

VI. Rapport du lot de travail no. 6

Analyse de la cybersécurité

Membres :

Prof. Dr. Djaffar OULD ABDESLAM, UHA

Bushra CANAAN, UHA

Yosra KADRI, UHA

Abderrazek BADJI, UHA

VI.1. Contexte et objectif

Alors que la région du Rhin supérieur s'engage dans sa transformation en une zone économique sans émissions de gaz à effet de serre, l'intégrité, la fiabilité et la résilience de ses systèmes énergétiques sous-jacents deviennent essentielles à la réussite de cette initiative. Le projet CO2InnO soutient cette transformation par la démonstration et l'évaluation de technologies neutres sur le plan climatique, notamment des unités de cogénération à hydrogène, des solutions de mobilité durable et des infrastructures énergétiques intelligentes. Ces innovations, bien que bénéfiques pour l'environnement, introduisent de nouveaux niveaux de complexité et d'interdépendance numérique qui renforcent considérablement l'importance de la cybersécurité.

Dans ce contexte, le lot de travail 6 (WP6) sur la cybersécurité dans les systèmes énergétiques contribue directement au fonctionnement sûr et durable des principaux démonstrateurs du projet. Il renforce également la confiance des parties prenantes, favorise la conformité réglementaire et garantit que la transition vers la neutralité climatique est non seulement viable sur le plan technique et économique, mais aussi sûre et socialement acceptée.

La cybersécurité est une préoccupation transversale qui touche chaque composante majeure du projet CO2InnO. Les systèmes de contrôle en temps réel des démonstrateurs de cogénération à hydrogène, l'infrastructure de recharge intelligente pour la mobilité électrique et le fonctionnement à forte intensité de données des réseaux énergétiques modernes reposent tous sur des systèmes numériques potentiellement vulnérables aux cyberattaques. Une cybersécurité compromise dans l'un de ces systèmes pourrait perturber l'approvisionnement énergétique, mettre en danger la sécurité publique, éroder la confiance des utilisateurs et compromettre les objectifs généraux du projet.

En abordant explicitement et systématiquement la cybersécurité, ce lot de travail jette les bases d'une infrastructure énergétique résiliente et fiable dans la région du Rhin supérieur. Il soutient l'approche « laboratoire vivant » du projet CO2InnO en intégrant les considérations de cybersécurité dans les dimensions techniques, juridiques et sociales de la transition énergétique. Les connaissances acquises servent également de modèle reproductible pour d'autres régions entreprenant des transformations similaires.

L'objectif principal de ce lot de travail est d'étudier, de développer et d'évaluer des stratégies de cybersécurité qui soutiennent la mise en œuvre de solutions énergétiques décentralisées, numériques et durables. Il se concentre sur l'identification des vulnérabilités, la compréhension de la dynamique des menaces et la proposition de stratégies de détection et d'atténuation robustes et spécifiques au contexte.

Trois sous-tâches interdépendantes structurent le travail :

6.1. Modèle de simulation d'un micro-réseau réaliste, comprenant un rapport sur divers aspects de la conception du modèle, illustrant les défis rencontrés lors de son développement.

Cela comprend une analyse détaillée des décisions architecturales, des contraintes techniques, des préoccupations des parties prenantes et des obligations légales. Le rapport rend compte des enseignements tirés lors de la mise en œuvre du projet et fournit des recommandations concrètes pour les déploiements futurs.

6.2. Analyse basée sur l'IA pour la détection précoce des cybermenaces, répondant au besoin de mesures de sécurité proactives et adaptatives. L'objectif ici est de développer et d'évaluer un système basé sur l'apprentissage machine- , capable de détecter les anomalies et les intrusions potentielles, en utilisant les données opérationnelles des composants du système énergétique. Cette tâche soutient l'automatisation et l'évolutivité de la gestion de la cybersécurité dans des environnements complexes riches en données.

6.3. Rapport sur les aspects liés à la sécurité des compteurs intelligents modernes, proposant une analyse comparative de l'impact des différentes approches nationales et régionales en matière d'acquisition de données et de confidentialité sur la cybersécurité. Cette tâche examine comment les politiques, la réglementation et les tendances du marché influencent la conception, le déploiement et l'acceptation des infrastructures de comptage intelligent, en mettant l'accent sur le contexte européen et la région du Rhin supérieur.

Il convient de noter que le lot de travail comprend également deux sous-tâches supplémentaires qui ne relèvent pas du champ d'application du présent document. La sous-tâche 6.4, qui fournit une mise à jour réglementaire sur l'intégration de la sécurité cyber-physique dans les systèmes énergétiques, est traitée dans le rapport dédié préparé par le partenaire HS Kehl. De même, la sous-tâche 6.5, qui se concentre sur l'acceptation sociale des appareils intelligents et connectés dans les systèmes énergétiques, est présentée dans le rapport rédigé par le partenaire KIT-DFIU. Par conséquent, ce rapport final couvre exclusivement les trois premières sous-tâches.

Ces tâches s'inscrivent dans les objectifs plus larges de recherche et développement du projet CO2InnO et fournissent des informations essentielles aux axes de travail techniques, juridiques et sociétaux. Les résultats garantissent que la cybersécurité n'est pas traitée comme un problème technique isolé, mais comme un facteur clé de l'innovation, de l'intégration et de l'engagement des utilisateurs.

La cybersécurité des systèmes énergétiques a fait l'objet d'une attention croissante ces dernières années, en particulier avec le développement des réseaux intelligents, des appareils connectés à l'Internet des objets et de la production décentralisée. Les recherches ont mis en évidence des vulnérabilités dans les architectures des systèmes, les protocoles de communication et les composants hérités. En outre, des études montrent que les cyberattaques contre les infrastructures énergétiques sont de plus en plus fréquentes, ciblées et sophistiquées.

Dans le domaine des compteurs intelligents, les préoccupations relatives à l'intégrité des données, à la confidentialité et à l'exploitation à distance ont conduit à des approches nationales divergentes, créant ainsi un paysage réglementaire fragmenté. Parallèlement, l'intelligence artificielle apparaît comme un outil puissant pour la détection des intrusions, mais son efficacité dépend fortement de la qualité des données d'entraînement, de l'adaptation contextuelle et de la capacité à distinguer les anomalies bénignes des menaces réelles.

Malgré ces progrès, des lacunes subsistent dans l'intégration de la cybersécurité dès les premières étapes de la conception des systèmes énergétiques, en particulier pour les configurations novatrices telles que la cogénération à hydrogène. Les recherches empiriques sur l'interaction entre les cadres politiques nationaux et les choix de conception liés à la sécurité dans les infrastructures de comptage intelligent sont également limitées.

Le programme de travail repose sur les hypothèses de travail suivantes.

- Les systèmes énergétiques décentralisés et basés sur les données nécessitent des approches fondamentalement nouvelles en matière de cybersécurité.
L'hypothèse est que les modèles de sécurité traditionnels basés sur le périmètre sont insuffisants et que des modèles intégrés, adaptatifs et basés sur les données sont nécessaires.
- L'IA peut améliorer considérablement la détection des menaces dans les environnements énergétiques dynamiques. On s'attend à ce que les méthodes d'apprentissage automatique permettent d'identifier les cybermenaces plus tôt et avec plus de précision que les systèmes basés sur des règles, à condition qu'elles soient entraînées sur des données pertinentes pour le domaine et contextualisées pour les applications énergétiques.
- Les différences nationales en matière de politiques de comptage intelligent ont une incidence sur les résultats en matière de cybersécurité. Cette hypothèse explore la manière dont les cadres juridiques et réglementaires divergents en Allemagne et en France influencent la configuration technique et la posture de sécurité des systèmes de comptage intelligent.

Sur la base de ces hypothèses, le programme de travail poursuit les objectifs partiels suivants.

- Documenter et évaluer les défis et les solutions en matière de conception liés à la cybersécurité dans les démonstrateurs du projet.
- Étudier la détection et l'atténuation des menaces basées sur l'IA à l'aide de données et de scénarios spécifiques au projet.
- Analyser et comparer les implications en matière de cybersécurité des différentes politiques nationales en matière de compteurs intelligents, en mettant l'accent sur l'acquisition de données et la confidentialité des utilisateurs.

VI.2. Méthodologie

Ce lot de travail combine quatre axes de recherche complémentaires qui abordent les défis actuels et émergents dans les systèmes énergétiques distribués. La première partie fournit un compte rendu détaillé de la conception, de la mise en œuvre et de la simulation d'un démonstrateur de micro-réseau réel situé à l'IUT de Mulhouse, dans l'UHA. Elle se concentre sur l'architecture du système physique, l'intégration des énergies renouvelables et les premières étapes vers le développement d'un jumeau numérique comme base pour de futures applications de sécurité cyber-physique. Ce micro-réseau réel sert de cadre opérationnel polyvalent qui favorise la reproductibilité et les futurs scénarios de déploiement pour les infrastructures régionales dans le Rhin supérieur et dans toute l'Europe.

Sur cette base, la deuxième partie examine les techniques basées sur l'IA pour détecter les menaces cyber-physiques dans les environnements de micro-réseaux. Elle décrit le développement et le test de modèles d'apprentissage profond, en particulier les réseaux neuronaux récurrents LSTM, pour la détection d'anomalies dans les flux énergétiques critiques. Cette partie met en évidence la manière dont l'IA peut améliorer la connaissance de la situation et fournir des mécanismes d'alerte précoce pour les perturbations cybernétiques et physiques dans les systèmes énergétiques distribués.

La troisième partie se concentre sur les infrastructures de comptage intelligent et les défis de cybersécurité qui y sont associés, en particulier dans le contexte de l'interopérabilité transfrontalière et des objectifs de politique régionale dans le Rhin supérieur. Elle examine l'état actuel du déploiement des compteurs intelligents en France, en Allemagne et en Suisse, met en évidence les obstacles techniques et juridiques qui affectent leur déploiement et analyse les vulnérabilités découlant de la connectivité numérique accrue.

Enfin, la quatrième partie élargit la portée des travaux en explorant les considérations relatives à la numérisation, à la cybersécurité et à la résilience d'un système hypothétique de cogénération (CHP) à base d'hydrogène. Directement liée aux objectifs généraux du projet CO2InnO, elle documente les architectures potentielles, les vulnérabilités et les stratégies d'atténuation basées sur l'IA pour les infrastructures énergétiques fonctionnant à l'hydrogène.

Ensemble, ces quatre volets retracent le continuum de la transition énergétique européenne,

VI.2. reliant les micro-réseaux renouvelables actuels, la sécurité cyber-physique améliorée par l'IA, l'épine dorsale numérique de l'infrastructure de comptage intelligent et les futurs systèmes à base d'hydrogène dans un cadre climatiquement neutre, interopérable et cyber-résilient.

Conception et simulation d'un micro-réseau réel

Le système de micro-réseau de l'IUT de Mulhouse sert de démonstrateur modulaire et flexible pour l'intégration des énergies renouvelables distribuées. Il a été conçu pour reproduire des scénarios de déploiement urbain typiques tout en permettant des recherches avancées sur le contrôle, la simulation et la sécurité cyber-physique. Le système physique intègre la production

photovoltaïque (PV), le stockage d'énergie stationnaire et mobile, des dispositifs de conversion d'énergie et des contrôleurs communicants.

Ce micro-réseau s'inscrit dans les objectifs plus larges du projet, qui sont d'atteindre la neutralité climatique, de faire progresser la production d'énergie renouvelable distribuée et d'améliorer la résilience des systèmes énergétiques numérisés. La méthodologie de conception met l'accent à la fois sur la flexibilité opérationnelle et la validation du matériel, garantissant ainsi que les résultats sont applicables à des déploiements réels tout en restant évolutifs pour les recherches futures dans la région du Rhin supérieur et au-delà.

Structure du micro-réseau et sélection des équipements

VI.2.2. Le démonstrateur de micro-réseau comprend des unités modulaires de production, de stockage et de conversion qui reflètent les pratiques actuelles de déploiement dans les réseaux énergétiques urbains et semi-urbains à petite échelle. La capacité photovoltaïque totale installée est de 6,6 kWc, répartie entre des panneaux mobiles et fixes afin de faciliter l'analyse comparative et divers scénarios opérationnels. Cette infrastructure solaire diversifiée permet la collecte d'ensembles de données hétérogènes, qui sont essentiels pour l'entraînement des algorithmes de détection des anomalies et le test des stratégies de contrôle adaptatif.

