaques et les effets sur les protections électriques et les infrastructures réseaux ont été présentées en [8] et [9].

10.5 Liens avec les datasets

10.5.1 Datasets Modbus

Des datasets correspondant aux travaux de la thèse de Oualid Koucham [14] sont disponibles en format pcap. Les datasets et les attaques associées sont détaillés dans la section 3.3.3 (Implementation and datasets) de la thèse. Les datasets ont été générés sur une maquette Hardware-in-the-Loop également décrite dans la thèse avec des attaques Modbus/TCP. La maquette est construite sur le principe illustré en Figure 18 couplée à une simulation logicielle d'une version simplifiée d'un processus physique bien connu dans l'automatique : la colonne de distilation Tennessee-Eastman. Le schème du processus et l'architecture de communication industrielle utilisée sont présentés dans le Figure 22 Une démo réduite des attaques et de la détection est disponible en format machines virtuelles (rejeu des datasets, livrable du projet ANR ASTRID SACADE).

10.5.2 Datasets CANOpen

Des datasets des attaques ModbusTCP et CANOpen générés sur la maquette Robots 3D sont issus des travaux de thèse d'Estelle Hôtellier. Les datasets ainsi que la description détaillé des attaques seront rendus disponibles à partir du mois d'avril 2024.

10.5.3 Datasets IEC 61850

Un dataset correspondant à une attaque de type injection de faux signaux de trip dans un flot GOOSE est issu de la thèse de Maëlle Kebir-Querrec [15]).

14. https://theses.hal.science/tel-02108208v1/document
15. https://theses.hal.science/tel-01609230v2/

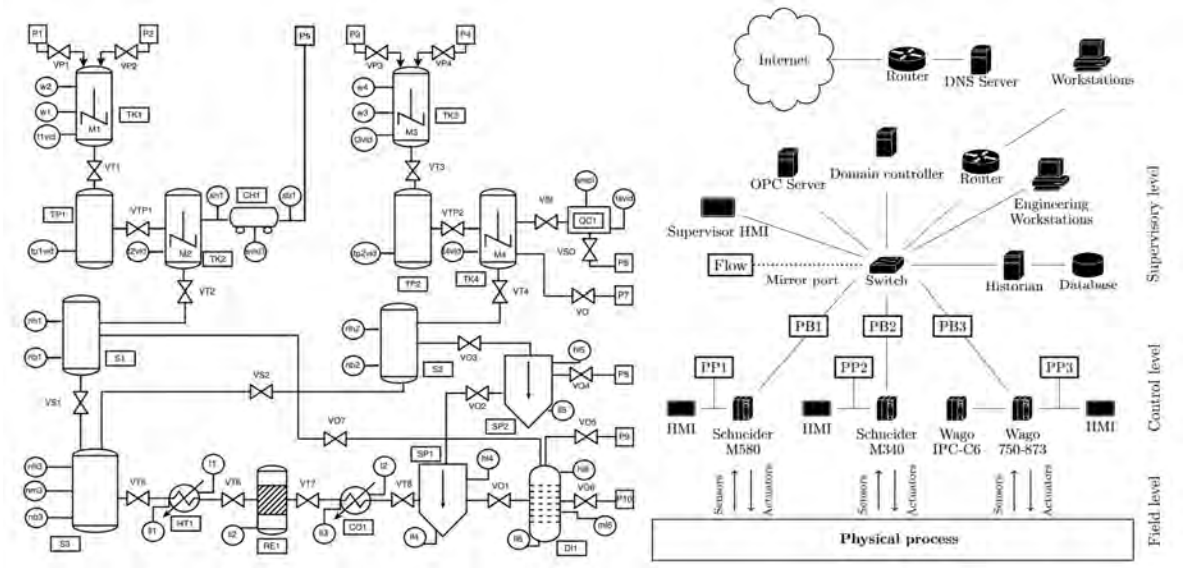

FIGURE 22 – Maquette Hardware-in-the-loop Tennesse-Eastman

Plusieurs datasets sont disponibles pour les attaques de type injection de fausse valeurs de capteurs dans les flots SMV (IEC 61850) ainsi que de type Ethernet flood dans les reséaux de haute fiabilité HSR/PRP.

.

10.6 Liste de publications commentée

[1] Estelle Hotellier, Franck Sicard, Julien Francq, and Stéphane Mocanu. Standard specification-based intrusion detection for hierarchical industrial control systems. *Information Sciences*, 659 :120102, February 2024. Le papier présente l'application de la méthodologie de détection des attaques sur le bus CANOpen et Modbus/TCP appliqués au cas d'usage des Robots 2D de la plateforme. Les attaques sont décrites également.

[2] Maëlle Kabir-Querrec, Stéphane Mocanu, Pascal Bellemain, Jean-Marc Thiriet, and Eric Savary. Corrupted GOOSE Detectors : Anomaly Detection in Power Utility Real-Time Ethernet Communications. In *GreHack 2015*, Grenoble, France, November 2015. Verimag. Les attaques sur le protocole GOOSE et l'algorithme de détection sont présentés ainsi que la maquette expérimentale utilisée pour validation.