Le sous-système photovoltaïque comprend deux grandes catégories d'installations. Les suiveurs photovoltaïques dynamiques se composent de deux structures fonctionnant indépendamment, chacune équipée de quatre panneaux solaires et de deux micro-onduleurs. Ces suiveurs sont équipés de contrôleurs intégrés de suivi du point de puissance maximale (MPPT) afin d'optimiser la collecte d'énergie. L'actionnement mécanique est assuré par deux motoréducteurs, tandis que des anémomètres intégrés et des systèmes de commande à distance garantissent un retrait sûr en cas de conditions météorologiques défavorables. En revanche, les panneaux photovoltaïques statiques fournissent une capacité de production solaire fixe. Il s'agit notamment d'un abri à vélos équipé de huit modules fixes délivrant 2,16 kWc sur une surface de 13,2 m². En combinant des unités photovoltaïques mobiles et fixes, le système se reproduit la diversité des scénarios de déploiement solaire urbain et enrichit l'ensemble de données opérationnelles du micro-réseau.

Le sous-système de stockage utilise également une double structure. Les batteries fixes se composent de deux modules, chacun contenant cinq batteries pour une capacité totale de 24 kWc. Ces batteries permettent le stockage d'énergie, l'équilibrage de charge et l'écrêtement des pics au sein du micro-réseau. Ce stockage fixe est complété par un véhicule électrique mobile (VE) équipé d'une batterie embarquée de 6,1 kWc.

Pour la conversion et le contrôle de l'énergie, le micro-réseau intègre plusieurs dispositifs.

- Des micro-onduleurs sont dédiés aux suiveurs PV dynamiques, chacun mettant en œuvre des algorithmes MPPT pour une collecte optimale de l'énergie solaire.
- Deux onduleurs monophasés CC/CA gèrent la conversion du courant continu en courant alternatif compatible avec le réseau, garantissant ainsi l'interopérabilité avec le réseau électrique.
- Des convertisseurs CC/CC bidirectionnels sont mis en œuvre pour les systèmes de stockage, contrôlés via des algorithmes proportionnels-intégraux (PI) avec des mécanismes anti-saturation afin de maintenir des comportements de charge et de décharge stables.

L'architecture générale du démonstrateur de micro-réseau et les flux électriques qui le traversent sont représentés dans la Figure VI-1 ci-dessous.

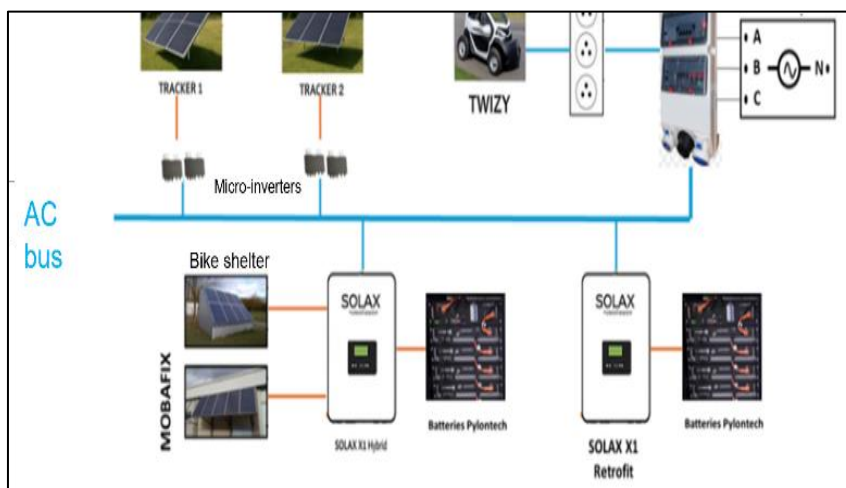


Figure VI-1: Architecture générale du démonstrateur de micro-réseau
VI.2.3.

Modélisation et simulation des composants physiques

Le système énergétique et ses composants sont modélisés à l'aide de MATLAB/Simulink avec la bibliothèque Simscape Power Systems. L'environnement de simulation peut servir à la fois de modèle numérique et de plateforme pour la détection d'anomalies et l'expérimentation cyber-physique.

Pour la modélisation des cellules photovoltaïques, chaque module photovoltaïque est représenté à l'aide d'un modèle électrique équivalent basé sur les paramètres du fabricant, les profils d'irradiation solaire et la température ambiante. Cette modélisation facilite la prévision précise de la puissance de sortie et permet de prévoir le comportement en temps réel.

L'algorithme Perturb and Observe (P&O) a été sélectionné pour le MPPT en raison de sa simplicité et de son efficacité. Il est mis en œuvre numériquement dans le cadre de la simulation afin d'évaluer les performances de contrôle sous un apport solaire variable.

Pour la modélisation des batteries, un modèle dynamique non linéaire issu de la bibliothèque de modèles de batteries SimPowerSystems a été utilisé pour simuler la tension aux bornes et estimer l'état de charge (SoC) des batteries. Ce modèle permet d'estimer avec précision les profils de charge et de décharge. Les convertisseurs CC/CC ont été modélisés de manière à refléter les flux d'énergie bidirectionnels avec un contrôle basé sur PI pour la régulation du courant. Les onduleurs CC/CA ont utilisé des stratégies PWM (modulation de largeur d'impulsion) pour synthétiser des sorties sinusoïdales de qualité réseau.

Toutes les fonctions de contrôle sont coordonnées par un cadre centralisé qui garantit un fonctionnement fiable et permet la surveillance externe des flux d'énergie. L'infrastructure est donc bien adaptée à l'intégration ultérieure de technologies de jumeaux numériques qui reposent sur l'acquisition et l'analyse de données en temps réel.

Développement du jumeau numérique

VI.2.4. Sur la base de la modélisation, de la simulation et de la validation du contrôle, des efforts ont été entrepris pour créer un jumeau numérique (DT) du micro-réseau. Reconnaisant l'importance croissante des jumeaux numériques dans l'amélioration de la sécurité cyber-physique, une revue de la littérature sur les jumeaux numériques de micro-réseaux (MGDT) a été réalisée. Cette revue s'est concentrée sur leur rôle potentiel dans l'amélioration de la résilience face aux menaces cyber-physiques et l'intégration de l'intelligence artificielle pour un contrôle prédictif et adaptatif. Les résultats de ces travaux ont abouti à un article détaillé, actuellement en cours d'examen par des pairs, qui propose une classification des MGDT en fonction des fonctions de sécurité et examine les possibilités d'intégration de l'IA dans les cadres de jumeaux numériques pour la cyber-résilience des micro-réseaux. L'étude met également en évidence les orientations futures de la recherche, en particulier vers des MGDT plus intelligents et axés sur la sécurité.

Dans le cadre d'une démarche pratique visant à mettre en œuvre un jumeau numérique du démonstrateur de micro-réseau à l'UHA, des efforts de benchmarking ont été entrepris afin de collecter des données en temps réel sur les flux d'énergie pendant plusieurs jours et dans des conditions météorologiques variables. La Figure VI-2 présente un exemple de graphique de la production et de la consommation du micro-réseau obtenu sur 7 heures le 3 avril 2025.

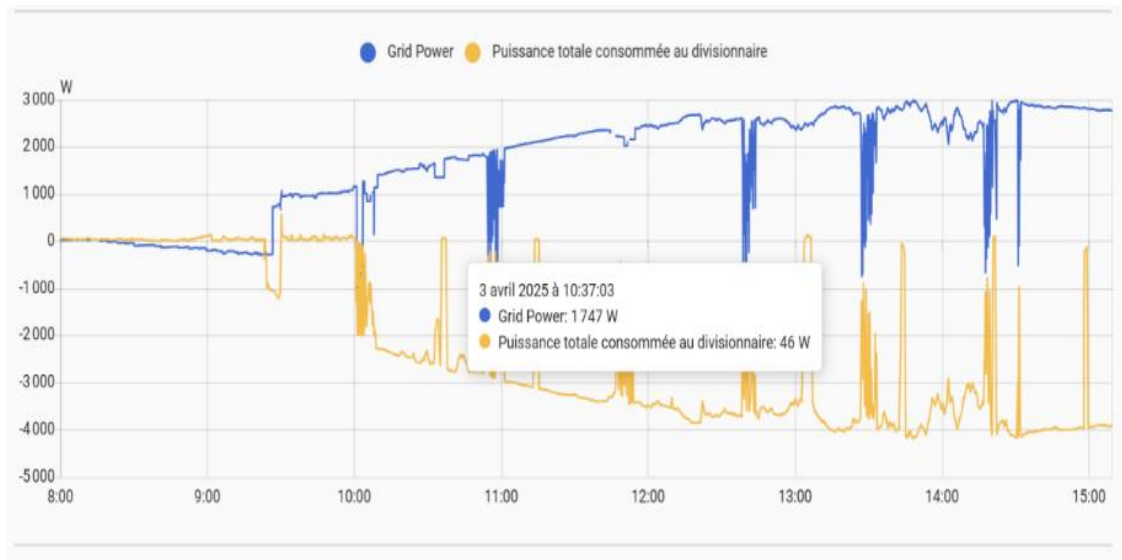


Figure VI-2: Graphiques en temps réel de la production et de la consommation d'électricité

L'ensemble de données haute résolution qui en résulte capture le comportement du système dans divers états opérationnels, servant deux objectifs clés. Premièrement, il fournit une base empirique pour le développement d'un jumeau numérique dynamique, basé sur les données, capable de refléter les conditions opérationnelles évolutives du micro-réseau physique. Deuxièmement, il soutient la formation et la validation de modèles basés sur l'IA pour la détection d'anomalies, la prédiction ou l'optimisation, comblant ainsi le fossé entre les stratégies actuelles de contrôle des micro-réseaux et les futurs cadres cyber-physiques intelligents.

Ces premières étapes dans le développement du jumeau numérique établissent une feuille de route pour la transition du démonstrateur de micro-réseau vers une plateforme de recherche plus avancée sur la résilience cyber-physique. En combinant une infrastructure physique soigneusement instrumentée avec une analyse comparative des données en temps réel, les bases sont jetées pour l'intégration de fonctions basées sur l'IA qui permettront l'analyse prédictive, la détection avancée des intrusions et une cybersécurité renforcée.

Système de détection basé sur l'IA pour la surveillance des anomalies cyber-physiques

Afin de garantir la sécurité et la fiabilité du micro-réseau, un système de détection basé sur l'apprentissage profond a été développé à l'aide d'un réseau neuronal récurrent à mémoire à court et long terme (LSTM). Les modèles LSTM ont été sélectionnés en raison de leur capacité supérieure à gérer les dépendances à long terme dans les données chronologiques, surmontant ainsi le problème de gradient disparaissant courant dans les réseaux neuronaux récurrents (RNN) traditionnels. Leur architecture à portes permet au réseau de conserver de manière sélective les informations pertinentes et d'écarter les entrées non pertinentes,

améliorant ainsi la précision des prévisions futures. Le LSTM fonctionne en boucle fermée, utilisant les entrées et sorties passées pour estimer les états actuels du système, ce qui renforce sa robustesse dans la détection d'anomalies subtiles causées par des cyberattaques physiques.

Cette approche s'appuie sur des travaux antérieurs réalisés dans le cadre du projet RES-TMO Interreg, où un réseau neuronal de type NARX (Nonlinear AutoRegressive model with eXogenous inputs) a été déployé comme système de détection intelligent pour surveiller les échanges d'énergie active au point de couplage commun (PCC). Si le réseau NARX a réussi à détecter des anomalies dans des configurations plus simples en comparant les valeurs prévues et réelles des capteurs, il a montré ses limites lorsqu'il a été appliqué à des systèmes de contrôle plus complexes avec des systèmes de gestion de batterie (BMS) à conditions multiples. Ces limites résultaient, entre autres, du problème de gradient disparaissant, qui affectait la capacité du réseau à apprendre les dépendances à long terme.

Le système actuel basé sur LSTM a été évalué dans le cadre de deux grandes catégories de scénarios d'attaque. La première concernait les cyberattaques telles que l'injection de fausses données (FDI) et les attaques par rejeu, dans lesquelles des canaux de communication compromis permettent aux attaquants de modifier les mesures transmises. Le second type ciblait la couche physique, où un intrus pouvait manipuler le programme de contrôle des batteries pour provoquer des effets néfastes. Ensemble, ces scénarios ont permis une évaluation complète de la capacité du système à détecter et à répondre aux intrusions cybernétiques et physiques dans le micro-réseau.

VI.2.6.

Infrastructure de comptage intelligent et intégration dans les systèmes de cogénération

L'approche méthodologique adoptée pour étudier les compteurs intelligents dans le cadre du projet CO2InnO a combiné des perspectives réglementaires, techniques et opérationnelles afin de fournir une compréhension holistique de leur rôle dans les futurs systèmes énergétiques distribués. Une analyse comparative des politiques et pratiques de déploiement des compteurs intelligents a été réalisée en France, en Allemagne et en Suisse, avec un accent particulier sur la région du Rhin supérieur. Cette évaluation a consisté à examiner les infrastructures de comptage actuelles, telles que le système français Linky et les compteurs de gaz Gazpar utilisant la technologie Wize. Ces résultats ont ensuite été mis en correspondance avec les exigences évolutives du couplage sectoriel, soulignant la manière dont les infrastructures de comptage doivent évoluer pour prendre en compte non seulement les données électriques, mais aussi les flux d'énergie multivectoriels tels que l'hydrogène.

La méthodologie a ensuite été étendue afin d'examiner comment les infrastructures de comptage intelligent peuvent soutenir l'intégration des systèmes de cogénération (CHP) à base d'hydrogène. Cette étape s'est concentrée sur l'identification des besoins

supplémentaires en données des unités de cogénération, tels que la surveillance du flux d'hydrogène, de la pression et des émissions, et sur l'évaluation de la manière dont les technologies de communication basées sur l'IoT, telles que LoRaWAN, pourraient connecter ces actifs au sein des réseaux intelligents. Si LoRa offre des avantages pratiques pour les systèmes distribués, ses limites connues en matière de sécurité nécessitent une évaluation ciblée des risques afin de remédier aux vulnérabilités des systèmes de communication, de contrôle et de sécurité. Une modélisation basée sur des scénarios a été utilisée pour illustrer comment les cyberintrusions ciblant la surveillance numérique ou les boucles de contrôle de sécurité pourraient dégénérer en dangers physiques, notamment des défaillances en cascade ou des explosions.

En alignant ces connaissances méthodologiques sur le contexte plus large de la politique et du déploiement des compteurs intelligents dans le Rhin supérieur, la recherche a établi un cadre analytique cohérent qui relie la préparation des infrastructures numériques au déploiement sûr et résilient des unités de cogénération à hydrogène.

Cybersécurité et résilience des systèmes de cogénération à hydrogène

VI.2. Alors que le démonstrateur de micro-réseau se concentre sur les technologies renouvelables actuelles, le projet CO2InnO se tourne également vers les infrastructures futures qui intègrent l'hydrogène comme vecteur énergétique clé. Les systèmes de cogénération à hydrogène sont envisagés comme un élément essentiel des réseaux énergétiques neutres sur le plan climatique, fournissant à la fois de l'énergie électrique et thermique tout en permettant le couplage sectoriel entre l'électricité, le chauffage et la mobilité. Cependant, la numérisation croissante des infrastructures énergétiques à hydrogène introduit de nouveaux risques, faisant de la cybersécurité et de la résilience des domaines de recherche essentiels.

Cette partie du travail examine les implications en matière de cybersécurité d'une unité de cogénération hypothétique à base d'hydrogène. Elle se concentre sur les architectures conceptuelles, les vulnérabilités potentielles et les stratégies d'atténuation qui peuvent éclairer la conception et le développement futurs.

Les systèmes de cogénération à hydrogène diffèrent des systèmes traditionnels à plusieurs égards. L'utilisation de l'hydrogène comme combustible introduit une dynamique opérationnelle, notamment la nécessité de solutions de stockage avancées, de systèmes de gestion de la sécurité complexes et de réseaux de communication sensibles pour surveiller la pression, la température et la composition du gaz. L'intégration de ces systèmes dans des réseaux intelligents plus larges nécessite des interfaces sécurisées avec des systèmes de contrôle de supervision et d'acquisition de données (SCADA), des plateformes de gestion de l'énergie basées sur le cloud et des capteurs compatibles avec l'IoT. Chacune de ces interfaces numériques élargit la surface d'attaque pour les cybermenaces potentielles. La

Figure VI-3 illustre l'intégration de la cogénération dans l'infrastructure énergétique et les vecteurs d'attaque potentiels impliqués.

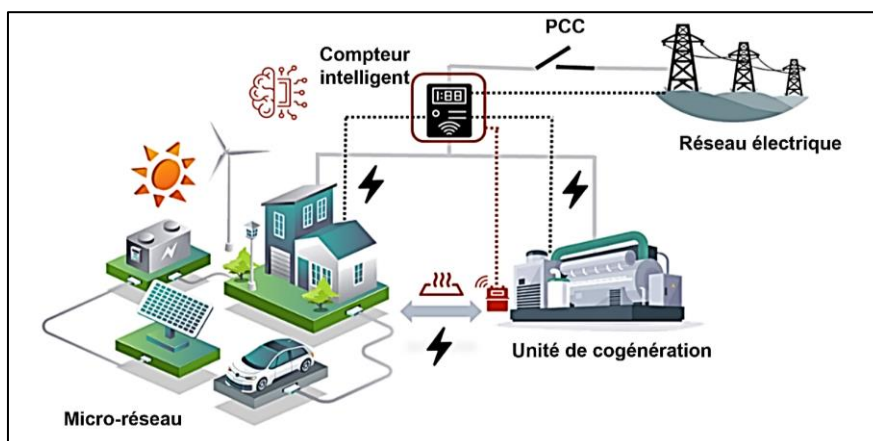


Figure VI-3: Intégration de la cogénération dans les systèmes énergétiques et vecteurs d'attaque de cybersécurité

Les cyberattaques physiques visant la cogénération à hydrogène pourraient avoir des conséquences importantes, allant de perturbations opérationnelles à des risques pour la sécurité physique. Il s'agit notamment de la manipulation de capteurs de pression ou de vannes de régulation de débit, entraînant des conditions de fonctionnement dangereuses. L'interférence avec les boucles de contrôle en temps réel peut entraîner des inefficacités ou des arrêts forcés, tandis que la falsification des flux de données peut masquer la présence de défauts, retardant ainsi les temps de réponse. Au-delà des conséquences physiques directes sur l' , de telles attaques pourraient également compromettre l'intégrité des transactions commerciales et éroder la confiance des parties prenantes dans les systèmes énergétiques à hydrogène.

Pour faire face à ces risques, l'étude explore comment l'intelligence artificielle et les technologies de jumeaux numériques peuvent améliorer la cybersécurité. Des cadres conceptuels illustrent comment l'IA pourrait être intégrée dans les jumeaux numériques afin d'assurer une surveillance continue et la détection des anomalies. Une telle approche permettrait au système d'apprendre les schémas de fonctionnement normaux et de signaler automatiquement les écarts pouvant indiquer des cyberintrusions ou des défaillances.

Les stratégies de résilience pour la cogénération à hydrogène vont également au-delà de la détection des anomalies. Des protocoles de communication sécurisés, des systèmes de détection des intrusions et la redondance des composants de contrôle critiques sont des mesures essentielles pour garantir qu'une cogénération à hydrogène puisse continuer à fonctionner en toute sécurité en cas de stress cyber-physique. De plus, la résilience au niveau du système nécessite des stratégies de réponse coordonnées qui intègrent la cogénération

aux réseaux énergétiques environnants, garantissant ainsi que les perturbations soient contenues et que la reprise soit rapide.

En tenant compte de ces éléments dans le contexte du projet CO2InnO, les travaux soulignent que la cybersécurité de la cogénération à hydrogène n'est pas un défi isolé, mais s'inscrit dans le cadre plus large de la transition énergétique. L'intégration sûre et sécurisée des infrastructures hydrogène dans les réseaux intelligents numérisés nécessitera une combinaison de conception matérielle robuste, d'architectures logicielles sécurisées et de surveillance intelligente basée sur des modèles alimentés par l'IA.

VI.3. Résultats

Cette section présente les résultats obtenus dans quatre domaines complémentaires. La première partie traite des performances opérationnelles du démonstrateur de micro-réseau dans diverses conditions, soulignant sa capacité à maintenir la stabilité, à garantir une gestion optimale de l'énergie et à réagir aux événements du réseau. Sur la base de cette validation, la deuxième partie examine l'utilisation de techniques basées sur l'IA, en particulier les modèles d'apprentissage profond LSTM, pour détecter les menaces cyber physiques dans les opérations des micro-réseaux. Ces résultats démontrent comment la détection avancée des anomalies peut améliorer la résilience contre les intrusions numériques et les interventions physiques malveillantes. La troisième partie analyse le paysage politique et pratique des compteurs intelligents dans la région du Rhin supérieur, élargissant la discussion aux défis réglementaires et d'intégration transfrontalière. La dernière partie s'appuie sur les discussions précédentes pour aborder les défis de la cybersécurité et de la numérisation des infrastructures couplées au secteur, en se concentrant spécifiquement sur les systèmes de cogénération à hydrogène. À travers un scénario illustratif d'attaque cyber-physique, elle met en évidence les risques introduits par une connectivité accrue et souligne la nécessité d'une surveillance intégrée basée sur l'IA et de stratégies de sécurité robustes. Ensemble, ces résultats fournissent une vue d'ensemble de la résilience physique et numérique des futures infrastructures énergétiques décentralisées.

Validation des performances du démonstrateur de micro-réseau en conditions réelles

Le système de micro-réseau de l'UHA a été conçu pour intégrer des sources d'énergie renouvelables distribuées, des unités de stockage et une flexibilité du côté de la demande, tout en maintenant un fonctionnement fiable en mode connecté au réseau et en mode îloté. Les résultats de simulation obtenus dans MATLAB/Simulink démontrent la capacité des stratégies de contrôle du micro-réseau à gérer des conditions dynamiques, des perturbations du réseau et des profils de charge et de production variables.

Robustesse de la synchronisation du réseau

Deux scénarios de défaillance du réseau ont été simulés afin d'évaluer la stabilité de la boucle à verrouillage de phase (PLL) de l'onduleur. Tout d'abord, une forte chute de tension de 90 % d'amplitude a été appliquée pendant 1 seconde. Comme l'illustre la Figure VI-4, la chute de tension n'a entraîné aucune perte de verrouillage de la PLL. Le courant i_g de l'onduleur est resté aligné en phase et stable, avec une distorsion harmonique minimale.

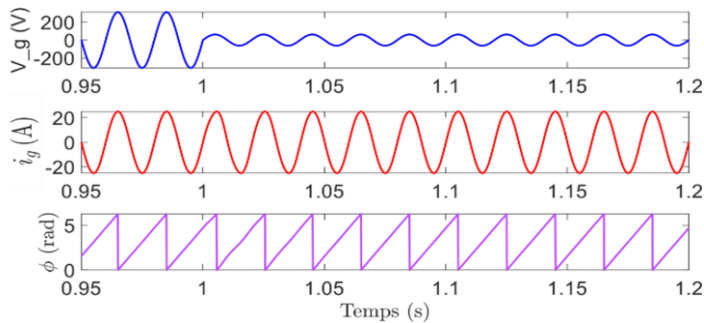


Figure VI-4: Réponse à une chute de tension de 90 %, formes d'onde de tension, de courant et de phase

Pour le deuxième scénario de défaut, un saut de phase brusque du réseau a également été introduit à 1 seconde. La PLL a réussi à suivre et à corriger le signal déformé du réseau en un cycle, avec un dépassement minimal, comme le montre la Figure VI-5. La convergence rapide a empêché l'apparition de courants circulants indésirables et a protégé les charges sensibles contre l'instabilité transitoire.

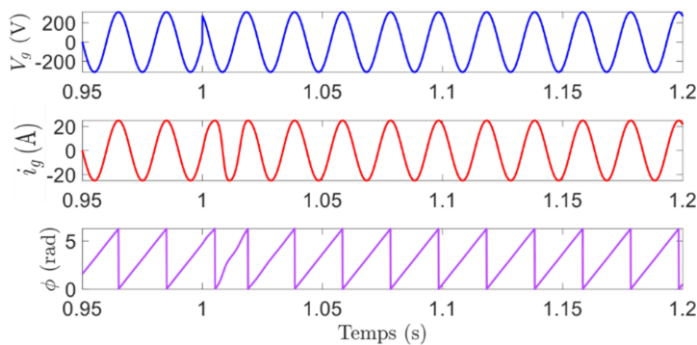


Figure VI-5: Réponse de la PLL au saut de phase

VI.3.3.

Ces tests ont confirmé une forte résilience de la synchronisation en cas de perturbations importantes.

Fonctionnement normal sous des apports solaires variables

Un profil d'irradiance variable dans le temps a reproduit des conditions de ciel clair, de fluctuations et d'ombrage. La Figure VI-6 montre comment la production d'énergie photovoltaïque a suivi avec précision les modèles d'irradiance. Les résultats du système

complet, présentés dans la Figure VI-7, confirment que le courant I_g suit parfaitement la référence, avec un temps de réponse acceptable. L'amplitude de I_g est également cohérente avec la référence, reflétant le profil d'irradiation solaire. Les tensions V_g et U_{dc} conservent leurs valeurs initiales, démontrant une régulation correcte de la tension du bus CC.