[3] Maëlle Kabir-Querrec, Stéphane Mocanu, Jean-Marc Thiriet, and Eric Savary. A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks. In *ETFA 2016 - 21st IEEE Emerging Technologies and Factory Automation*, Berlin, Germany, September 2016. Ce papier présente les possibilités d'utilisation de la plateforme G-ICS pour l'étude de la cybersécurité des postes électriques IEC 61850.

[4] Oualid Koucham, Stéphane Mocanu, Guillaume Hiet, Jean-Marc Thiriet, and Frédéric Majorczyk. Detecting Process-Aware Attacks in Sequential Control Systems. In *NordSec 2016 - 21st Nordic Conference on Secure IT Systems (NordSec 2016)*, pages p.20–36, Oulu, Finland, November 2016.

Ce papier présente la méthodologie de détection des attaques orientés processus de type injection de commandes. La maquette expérimentale de typ eHardware-in-the loop est présentée également.

[5] Oualid Koucham, Stéphane Mocanu, Guillaume Hiet, Jean-Marc Thiriet, and Frédéric Majorczyk. Efficient Mining of Temporal Safety Properties for Intrusion Detection in Industrial Control Systems. In *SAFEPROCESS 2018 - 10th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*, pages 1–8, Varsovie, Poland, August 2018.

[6] Oualid Koucham, Stéphane Mocanu, Guillaume Hiet, Jean-Marc Thiriet, and Frédéric Majorczyk. Cross-domain Alert Correlation methodology for Industrial Control Systems. *Computers and Security*, 118(July) :102723, April 2022. Papier de synthèse des travaux de la thèse d'Oualid Koucham. On y présente : les attaques par injection des commandes, la détéction et la correlation des alertes avec d'autres méthodologies de détction (grammaires du protocoles et whitelists). Cas d'usage Tennesee-Eastman.

[7] Stéphane Mocanu, Maxime Puys, and Pierre-Henri Thevenon. An Open-Source Hardware-In-The-Loop Virtualization System for Cybersecurity Studies of SCADA Systems. In *C&esar 2019 - Virtualization and Cybersecurity*, pages 1–16, Rennes, France, November 2019. Ce papier détaille le système Hardware-in-the-loop : les cartes électroniques, l'interface avec la simulation logicielle et deux cas d'usage (Tennesee-Eastman et Smart-Grid).

[8] Stéphane Mocanu and Jean-Marc Thiriet. Experimental study of performance and vulnerabilities of IEC 61850 process bus communications on HSR networks. In *EuroS&PW 2020 - IEEE European Symposium on Security and Privacy Workshops*, pages 584–593, Gênes, Italy, September 2020. IEEE. Le papier présente les attaques par injection de fausses mesures dans les flots SMV ainsi que les flood Ethernet dans des architectures HSR. Les résultats sont validés sur la maquette Smart-Grids.

[9] Stéphane Mocanu and Jean-Marc Thiriet. Real-Time Performance and Security of IEC 61850 Process Bus Communications. *Journal of Cyber Security and Mobility*, 10(2) :1–42, April 2021. Le papier étend les résultats obtenus pour les architectures HSR aux architectures PRP. Les résultats sont validés sur une maquette Smart-Grid modifiée (architecture PRP).

[10] Maxime Puys, Pierre-Henri Thevenon, and Stéphane Mocanu. Hardware-In-The-Loop Labs for SCADA Cybersecurity Awareness and Training. In *ARES 2021 - 16th International Conference on Availability, Reliability and Security - Workshop on Education, Training and Awareness in Cybersecurity (ETACS 2021)*, Vienna, Austria, August 2021. On présente ici les scénarios pédagogiques déployées sur la plateforme G-ICS ainsi que sur les cas d'usage dévéloppées sur la même technologie Hardware-in-the-loop au CEA Grenoble(plateforme WonderICS).

[11] Maxime Puys, Pierre-Henri Thevenon, Stéphane Mocanu, Mathieu Gallissot, and Camille Sivelle. SCADA cybersecurity awareness and teaching with Hardware-In-The-Loop platforms. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 13(1) :4–32, 2022. Présentation des scénarios d'attaques complexes de type APT déployés sur les plateformes G-ICS et WonderICS.

[12] Jean-Marc Thiriet and Stéphane Mocanu. A course in cyber-security, with orientations towards cyber-physical systems. In *EAEEIE 2019 - 29th EAEEIE Annual Conference on Innovation in Education for Electrical and Information Engineering*, Ruse, Bulgaria, September 2019. Ce papier présente les possibilités d'utilisation de la plate-forme G-ICS pour l'enseignement en particulier les applications et cas d'usage qui ont été crées pour le projet Européen ASEAN FACTORI 4.0.