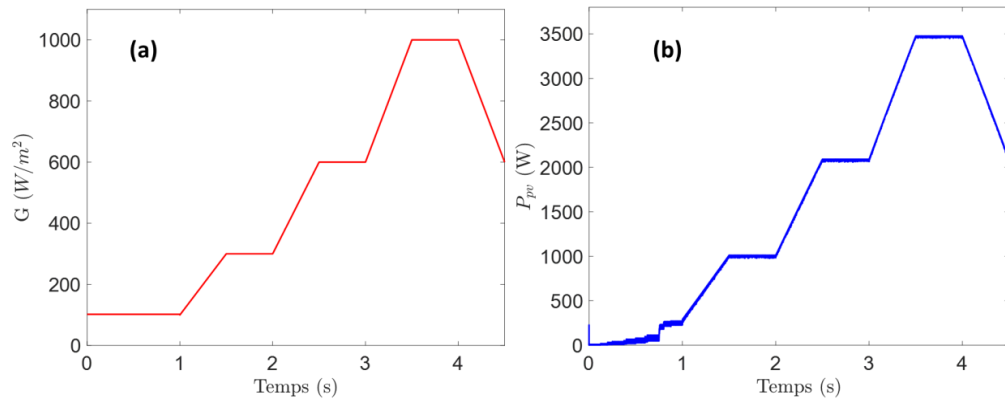


Figure VI-6: Production des panneaux photovoltaïques fixes dans des conditions d'ensoleillement variables (a) Profil d'irradiance (b) Profil de production d'énergie solaire

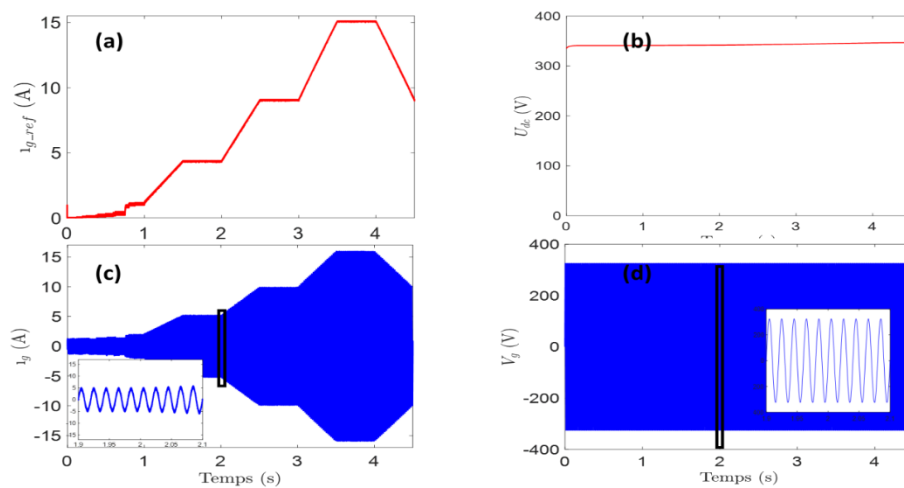


Figure VI-7: Résultats des performances de l'onduleur. (a) Profil du courant de référence du réseau (b) Tension du bus CC (c) Courant alternatif du réseau (d) Tension du réseau

VI.3.4.

Cela indique une régulation efficace et une alimentation électrique stable, même en cas de fluctuations des apports renouvelables.

Stratégie de gestion de l'énergie

Afin de valider les performances du système de gestion de l'énergie mis en place, une étude observationnelle approfondie a été menée pendant plusieurs jours dans différentes conditions de fonctionnement, y compris des scénarios avec et sans connexion d'un véhicule électrique (VE). Les paramètres électriques clés, tels que la tension, le courant et la puissance de sortie des panneaux photovoltaïques (PV), ainsi que les sorties des onduleurs, ont été mesurés en

continu à plusieurs points de l'installation. Ces mesures ont permis une évaluation détaillée de la disponibilité totale d'énergie, de l'état de charge des batteries, de la consommation globale et des flux d'énergie bidirectionnels entre le micro-réseau et le réseau électrique externe.

L'analyse a confirmé que le système hybride privilégie l'utilisation directe de l'énergie solaire produite localement pour alimenter la charge, les onduleurs étant configurés pour acheminer l'énergie PV vers les points de consommation avant de faire appel à d'autres ressources. Lorsque la production PV était insuffisante, les batteries complétaient de manière transparente l'approvisionnement en énergie, garantissant ainsi l'équilibre et la continuité. Ce n'est que lorsque la production photovoltaïque et les réserves des batteries étaient insuffisantes que le micro-réseau puisait de l'énergie dans le réseau externe. En outre, l'étude a vérifié que la charge des batteries était strictement limitée à la production solaire excédentaire, renforçant ainsi l'objectif de maximiser l'autoconsommation et de minimiser la dépendance vis-à-vis des sources externes. Ces résultats démontrent l'efficacité de la stratégie de gestion de l'énergie mise en œuvre pour optimiser l'utilisation des ressources et maintenir un fonctionnement stable dans des conditions de charge et de production dynamiques.

Ces résultats confirment que le démonstrateur de micro-réseau peut maintenir sa stabilité dans des conditions de réseau perturbées et normales, tandis que son cadre de gestion de l'énergie maximise efficacement l'utilisation locale des énergies renouvelables et soutient les services auxiliaires.

VI.3.5.

Performances de détection des cyberattaques physiques basées sur le LSTM

Cette section présente les résultats de la formation du système de détection basé sur LSTM et évalue ses performances dans divers scénarios d'attaques cyber-physiques ciblant le micro-réseau. L'analyse se concentre d'abord sur la capacité du modèle à apprendre et à prédire la puissance active au point de couplage commun (Ppcc) dans des conditions de fonctionnement normales, puis sur sa réponse aux cyberattaques sur la couche de communication et aux intrusions physiques au niveau du contrôle.

VI.3.6.

Résultats de l'entraînement LSTM

Le système de détection basé sur LSTM a été formé pour prédire directement le Ppcc, en contournant l'étape intermédiaire d'estimation de l'état de la batterie. Cette approche directe s'est avérée avantageuse pour reconnaître plusieurs conditions de fonctionnement, permettant la détection d'attaques même lorsque le système de gestion de batterie (BMS) fonctionne selon des schémas de contrôle complexes. Trois configurations ont été testées et les résultats sont présentés dans les graphiques comparatifs de l'VI-8 . Les tests initiaux ont utilisé un réseau avec une seule couche LSTM de 200 unités cachées, combinée à une couche entièrement connectée, et ont été entraînés sur un ensemble de données de 1000 secondes.

Bien que cette configuration (Istm1) ait fourni des résultats généralement précis, des perturbations mineures et des erreurs d'estimation occasionnelles ont été observées. Ces imprécisions ont été considérablement réduites lorsque l'ensemble de données d'entraînement a été étendu à 4 000 secondes, ce qui a permis d'améliorer les performances de la deuxième configuration (Istm2). Cependant, les meilleurs résultats ont été obtenus avec une architecture plus profonde comprenant deux couches LSTM empilées (Istm3), qui ont permis d'obtenir des performances d'estimation optimales. Les résultats de l'entraînement de Istm3 ont démontré des prévisions très stables avec un écart minimal dans des conditions normales.

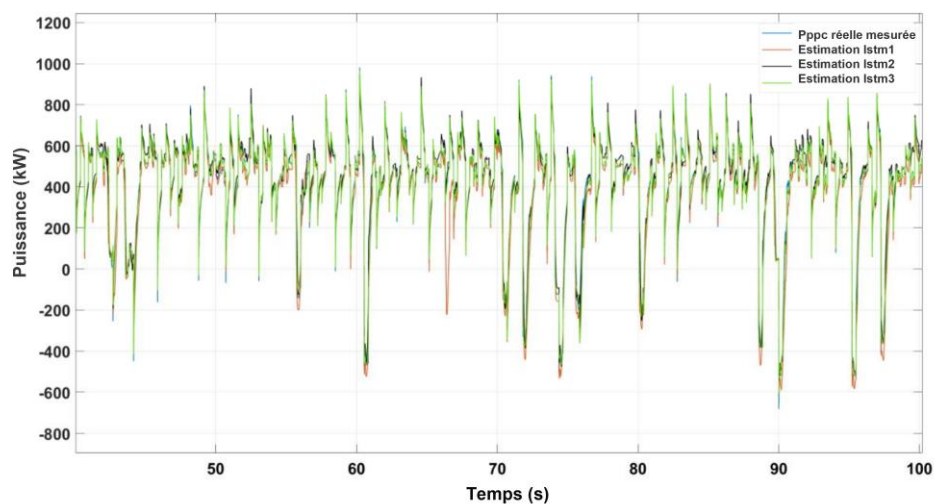


Figure VI-8: puissance prévue des trois configurations par rapport à la mesure réelle

La Figure VI-9 détaille les indicateurs de performance RMSE (Root mean Square Error) et Loss de Istm3.

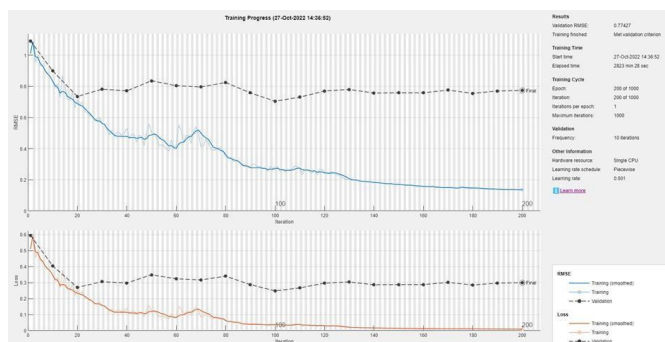


Figure VI-9 : Résultats de l'entraînement de la configuration Istm3

Scénarios d'attaques cyber-physiques et évaluation

Une fois que le modèle a atteint des performances de base stables, il a été évalué dans différents scénarios d'attaques cyber-physiques.

VI.3.7. Pour l'attaque par injection de fausses données (FDI) sur la production photovoltaïque, un signal de surproduction a été injecté à la 20e seconde du test. Ce type d'attaque imite un comportement frauduleux visant à manipuler les programmes de subventions en gonflant artificiellement la production photovoltaïque déclarée. L'attaque a provoqué une divergence immédiate entre le Ppcc mesuré physiquement et le signal estimé par le LSTM, clairement visible dans Figure VI-10 (a) et dans l'Figure VI-10(b). Contrairement aux perturbations transitoires qui génèrent généralement des pics d'erreur isolés, cette attaque a entraîné un décalage soutenu entre les valeurs mesurées et estimées, signalant une manipulation intentionnelle des données.

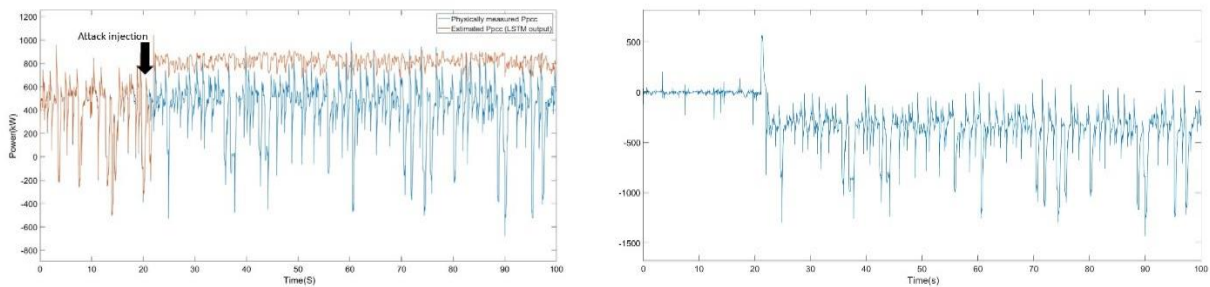


Figure VI-10: prédiction LSTM avant et après l'injection de l'attaque FDI (a) Graphique du signal (b) Graphique des erreurs

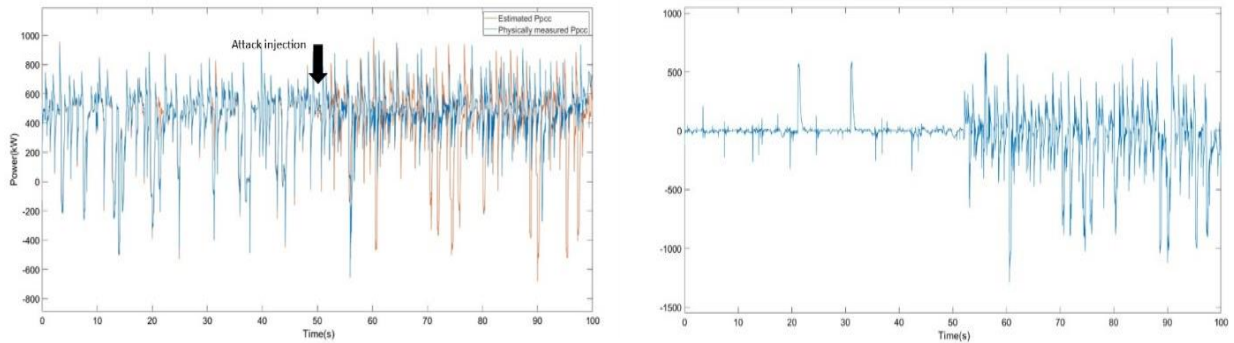


Figure VI-11: prédiction LSTM avant et après l'injection de l'attaque par rejeu (a) Graphique du signal (b) Graphique des erreurs

Une attaque par rejeu a ensuite été introduite à la 50e seconde d'un autre test. Dans ce scénario, un profil de production photovoltaïque précédemment enregistré dans des conditions favorables a été rejoué afin de tromper le système. De telles attaques sont particulièrement difficiles à détecter, car les mesures injectées suivent une distribution parfaitement valide, provenant du même système. Malgré cela, le modèle LSTM a réussi à détecter l'anomalie, comme le montre l'écart persistant entre les mesures en temps réel et les valeurs prédites (Illustration VI-11. (a)). Cette discordance était encore plus évidente dans le graphique d'erreur

d'Figure VI-11. (b), où la divergence continue distinguait clairement l'attaque des fluctuations opérationnelles normales.

Au-delà des cyberattaques, le système a également été testé contre des intrusions au niveau de la couche physique, en particulier un scénario de charge forcée. Ici, l'attaquant a émis une commande qui contournait les contraintes du BMS et déclençait la charge de la batterie dans des conditions défavorables. Cette manipulation a forcé la batterie à consommer de l'énergie alors qu'elle n'aurait pas dû, ce qui aurait pu solliciter le micro-réseau ou même entraîner une dégradation du système de stockage. Dans ce test, la commande de charge forcée a provoqué un déraillement clair de la courbe Ppcc mesurée par rapport au SIGNAL estimé, comme le montre la figure 12, soulignant la capacité du LSTM à identifier les anomalies au-delà de la couche de communication.

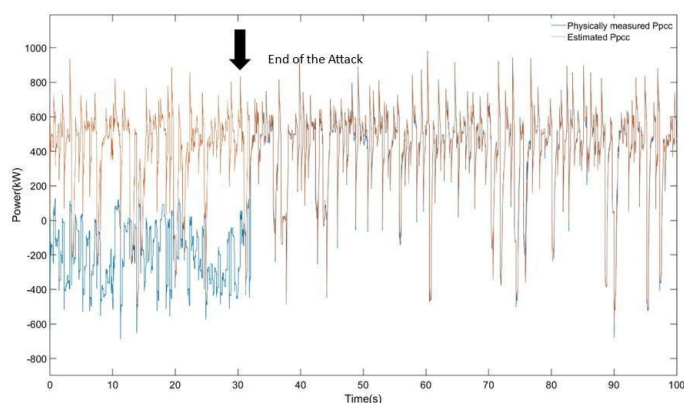


Figure VI-12: : Attaque par charge forcée de la batterie jusqu'à la 30e seconde

Dans l'ensemble, ces résultats confirment que le système de détection basé sur le LSTM peut différencier efficacement les perturbations transitoires et les incohérences persistantes indiquant des cyberattaques physiques. Sa capacité à détecter à la fois les fausses données d'origine cybernétique et les anomalies opérationnelles d'origine physique en fait un outil robuste pour améliorer la sécurité des micro-réseaux.

Cette capacité est particulièrement pertinente lorsqu'on envisage l'intégration d'infrastructures plus complexes, telles que les systèmes de cogénération à hydrogène, où l'interaction entre la surveillance numérique et la sécurité physique devient encore plus critique. La robustesse démontrée de l'approche LSTM fournit une base solide pour étendre des stratégies de détection similaires afin de protéger les futurs réseaux énergétiques couplés entre différents secteurs.

Analyse comparative des politiques et pratiques en matière de comptage intelligent dans le Rhin supérieur

Au-delà de la validation opérationnelle du démonstrateur de micro-réseau et de l'analyse de sécurité basée sur l'IA, le projet a exploré le paysage plus large de la numérisation des

systèmes énergétiques décentralisés grâce aux technologies de comptage intelligent. Une étude comparative de l'état actuel des infrastructures de comptage intelligent dans les pays du Rhin supérieur a été menée.

La région du Rhin supérieur, qui englobe certaines parties de la France, de l'Allemagne et de la Suisse, offre un contexte unique car elle implique différents cadres réglementaires nationaux au sein d'un marché énergétique géographiquement interconnecté. Plusieurs initiatives transfrontalières ont été lancées afin d'harmoniser les politiques et les pratiques énergétiques. Le programme Interreg VI-A France-Allemagne-Suisse (2021-2027) vise à développer des systèmes énergétiques intelligents, notamment des réseaux intelligents et des systèmes TIC, afin de faciliter la transition énergétique et la durabilité écologique dans la région (Commission européenne, 2021).

Un autre projet notable est l'initiative « Smart Border » entre la France et l'Allemagne, qui se concentre sur l'intégration des technologies de réseaux intelligents afin d'améliorer l'efficacité énergétique et le couplage sectoriel dans les régions de la Sarre (DE) et de la Lorraine (FR). Cette initiative vise à fournir des solutions rentables pour renforcer la sécurité et encourager les investissements dans les énergies renouvelables (Commission européenne, 2019).

Malgré ces efforts de collaboration, des divergences persistent entre les intentions politiques et la mise en œuvre pratique. Par exemple, alors que la France a réalisé des progrès significatifs dans le déploiement des compteurs intelligents grâce à son programme Linky, le déploiement en Allemagne a pris du retard en raison de difficultés juridiques et bureaucratiques, avec un taux de pénétration de seulement 14 % selon les dernières évaluations (De Paola et al, 2023). La Suisse, en revanche, a l'obligation légale d'atteindre une couverture de 80 % en compteurs intelligents d'ici 2027, mais n'avait atteint que 20 % selon les dernières données, ce qui indique un écart important entre les objectifs politiques et les progrès réels (Brightly Energy, 2024).

Les partenariats public-privé (PPP) ont joué un rôle crucial dans l'amélioration de la sécurité des réseaux intelligents dans la région. En France, le déploiement des compteurs de gaz intelligents Gazpar par GRDF a utilisé la technologie Wize, un protocole de réseau étendu à faible consommation d'énergie développé grâce à la collaboration entre des services publics et des entreprises privées telles que Suez et Sagemcom. Ce partenariat a facilité l'intégration de technologies de communication sécurisées et efficaces dans l'infrastructure nationale de comptage du gaz (Wize Alliance, n.d.).

De même, l'initiative Smart Border illustre les PPP transfrontaliers, avec la collaboration entre Enedis (FR) et Energis-Netzgesellschaft mbH (DE) pour mettre en œuvre un réseau intelligent qui intègre la flexibilité liée à la mobilité intelligente et à l'efficacité énergétique, renforçant ainsi la sécurité et encourageant les investissements dans les énergies renouvelables (Commission européenne, 2019).

En résumé, les implications pratiques pour les projets transfrontaliers sont importantes. Les systèmes français sont techniquement prêts pour des services rapides basés sur les données, mais sont confrontés à des défis potentiels d'interopérabilité avec les compteurs allemands et suisses en raison de formats de données et de protocoles de sécurité différents. Les systèmes allemands donnent la priorité à la cybersécurité et à la confidentialité, mais retardent la pleine réalisation des marchés de flexibilité numérique. Les déploiements suisses mettent l'accent sur l'intégration multi-énergies, mais restent fragmentés par la gouvernance au niveau cantonal.

Pour les initiatives transnationales telles que CO2InnO, il est essentiel d'harmoniser les normes en matière de données et les exigences d'interopérabilité. Sans protocole commun d'échange de données et sans systèmes de certification de sécurité compatibles, l'intégration des données des compteurs intelligents dans les micro-réseaux régionaux devient fastidieuse. Cette hétérogénéité pourrait entraver la création de programmes transfrontaliers de réponse à la demande ou retarder l'adoption d'outils régionaux d'optimisation énergétique basés sur l'IA.

Cybersécurité et numérisation dans les systèmes de cogénération à hydrogène

À la suite de l'analyse comparative des politiques et pratiques en matière de comptage intelligent dans la région du Rhin supérieur, il apparaît clairement que l'évolution future des réseaux intelligents ne peut se limiter au seul comptage de l'électricité. L'intégration d'unités de cogénération à hydrogène représente une étape cruciale dans la promotion du couplage sectoriel et le renforcement de la résilience des systèmes énergétiques distribués. Dans le cadre du projet CO2InnO, ces unités sont envisagées comme des atouts stratégiques qui complètent la production intermittente d'énergie renouvelable tout en favorisant des flux d'énergie flexibles et bidirectionnels. Cependant, leur déploiement introduit des niveaux de complexité supplémentaires, notamment en termes de sécurité cyber-physique, car ces

VI.3.9. Les systèmes reposent sur des infrastructures de surveillance et de communication numériques étendues.

Implications de l'intégration des compteurs intelligents en matière de sécurité cyber-physique

Les unités de cogénération à hydrogène dépendent de plus en plus des plateformes de détection basées sur l'IoT pour fournir une visibilité en temps réel sur les indicateurs de performance, les débits d'hydrogène, les niveaux de pression et les émissions. La technologie LoRaWAN (Long Range Wide Area Network) s'est imposée comme une solution rentable et économe en énergie pour connecter ces actifs distribués à des plateformes de gestion centrales. Les passerelles LoRa déployées au niveau des unités peuvent transmettre des données télémétriques, permettant aux opérateurs d'optimiser les performances et de garantir

la conformité aux normes de sécurité. Cependant, si LoRa offre de solides avantages en termes de portée et de faible consommation d'énergie, elle présente également des limites inhérentes en matière de sécurité par rapport aux alternatives filaires ou cellulaires. La gestion statique des clés, les capacités de cryptage limitées et la vulnérabilité aux attaques par rejeu ou brouillage créent des points d'entrée potentiels pour les acteurs malveillants. À mesure que la pénétration des unités de cogénération à hydrogène se développe, la robustesse de la sécurité des communications IoT deviendra un élément essentiel pour garantir à la fois l'intégrité opérationnelle et la sécurité.

Ces risques ne sont pas théoriques. Les cyberattaques contre les systèmes de cogénération à hydrogène peuvent rapidement dégénérer, passant de violations numériques à des incidents physiques graves. Par exemple, une attaque visant à usurper un capteur de concentration de gaz pourrait masquer une accumulation dangereuse d'hydrogène, en particulier si les systèmes de ventilation ou de sécurité sont simultanément compromis. Dans de tels cas, des fuites non détectées pourraient entraîner des explosions aux conséquences dévastatrices pour la sécurité humaine, l'environnement et les infrastructures environnantes. De même, les attaques par déni de service contre les PLC ou les systèmes SCADA peuvent interrompre la production d'électricité et de chaleur, menaçant ainsi des installations critiques telles que les hôpitaux ou les sites industriels où une alimentation électrique ininterrompue est essentielle. Des manipulations plus subtiles, telles que la modification des boucles de contrôle de pression ou la compromission des mises à jour du micrologiciel par des attaques de la chaîne d'approvisionnement, peuvent entraîner des défaillances mécaniques ou une dégradation à long terme de la fiabilité du système.

Plusieurs scénarios illustratifs soulignent ces risques. Une attaque coordonnée contre le fonctionnement des piles à combustible, par exemple, pourrait induire les opérateurs en erreur en affichant de fausses valeurs normales tandis qu'un processus de surchauffe caché déclenche un emballement thermique. Dans un autre cas, une attaque de type « man-in-the-middle » contre des unités de cogénération intégrées au réseau pourrait manipuler les signaux de réponse à la demande, déstabilisant à la fois l' locale et l'équilibre énergétique régional. La désactivation de la logique d'arrêt d'urgence pendant la maintenance pourrait permettre à une fuite d'hydrogène de se transformer en explosion, tandis que des compromissions en amont de la chaîne d'approvisionnement pourraient introduire des bombes logiques déclenchées par le temps qui perturberaient progressivement le fonctionnement des vannes.

Bien que ces exemples soient hypothétiques, ils correspondent aux vulnérabilités connues des systèmes énergétiques industriels et soulignent le besoin urgent de mesures de cybersécurité intégrées dans la conception, le déploiement et l'exploitation des unités de cogénération à hydrogène. À mesure que les réseaux intelligents évoluent pour intégrer ces nouveaux actifs, l'interaction entre la connectivité numérique et la sécurité physique doit être gérée avec soin.

Ces conclusions renforcent la nécessité de stratégies de sécurité à plusieurs niveaux, de décisions architecturales fondées sur les risques et de cadres réglementaires solides pour protéger l'économie future de l'hydrogène.

Scénario illustratif d'attaque cyber-physique dans les systèmes de cogénération à hydrogène

Afin d'examiner les vulnérabilités potentielles des futurs systèmes énergétiques à hydrogène, un scénario illustratif a été développé impliquant une centrale de cogénération de taille moyenne de 500 kW à 5 MW comprenant un électrolyseur, des réservoirs de stockage, une turbine et une intégration SCADA. Le scénario montre comment une cyberintrusion coordonnée pourrait exploiter les vulnérabilités du système de contrôle pour déclencher des conditions de fonctionnement dangereuses, et comment une surveillance assistée par l'IA intégrée à un jumeau numérique pourrait atténuer ces risques.

Dans ce scénario, les attaquants ont obtenu un accès non autorisé au réseau de la centrale via des identifiants de maintenance à distance compromis. Une fois à l'intérieur de l'environnement technologique opérationnel, ils ont exploité la faiblesse des politiques de contrôle d'accès pour augmenter leurs privilèges et obtenir un accès en écriture à des variables de processus critiques. Leur première action a consisté à manipuler le canal de communication Modbus/TCP reliant les contrôleurs logiques programmables (PLC) de la centrale à l'interface SCADA. En envoyant des paquets spécialement conçus, ils ont émis des commandes malveillantes qui ont désactivé les capteurs de sécurité critiques surveillant la pression et la température de stockage de l'hydrogène. Simultanément, ils ont injecté de fausses lectures « normales » dans l'interface homme-machine (IHM) SCADA, dissimulant ainsi le fait que la pression réelle du réservoir de stockage dépassait progressivement les seuils de sécurité en raison de la surcharge intentionnelle de l'électrolyseur.

D'un point de vue opérationnel, les opérateurs de l'usine n'ont constaté aucune anomalie, car le tableau de bord SCADA continuait d'afficher des valeurs nominales. Cependant, en réalité, les réservoirs de stockage étaient remplis au-delà de leur pression nominale, créant un risque latent de rupture catastrophique. Une telle attaque, si elle n'était pas détectée, pouvait entraîner des fuites d'hydrogène, des risques d'incendie et des dommages potentiellement graves pour les personnes et les infrastructures.

Le cadre de cybersécurité envisagé dans le projet intègre une couche de surveillance basée sur l'IA étroitement couplée à un jumeau numérique du système de cogénération. Le moteur de détection des anomalies basé sur l'IA analyse plusieurs flux de données, notamment le trafic réseau, les journaux d'authentification des utilisateurs et les séries chronologiques des variables de processus. Dans ce cas, le système reconnaîtrait des schémas de connexion irréguliers, tels que une connexion à distance se produisant en dehors des fenêtres de maintenance habituelles, combinée à des séquences de commandes inhabituelles ciblant des

registres critiques pour la sécurité. Ces cyberindicateurs déclencheraient déjà une alerte de sécurité de faible niveau.

En parallèle, le jumeau numérique physique du système de cogénération prédit en permanence les trajectoires attendues du processus dans des conditions normales. Par exemple, compte tenu du profil de charge de l'électrolyseur et des conditions ambiantes, le jumeau numérique calcule les taux attendus de production d'hydrogène et l'évolution correspondante de la pression du réservoir de stockage. Dans le scénario d'attaque, les lectures réelles des capteurs, désormais manipulées, s'écarteraient considérablement des valeurs prévues par le modèle. Cette incohérence entre la prévision du jumeau et les données rapportées par le SCADA déclencherait un signal d'anomalie de niveau supérieur.

Dès la détection de l'anomalie, une réponse automatisée isolerait le segment de réseau affecté en révoquant les identifiants compromis des utilisateurs et en bloquant les connexions externes. Le système reviendrait également à des capteurs de secours redondants directement connectés à un PLC de sécurité isolé. Si les données de secours confirmaient une pression anormale dans le réservoir, la logique de contrôle lancerait un arrêt contrôlé de l'électrolyseur afin d'éviter toute surpression supplémentaire. Dans les cas extrêmes, des soupapes de sécurité mécaniques pourraient être activées indépendamment des commandes logicielles. (La figure illustre le processus de détection et d'atténuation des attaques par couches, combinant l'analyse du réseau, la détection des anomalies par l'IA et la validation par jumeau numérique).

Ce scénario illustre comment la détection avancée des anomalies basée sur l'IA, combinée à la validation des jumeaux numériques basée sur la physique, pourrait améliorer la cybersécurité des centrales de cogénération à hydrogène. Il souligne l'importance d'intégrer des mesures de résilience cyber-physique dans les infrastructures énergétiques critiques

VI.3.12 avant que ces actifs ne se généralisent.

Discussion

Les résultats combinés de la validation du micro-réseau hybride de Mulhouse, des expériences de détection basées sur le LSTM, de l'analyse comparative des compteurs intelligents et du scénario illustratif de cybersécurité des centrales de cogénération à hydrogène brossent un tableau multiforme du paysage énergétique en pleine évolution.

La simulation de micro-réseau en conditions réelles a démontré que les systèmes énergétiques hybrides décentralisés peuvent intégrer de manière fiable la production d'énergie renouvelable et fournir des services de réseau local même en cas de perturbations. En donnant la priorité à l'énergie solaire produite localement, en équilibrant dynamiquement le stockage des batteries et en interagissant de manière transparente avec le réseau principal lorsque cela est nécessaire, le système a prouvé sa capacité à maintenir la continuité opérationnelle. Cependant, cette validation a également souligné que la numérisation accrue,

nécessaire à la gestion intelligente de l'énergie et au fonctionnement à distance, élargit inévitablement la surface d'attaque potentielle de ces infrastructures.

Sur la base de ces informations, le système de détection basé sur le LSTM a été évalué comme une couche de sécurité cyber-physique avancée pour les opérations des micro-réseaux. Les résultats ont montré que le modèle d'apprentissage profond identifiait efficacement les anomalies cybernétiques et physiques, y compris l'injection de fausses données, la relecture de profils de mesure et la charge forcée des batteries, même dans des conditions complexes de gestion des batteries. Des architectures réseau plus profondes, entraînées sur des ensembles de données étendus, ont permis de saisir plus précisément les dépendances à long terme dans la dynamique du système, minimisant ainsi les fausses alarmes tout en améliorant la sensibilité aux modèles d'attaque subtils. Ces résultats soulignent le potentiel de la détection des anomalies par l'IA pour renforcer la résilience des micro-réseaux face à l'évolution des menaces.

À une échelle régionale plus large, l'analyse comparative des politiques de comptage intelligent dans la région du Rhin supérieur a révélé à la fois les opportunités et les défis liés à la mise à l'échelle de ces systèmes intelligents. La France fait preuve d'une grande capacité de déploiement rapide, l'Allemagne donne la priorité à des normes de sécurité strictes et la Suisse se concentre sur l'intégration intersectorielle. Cependant, cette diversité crée également une fragmentation réglementaire et technique qui pourrait entraver le fonctionnement harmonieux des micro-réseaux transnationaux. L'harmonisation des infrastructures numériques, des protocoles de sécurité et de la gouvernance des données est donc essentielle, non seulement pour le comptage de l'électricité, mais aussi pour l'intégration d'actifs plus complexes tels que les systèmes de cogénération à hydrogène, qui reposent sur une surveillance étendue via l'IoT et une communication bidirectionnelle.

Enfin, le scénario de cybersécurité de la cogénération à hydrogène illustre comment ces vulnérabilités pourraient se manifester dans les futures infrastructures couplées entre secteurs. Les attaques contre les unités de cogénération à hydrogène, allant de la falsification des données des capteurs à la manipulation des signaux de réponse à la demande, pourraient passer de simples violations numériques à des incidents physiques graves. Cela souligne la nécessité de stratégies de sécurité à plusieurs niveaux combinant une conception robuste des systèmes, des mécanismes de détection avancés tels que les modèles basés sur LSTM et des cadres réglementaires coordonnés. Pour atténuer ces risques, il faut considérer la sécurité cyber-physique non pas comme un ajout isolé, mais comme une composante intégrante de la conception, du déploiement et de l'exploitation des systèmes énergétiques distribués de nouvelle génération.

En fin de compte, la mise en place de réseaux énergétiques résilients, sobres en carbone et intelligents exige une approche équilibrée. La robustesse physique doit être complétée par

une résilience cyber-physique, une surveillance basée sur l'IA et des infrastructures numériques harmonisées. Ce n'est qu'en abordant ces dimensions ensemble que les futurs systèmes énergétiques pourront fournir des services fiables, durables et sûrs aux communautés locales et aux régions transnationales.

VI.4. Problèmes et risques

Tout au long de la mise en œuvre du projet, plusieurs défis techniques et contextuels sont apparus, notamment en ce qui concerne l'intégration des systèmes de cogénération à hydrogène et leur numérisation. Si bon nombre de ces risques étaient dans une certaine mesure prévisibles, leurs implications pratiques ont nécessité des stratégies adaptatives afin de garantir la continuité et la pertinence de la recherche.

L'un des défis les plus importants concerne la nature intrinsèque de l'hydrogène en tant que vecteur énergétique. L'hydrogène est très réactif et présente des contraintes de sécurité uniques, en particulier dans les applications à petite et moyenne échelle situées dans des environnements urbains ou semi-urbains. Les conditions de stockage, la gestion de la pression et l'interaction de l'hydrogène avec d'autres éléments à l'intérieur des chambres de combustion exigent un contrôle précis. Même des écarts mineurs de température, de pression ou de débit peuvent compromettre la stabilité du système ou présenter des risques pour la sécurité. Dans les zones urbaines confinées, où la proximité des infrastructures et la densité de population augmentent les enjeux de toute défaillance technique, ces risques sont amplifiés.

Ces contraintes de sécurité ont eu un impact direct sur la portée des tests de sécurité cyber-physique. Alors qu'il était initialement prévu que les unités de cogénération à hydrogène puissent servir de bancs d'essai pour des expériences de sécurité intégrée, la réalisation de tels tests dans des environnements contenant des gaz combustibles s'est avérée impossible. Le risque de fuites accidentelles d'hydrogène, de surpressurisation ou d'inflammation SIGnifiait que la simulation intentionnelle d'attaques cyber-physiques ne pouvait pas être réalisée dans des conditions de fonctionnement réalistes. L'absence d'un environnement de test suffisamment contrôlé et isolé limitait encore davantage la capacité à exposer ces systèmes à des scénarios de stress cyber-physique délibérés.

Outre les obstacles liés à la sécurité, une limitation critique est apparue en raison de l'état actuel de l'infrastructure de comptage intelligent. Les compteurs intelligents déployés dans la région du projet sont principalement conçus pour les paramètres électriques, tels que la tension, le courant et les flux d'énergie active/réactive. Cependant, le fonctionnement des unités de cogénération à hydrogène dépend également de données non électriques, notamment la température, la pression et les débits d'hydrogène. Sans la possibilité de collecter et d'intégrer nativement ces données dans les plateformes de comptage intelligent existantes, il était impossible de réaliser la représentation numérique complète envisagée des

unités de cogénération. Cette lacune a entravé à la fois la capacité d'effectuer une surveillance cyber-physique en temps réel et la génération d'ensembles de données complets nécessaires aux modèles de détection d'anomalies basés sur l'IA.

De plus, une collaboration prévue avec l'organisation partenaire HKA pour l'analyse de la sécurité cyber-physique de leur unité de cogénération à hydrogène s'est heurtée à des contraintes inattendues. Le banc d'essai entretenu par HKA était principalement conçu pour la recherche sur l'efficacité énergétique et la gestion thermique. Il ne disposait pas du matériel et des couches de communication nécessaires à l'intégration des compteurs intelligents et aux tests de cybersécurité externes. La modernisation de cette infrastructure aurait nécessité des modifications importantes, tant pour la certification de sécurité que pour la compatibilité avec les systèmes de surveillance numériques externes, ce qui dépassait le temps et les ressources disponibles pour le projet.

Cette situation a révélé une dualité intéressante dans la connectivité des systèmes de cogénération à hydrogène. D'une part, l'absence d'intégration avec les compteurs intelligents et les réseaux de communication à distance entrave l'optimisation énergétique et la gestion dynamique. Par exemple, lorsque les unités de cogénération fonctionnent en parallèle avec des sources d'énergie renouvelables variables, l'absence de données détaillées sur la consommation et la production réduit la capacité du système à allouer efficacement les ressources, à anticiper les pénuries d'énergie ou à planifier la maintenance prédictive. Cette déconnexion limite la continuité opérationnelle et compromet le potentiel d'optimisation basée sur l'IA, qui repose sur des données multidomaines à haute résolution.

D'autre part, ce même manque de connectivité a fourni une couche de protection fortuite. Comme ces unités de cogénération ne sont pas exposées en permanence aux réseaux numériques externes, elles sont intrinsèquement moins vulnérables aux cyberattaques à distance, à l'espionnage ou à la manipulation du système. Cet isolement peut être considéré comme une protection à court terme, particulièrement pertinente dans les infrastructures critiques telles que les hôpitaux, les micro-réseaux industriels ou les services municipaux où la cogénération à hydrogène joue un rôle dans l'amélioration de la résilience. Cependant, cet effet protecteur n'est que temporaire. À mesure que les systèmes énergétiques évoluent vers un couplage sectoriel plus profond, les exigences réglementaires nécessiteront une intégration numérique complète des systèmes à hydrogène, y compris la surveillance des flux de gaz, des émissions et des échanges thermiques. À ce stade, la surface d'exposition au risque s'étendra inévitablement.

Afin d'atténuer ces défis techniques et numériques étroitement liés, le projet a adapté son approche. Plutôt que de mener des simulations expérimentales à grande échelle d'attaques cyber-physiques sur des unités de cogénération à hydrogène opérationnelles, un scénario d'attaque hypothétique mais techniquement fondé a été envisagé. Cela a permis une analyse

conceptuelle des stratégies de détection et d'atténuation sans compromettre la sécurité physique.

Malgré ces adaptations, certaines limites n'ont pas pu être entièrement surmontées dans le cadre du projet actuel. Par exemple, l'absence de comptage intelligent intégré pour les paramètres spécifiques à l'hydrogène n'a pas pu être résolue sans repenser les infrastructures de comptage existantes au niveau réglementaire. De même, l'impossibilité de réaliser des tests de résistance cyber-physiques en conditions réelles signifie que certains aspects de la résilience, en particulier ceux impliquant des défaillances en cascade couplées, restent théoriques plutôt que validés empiriquement.

Néanmoins, ces défis ont permis d'obtenir des informations précieuses. Ils ont souligné l'importance de concevoir dès le départ des unités de cogénération à hydrogène en tenant compte des considérations de cybersécurité, afin de garantir à la fois un fonctionnement sûr et une numérisation sécurisée. Ils ont également mis en évidence le besoin urgent de cadres de comptage intelligent interopérables capables de capturer des données énergétiques multivectorielles, notamment les flux d'hydrogène, les variables thermiques et les mesures d'émissions. Ces conclusions serviront de base à la stratégie de transition pour une intégration sécurisée de la cogénération dans les phases de recherche futures, en équilibrant les impératifs d'optimisation, de sécurité et de résilience.

VI.5. Écarts

Peu d'écarts par rapport au plan initial du projet ont été constatés, principalement en raison des contraintes techniques et infrastructurelles liées aux systèmes de cogénération à hydrogène. Si ces changements ont nécessité des ajustements dans l'exécution de certaines activités, ils n'ont pas compromis fondamentalement les objectifs généraux du projet. Au contraire, ils ont remodelé certains sous-objectifs et réorienté la recherche vers des résultats plus conceptuels et stratégiques.

Le premier écart concernait l'analyse expérimentale prévue de la sécurité cyber-physique d'une unité de cogénération à hydrogène en collaboration avec HKA. Au départ, cette configuration devait fournir un banc d'essai en direct pour simuler des intrusions dans le réseau, des falsifications de capteurs et des attaques de manipulation de processus dans des conditions contrôlées. Cependant, après une évaluation technique détaillée, il est apparu clairement que le banc d'essai n'était pas conçu pour être intégré à des dispositifs de comptage intelligents externes ou à des systèmes de surveillance à distance. De plus, l'absence d'environnements certifiés en matière de sécurité rendait impossible l'induction délibérée de conditions de fonctionnement anormales de l'hydrogène sans risque significatif.

Pour pallier cette limitation, le projet s'est orienté vers une étude de cas théorique d'attaque. Au lieu d'expériences en direct, l'équipe a développé un scénario basé sur un jumeau

numérique d'une intrusion hypothétique ciblant un système de stockage d'hydrogène. Cela a permis d'explorer en détail les voies d'attaque potentielles, les stratégies de détection basées sur l'IA et les réponses d'atténuation à plusieurs niveaux sans mettre en danger les actifs physiques ou le personnel. Bien que cette approche n'ait pas la richesse empirique des tests en direct, elle a néanmoins fourni des informations précieuses sur le paysage des risques cyber-physiques et a permis de formuler des recommandations éclairées pour les besoins futurs en matière d'infrastructures de recherche.

En ce qui concerne l'intégration avancée de l'IA, la mise en œuvre de modèles LSTM dans l'environnement Simulink a présenté une complexité supplémentaire. Bien que les LSTM soient très efficaces pour l'analyse de données chronologiques, leur déploiement dans des environnements en temps réel n'est pas encore simple. La prise en charge par MATLAB de l'inférence LSTM repose sur un bloc de prédiction avec état utilisant des formats de fichiers .mat, qui ne sont pas compatibles avec les workflows de génération de code. Cette limitation technique empêche la compilation du modèle en code C exécutable pour un déploiement sur des simulateurs en temps réel ou des systèmes embarqués. Bien qu'il existe diverses alternatives, telles que des implémentations basées sur Python, leur intégration dans RT-Lab ou des microcontrôleurs embarqués nécessiterait un développement et une adaptation supplémentaires, qui dépassaient le cadre de ce projet. Par conséquent, les tests HIL du modèle LSTM n'ont pas été réalisés. Le travail s'est plutôt concentré sur la démonstration des performances du LSTM dans le cadre de tests hors ligne et d'une comparaison avec le modèle NARX.

Une autre déviation est due aux limites de l'infrastructure actuelle de comptage intelligent. Le plan initial prévoyait un ensemble de données complet combinant des variables électriques et non électriques, notamment les flux d'hydrogène, les niveaux de pression et les données thermiques, provenant d'unités de cogénération intégrées. Cependant, étant donné que les compteurs intelligents disponibles étaient optimisés uniquement pour les paramètres électriques, le projet n'a pas pu réaliser une acquisition de données à spectre complet.

L'impact de cet écart a été atténué par le passage à une évaluation conceptuelle des avantages des stratégies avancées de surveillance et de contrôle. Bien que cette approche ait introduit un certain niveau d'abstraction, elle a mis en évidence les lacunes structurelles de la politique et de la technologie actuelles en matière de comptage intelligent, renforçant ainsi l'analyse comparative des pratiques régionales dans la région du Rhin supérieur.

Enfin, la dualité de la connectivité limitée dans les systèmes de cogénération à hydrogène a introduit un changement conceptuel dans le récit du projet. À l'origine, on supposait que l'intégration numérique complète était sans équivoque bénéfique pour l' . Cependant, au cours du projet, il est apparu clairement que l'isolement partiel offre actuellement un avantage temporaire en matière de cyber-résilience. Cette compréhension nuancée a enrichi les

recommandations finales, soulignant la nécessité d'une transition progressive et sécurisée vers une numérisation complète plutôt que d'une connectivité totale immédiate.

Dans l'ensemble, ces écarts ont réorienté certaines activités de recherche, mais ont finalement renforcé la pertinence stratégique du projet. Ils ont révélé des lacunes technologiques et politiques critiques qui doivent être comblées avant que les systèmes de cogénération à hydrogène puissent être intégrés de manière sûre et sécurisée dans les micro-réseaux numérisés. Si certains sous-objectifs ont été reformulés, l'objectif général du projet, qui consiste à promouvoir des systèmes énergétiques résilients, durables et intelligents, est resté inchangé.

VI.6. Perspectives

Les travaux menés dans le cadre de ce projet ont jeté des bases conceptuelles et méthodologiques solides pour la sécurité cyber-physique des systèmes de micro-réseaux hybrides, en particulier ceux qui intègrent des unités de cogénération à hydrogène. Dans le même temps, ils ont révélé plusieurs pistes où des recherches et des développements technologiques supplémentaires seront nécessaires pour combler les lacunes restantes et réaliser le plein potentiel de systèmes énergétiques sécurisés, intégrés numériquement et résilients. Les perspectives pour les travaux futurs sont donc à la fois techniques et stratégiques, nécessitant des avancées coordonnées dans les domaines des infrastructures de surveillance, des environnements de test cyber-physiques, de l'intelligence artificielle pour la détection des anomalies et des cadres politiques qui soutiennent l'intégration sécurisée des systèmes énergétiques à hydrogène dans des architectures de réseaux intelligents plus larges.

L'un des principaux domaines de recherche prospective concerne l'amélioration des capacités de comptage intelligent pour les systèmes énergétiques multivecteurs. Les infrastructures de comptage intelligent existantes sont principalement conçues pour les paramètres électriques, tels que la tension, le courant et le facteur de puissance, et offrent peu d'informations sur les aspects non électriques qui sont essentiels au fonctionnement sûr et efficace des unités de cogénération à hydrogène. Les développements futurs doivent donc se concentrer sur des technologies de comptage capables de capturer simultanément la puissance thermique, les débits d'hydrogène, les niveaux de pression et les conditions de la chambre de combustion, tout en restant compatibles avec les normes existantes d'échange de données du réseau. Cette approche de détection multidomaine constituera la base d'une surveillance en temps réel SIgnificative et d'une détection fiable des schémas opérationnels anormaux.

L'analyse comparative des politiques en matière de comptage intelligent dans la région du Rhin supérieur indique également des orientations importantes pour l'avenir en matière de gouvernance et de normalisation. La mosaïque actuelle de réglementations et de normes

techniques régissant les compteurs intelligents et les systèmes énergétiques à hydrogène crée des obstacles à l'interopérabilité, au partage des données et à la coordination des mesures de sécurité. Les futurs travaux de recherche et d'élaboration des politiques devraient donc viser à développer des normes transfrontalières harmonisées pour le comptage multivectoriel et la certification en matière de cybersécurité. De telles normes faciliteraient non seulement l'intégration de la cogénération à hydrogène dans les micro-réseaux régionaux, mais permettraient également de coordonner les réponses aux nouvelles menaces cyberphysiques. Outre l'innovation matérielle, les protocoles de communication et les modèles de données qui sous-tendent ces compteurs de nouvelle génération devront être affinés. Des formats de données sécurisés et normalisés, capables d'intégrer les mesures de gaz, de chaleur et d'électricité dans un cadre unifié, seront essentiels pour l'interopérabilité. Cela est particulièrement important dans les régions transfrontalières comme le Rhin supérieur, où différentes juridictions peuvent appliquer des normes techniques variables. En recherchant une architecture de comptage harmonisée et robuste, les études futures pourront éliminer bon nombre des angles morts actuels qui limitent la connaissance opérationnelle des systèmes de cogénération.

Une autre piste essentielle pour les recherches futures est la création d'environnements expérimentaux contrôlés pour la recherche sur la sécurité cyber-physique impliquant l'hydrogène. À l'heure actuelle, tester les effets d'intrusions cybernétiques délibérées ou de dysfonctionnements accidentels sur des unités de cogénération à hydrogène en service présente des risques importants pour la sécurité. La haute inflammabilité de l'hydrogène, combinée à la complexité des processus thermodynamiques impliqués, signifie que même des manipulations mineures pourraient avoir des conséquences dangereuses. Cette limitation nécessite des installations dédiées à l'échelle du laboratoire, dotées de mesures de confinement de sécurité avancées. De tels environnements devraient combiner du matériel physique de cogénération avec des mécanismes redondants de surveillance, de détection de gaz, de ventilation et d'arrêt de sécurité, permettant ainsi la simulation en toute sécurité de scénarios autrement dangereux.

En complément des installations d'essai physiques, les cadres de simulation virtualisés devraient également être développés. Des outils de simulation haute fidélité capables de reproduire à la fois les processus physiques au sein d'une unité de cogénération et les couches de contrôle et de communication associées peuvent constituer une plateforme alternative pour explorer des scénarios complexes sans mettre en danger le personnel ou les infrastructures. Les approches « hardware-in-the-loop » (HIL) pourraient combler le fossé entre les environnements purement virtuels et le matériel réel, permettant aux chercheurs d'injecter des cyberattaques réalistes et de surveiller leurs effets sur les paramètres opérationnels des unités

de cogénération à hydrogène. Ces approches hybrides élargiront considérablement l'éventail des conditions expérimentales pouvant être testées en toute sécurité.

Le développement de jumeaux numériques adaptés aux systèmes de cogénération à hydrogène est étroitement lié à cela. Les jumeaux numériques s'appuient sur des flux de données précis et à haute résolution pour modéliser le comportement opérationnel et simuler les perturbations en temps réel. L'absence de données complètes provenant de capteurs dans ce projet a limité la conception et la mise en œuvre de jumeaux numériques, en particulier lorsqu'il s'agissait de représenter les processus dynamiques au sein des chambres de combustion à hydrogène. Les recherches futures devraient donner la priorité au couplage de modèles physiques plus avancés avec des données réelles plus riches, permettant aux jumeaux numériques de servir d'outils prédictifs puissants pour l'optimisation opérationnelle et les tests de cybersécurité. Des jumeaux numériques améliorés permettraient également aux chercheurs d'explorer systématiquement les interactions complexes entre les unités de cogénération à hydrogène et d'autres ressources énergétiques distribuées au sein d'un micro-réseau, y compris les effets en cascade potentiels des pannes ou des attaques.

De plus, la sécurité des canaux de communication reliant les unités de cogénération aux systèmes de gestion des micro-réseaux plus larges mérite d'être approfondie. L'intégration numérique des systèmes de cogénération devenant inévitable, la surface d'attaque augmentera, rendant indispensable le développement et la validation de protocoles de communication sécurisés et à faible consommation d'énergie. Les recherches futures devraient se concentrer sur les systèmes de cryptage et de détection d'intrusion capables de fonctionner en temps réel sans imposer une charge de calcul excessive aux contrôleurs industriels aux ressources limitées.

Un domaine d'étude connexe est la résilience des systèmes de surveillance basés sur l'IA eux-mêmes. À mesure que l'intégration numérique des unités de cogénération progresse, les modèles d'IA qui contrôlent ou surveillent ces systèmes pourraient eux-mêmes devenir la cible d'attaques hostiles. Les recherches futures devront explorer la robustesse de l'IA et la cybersécurité, en veillant à ce que les algorithmes de détection ne puissent pas être facilement trompés ou manipulés par des injections de données fausses soigneusement conçues. Cela nécessite une approche holistique qui combine le développement de l'IA avec des protocoles de communication sécurisés, des environnements d'exécution fiables et des cadres de validation rigoureux.

Une autre perspective à long terme est l'intégration progressive des unités de cogénération dans des cadres coordonnés de gestion de l'énergie. À l'heure actuelle, de nombreuses unités de cogénération fonctionnent en mode isolé ou semi-isolé, avec une connectivité numérique limitée ou inexistante. Si cette isolation a constitué un rempart temporaire contre les cybermenaces à distance, elle empêche également les unités de contribuer efficacement à

l'optimisation au niveau du système. Les travaux futurs devraient porter sur des stratégies d'intégration progressive permettant aux unités de cogénération de participer aux mécanismes de réponse à la demande, aux services d'équilibrage du réseau et aux initiatives de couplage sectoriel, tout en maintenant des limites de sécurité rigoureuses. Cela impliquera une transition progressive où des mesures de renforcement de la sécurité seront déployées en tandem avec chaque nouvelle couche de connectivité.

L'évolution des stratégies de détection et d'atténuation des cyberattaques hypothétiques sur les unités de cogénération à hydrogène représente également un domaine fertile pour les recherches futures. L'étude de cas hypothétique développée dans le cadre de ce projet, dans laquelle un attaquant manipule les SIGnaux de contrôle pour créer des conditions de pression et de température dangereuses, peut être étendue à une bibliothèque plus large de scénarios de menaces. Ces scénarios peuvent ensuite servir de base à la conception de mécanismes de réponse automatisés capables d'isoler les sous-systèmes compromis, de déclencher des arrêts contrôlés ou de reconfigurer dynamiquement les modes de fonctionnement afin de minimiser les dommages.

Le déploiement à moyen et long terme de la cogénération à hydrogène dans les systèmes énergétiques urbains augmentera inévitablement la complexité des interactions entre les ressources distribuées. À mesure que les unités de cogénération seront intégrées aux systèmes photovoltaïques, aux systèmes de stockage et aux réseaux de chauffage urbain, le risque de défaillances en cascade augmentera. Les recherches futures devraient donc se concentrer sur des modèles de systèmes multi-énergétiques qui tiennent explicitement compte des interdépendances cybernétiques et physiques. De tels modèles fourniraient des informations précieuses sur la manière dont les défaillances ou les attaques se propagent à travers les réseaux interconnectés et aideraient à identifier les nœuds critiques sur lesquels les mesures de sécurité devraient se concentrer.

Enfin, les perspectives d'avenir devraient également inclure la formation et le renforcement des capacités des opérateurs et des ingénieurs qui gèreront des systèmes de cogénération de plus en plus numérisés. Si le développement technologique est essentiel, le facteur humain reste un élément crucial pour la sécurité des opérations. Le développement de modules de formation, d'exercices basés sur la simulation et de programmes de certification pour les opérateurs permettra de garantir que la main-d'œuvre est suffisamment préparée pour reconnaître, réagir et prévenir les risques cyber-physiques émergents dans les environnements de cogénération à hydrogène.

Dans l'ensemble, les perspectives d'études supplémentaires sont multiples et englobent le développement de technologies avancées de détection et de mesure, la création de plateformes expérimentales et de simulation sécurisées, le perfectionnement des protocoles de communication et des stratégies d'intégration, ainsi que l'harmonisation des cadres

réglementaires. En abordant ces domaines de manière systématique, les recherches futures pourront réduire considérablement les incertitudes et les limites auxquelles se heurte actuellement le déploiement sécurisé des systèmes de cogénération à hydrogène, contribuant ainsi à un avenir énergétique résilient, optimisé et décarboné.

VI.7. Recommandations

Sur la base des enseignements tirés tout au long du projet, plusieurs recommandations peuvent être formulées pour orienter à la fois les prochaines étapes de la recherche et l'élaboration d'une politique et d'une feuille de route plus larges pour une intégration sécurisée des systèmes énergétiques.

Au niveau de la recherche et du développement technologique, il est recommandé de donner la priorité à une infrastructure de comptage intelligent multidomaine en tant que catalyseur fondamental de la numérisation des systèmes de cogénération à hydrogène. Sans la capacité de mesurer et d'intégrer de manière transparente les paramètres électriques, thermiques et chimiques, ni les modèles avancés de jumeaux numériques ni la détection d'anomalies basée sur l'IA ne peuvent atteindre leur plein potentiel. Les programmes publics de financement de la recherche et les partenariats industriels devraient donc soutenir le développement et le déploiement de solutions de comptage de nouvelle génération qui répondent à la fois aux exigences opérationnelles et de cybersécurité. Ces dispositifs devraient être conçus spécifiquement pour les environnements multi-énergies et être compatibles avec les infrastructures de comptage électrique existantes, tout en ajoutant des capacités permettant de capturer des paramètres non électriques essentiels à la sécurité et à l'efficacité de la cogénération à hydrogène.

Parallèlement, il est essentiel de mettre en place des installations d'essai cyber-physiques dédiées aux systèmes énergétiques à hydrogène. Ces installations devraient combiner du matériel de cogénération réel, des environnements virtuels haute fidélité et des systèmes de sécurité avancés afin de permettre des essais contrôlés de scénarios de défaillance accidentelle et malveillante. De telles infrastructures permettraient non seulement d'accélérer la recherche sur les stratégies de détection et d'atténuation, mais aussi de fournir un environnement fiable pour valider les modèles d'IA, les protocoles de communication et les solutions de surveillance intégrées avant de les déployer dans les réseaux opérationnels.

Du point de vue de la gouvernance, des cadres réglementaires harmonisés sont nécessaires pour garantir l'interopérabilité et la sécurité des systèmes énergétiques régionaux. Dans la région du Rhin supérieur, la collaboration transfrontalière devrait être renforcée afin d'harmoniser les normes techniques en matière de comptage intelligent, de certification de la cybersécurité et de confidentialité des données. L'élaboration d'un ensemble unifié de lignes directrices pour la collecte, l'échange et la protection des données garantirait un niveau de

sécurité cohérent tout en permettant des approches collaboratives en matière d'optimisation énergétique. Une action politique coordonnée faciliterait l'intégration sécurisée des unités de cogénération à hydrogène dans les micro-réseaux existants, tout en maintenant la résilience face aux menaces cyber-physiques.

En outre, l'intégration numérique des systèmes de cogénération à hydrogène devrait être poursuivie par étapes soigneusement gérées. Plutôt que de rechercher immédiatement une connectivité totale, qui exposerait les systèmes à des risques inutiles, il convient d'adopter une approche progressive. Chaque phase d'intégration accrue devrait s'accompagner de tests de sécurité rigoureux, d'une planification de la redondance et d'une formation des opérateurs. Cette stratégie par étapes permettrait d'identifier et de traiter progressivement les vulnérabilités, empêchant ainsi l'apparition de faiblesses systémiques à mesure que le réseau s'étend.

De plus, la conception et le déploiement de protocoles de communication sécurisés pour les systèmes de cogénération à hydrogène devraient être explicitement prioritaires. Les futurs efforts d'intégration augmenteront inévitablement le flux de données opérationnelles entre les unités de cogénération et les systèmes de supervision, créant ainsi de nouveaux vecteurs d'attaque s'ils ne sont pas protégés. Les efforts de recherche et les politiques devraient donc se concentrer sur la validation de systèmes de cryptage légers, de mécanismes d'authentification et de systèmes de détection d'intrusion adaptés aux environnements énergétiques industriels.

Au niveau stratégique, il est également recommandé d'intégrer les considérations de cybersécurité dans la gestion du cycle de vie de la cogénération à hydrogène, de la conception et l'approvisionnement à l'exploitation et la mise hors service. Les directives d'approvisionnement devraient privilégier les équipements et les logiciels qui répondent à des normes de sécurité rigoureuses, et les stratégies de maintenance à long terme devraient inclure des audits de sécurité périodiques, des mises à jour et des formations pour le personnel opérationnel.

Enfin, la feuille de route politique visant à faire progresser l'intégration de la cogénération à hydrogène devrait explicitement relier les objectifs de sécurité cyberphysique et de transition énergétique. Si l'hydrogène joue un rôle crucial dans la décarbonisation des systèmes énergétiques et le renforcement de la résilience locale, son intégration numérique doit être gérée en accordant une attention égale à la sûreté et à la sécurité. L'action politique devrait donc promouvoir des consortiums de recherche multidisciplinaires réunissant des ingénieurs en énergie, des experts en cybersécurité, des régulateurs et des spécialistes en sciences sociales afin de garantir que les futurs systèmes à hydrogène soient non seulement durables, mais aussi sûrs et dignes de confiance pour toutes les parties prenantes.

Ces recommandations forment ensemble une voie cohérente pour l'avenir, reliant la recherche, le développement et l'action politique dans une stratégie unifiée pour l'intégration sûre et sécurisée des systèmes de cogénération à hydrogène. En donnant la priorité aux technologies de comptage avancées, aux infrastructures expérimentales contrôlées, à l'harmonisation des réglementations, à la numérisation progressive et aux protocoles de communication sécurisés, les parties prenantes peuvent progressivement surmonter les limites actuelles et garantir que la cogénération à hydrogène devienne un élément fiable et résilient du paysage énergétique en pleine évolution.

VI.8. Tableau de réalisation des objectifs

Objectif (résultat attendu)	Atteint ?
6.1. Rapport expliquant les différents aspects de la conception du modèle de micro-réseau, soulignant les défis à relever et fournissant des recommandations sur la manière de procéder.	Oui
6.2. Système d'analyse basé sur l'IA pour la détection précoce des cybermenaces.	Oui
6.3. Rapport sur les aspects liés à la sécurité des compteurs intelligents modernes, comparant les facteurs d'influence du marché et les tendances nationales dans l'adaptation des différentes politiques d'acquisition d'informations.	Oui