

TER SYSTEMES INDUSTRIELS

M1 FSI 2024/2025

COMPTE RENDU DE REUNION

COMPTE RENDU

(Réunion 006)

RÉSUMÉ DU DOCUMENT

La réunion numéro 6 s'est tenue le mardi 10 juin 2025 dans le cadre du TER Cybersécurité OT. Elle a principalement porté sur la critique du compte rendu précédent, la présentation des référentiels ANSSI et NIST, ainsi que des démonstrations d'attaques simulées à partir des environnements de test.

Un rappel méthodologique a été fait sur l'importance de l'amélioration continue, illustrée par le modèle de la roue de Deming, appliquée à la rédaction des comptes rendus et aux pratiques en cybersécurité. Des conseils pédagogiques ont également été donnés en vue des prochaines soutenances.

1 Propriétés du document

CLASSIFICATION DU DOCUMENT	Protégée
REFERENCE DU DOCUMENT	CR006_OT_24_25
DATE D'EMISSION DU DOCUMENT	12/06/2025
VERSION DU DOCUMENT	1
AUTEURS	DIA Mouhamadou Afiss
PROPRIETAIRE DU DOCUMENT	AGOPIAN Roland – Aix Marseille

Tableau 1 – Propriété du document

2 Historique des révisions

VERSION	DATE	AUTEUR	RESUME DES MODIFICATIONS
1	12/06/2025	DIA Mouhamadou Afiss	Version n°1

Tableau 2 - Historique des révisions

3 Diffusion

NOM	FONCTION
AGOPIAN Roland	Professeur Encadrant Pédagogique
PARNET Cyril	Chef de Projet
BERREBIHA Nasserline	Adjoint au chef de projet
YABDA Redouane	Membre de l'équipe
DIA Mouhamadou Afiss	Membre de l'équipe
DOUZI Youssef	Membre de l'équipe
KASMI Badreddine	Membre de l'équipe

Tableau 3 - Distribution

4 Approbation

NOM	FONCTION	SIGNATURE	DATE
PARNET Cyril	Chef de Projet	CP	11/06/2025
BERREBIHA Nasserline	Adjoint au chef de projet	NB	11/06/2025
YABDA Redouane	Membre de l'équipe	RY	11/06/2025
DIA Mouhamadou Afiss	Membre de l'équipe	MaD	11/06/2025
DOUZI Youssef	Membre de l'équipe	YD	11/06/2025
KASMI Badreddine	Membre de l'équipe	KB	11/06/2025

Tableau 4 - Approbation

1	Propriétés du document.....	2
2	Historique des révisions.....	3
3	Diffusion	4
4	Approbation	5
5	Présentation du document.....	7
6	Déroulement de la réunion	8
6.1	Lieu, durée et présence	8
6.2	Critiques du compte rendu précédente	8
6.3	Introduction à la roue de Deming.....	9
6.4	Présentation technique	9
6.5	Attentes pour la suite	10
6.6	Informations supplémentaires	11
7	Acronymes et définitions	12
	Table des acronymes.....	12

5 Présentation du document

Ce document constitue le compte rendu de la sixième réunion de travail du projet Cybersécurité OT, réalisée dans le cadre du Travail d'Étude et de Recherche (TER).

Il vise à formaliser les échanges, noter les remarques méthodologiques, résumer les présentations techniques, et définir les tâches à accomplir pour la prochaine échéance.

6 Déroulement de la réunion

6.1 Lieu, durée et présence

La réunion s'est déroulée le mardi 10 juin 2025, de 10h15 à 12h15, soit une durée de deux heures. Elle a eu lieu dans la salle de travail du bâtiment 7, côté A, au troisième étage, à la faculté de Saint-Charles. La salle était équipée d'un écran pour la présentation ainsi que d'un tableau pour un usage pédagogique.

Tous les membres de ce projet étaient présents à cette réunion, à l'exception de Badreddine KASMI et Youssef DOUZI, excusés.

6.2 Critique du compte rendu précédent

M. AGOPIAN a exprimé une déception sur la qualité rédactionnelle du compte rendu n°5, évoquant une régression sur la forme :

- Disparition de certaines bonnes pratiques précédemment intégrées.
- Défauts de relecture, vocabulaire imprécis, confusions entre langage oral et écrit.
- Absence de mentions claires concernant la présence ou l'absence des participants.

Il a insisté sur la nécessité de mettre en place une procédure rigoureuse de relecture et de validation, en prenant exemple sur d'autres groupes ayant déjà structuré ce processus.

6.3 Introduction à la roue de Deming

M. AGOPIAN a présenté la roue de Deming (PDCA) comme un modèle central d'amélioration continue. Il en a détaillé les quatre étapes :

- Plan : définition des objectifs et processus.
- Do : mise en œuvre.
- Check : vérification, évaluation ou audit.
- Act : correction et renforcement et prévention de la régression.

Ce modèle a été illustré à travers plusieurs domaines : rédaction documentaire, gestion des vulnérabilités (patch management), audits de cybersécurité, etc.

6.4 Présentations techniques

Chaque membre présent a réalisé une présentation ciblée :

- Cyril Parnet :
 - Démonstration d'une attaque DDoS sur Modbus via génération de requêtes massives.
 - Utilisation de Python multithreadé avec la bibliothèque PyModbus.
- Nasserline Berrebiha :
 - Injection de commande (démarrage/arrêt toutes les 3 secondes).
 - Tentative d'attaque Man-in-the-Middle (non finalisée en raison d'un problème technique).
- Redouane Yabda :
 - Présentation du référentiel NIST.
 - Utilisation de Modbus Doctor pour simuler des interactions avec les registres.
- Mouhamadou-Afiss Dia :
 - Présentation du référentiel ANSSI.
 - Simulation d'un système de contrôle-commande d'un tapis roulant

6.5 Attentes pour la suite

Les travaux attendus pour la suite incluent :

- Un rapport structuré contenant :
 - Présentation de l'environnement simulé.
 - Deux à trois scénarios d'attaque documentés.
 - Des schémas explicatifs (trames Modbus, modèle Purdue, etc.).
 - Une analyse des vulnérabilités et des mesures de contrôle associées (références techniques).
 - Une explication des protocoles industriels utilisés.
- Une présentation orale à préparer avec soin :
 - Langage professionnel exigé.
 - Démonstrations techniques valorisées.
 - Discours structuré, précis et synthétique

6.6 Informations supplémentaires

- Les soutenances finales sont prévues pour le mercredi 25 juin 2025.
- Les consignes définitives (durée, ordre de passage, modalités techniques) seront transmises par Mme Bertolissi, responsable de l'organisation de cette session.
- Une répétition générale est maintenue le lundi 23 juin 2025 à 13h30, en présence du groupe Hacking Éthique.
- Une session intermédiaire a également été organisée le lundi 16 juin 2025 à 13h30, afin de faire un point sur l'état d'avancement des présentations et des démonstrations.

7 Acronymes et définitions

Table des acronymes

ACRONYME	SIGNIFICATION
PDCA	Plan-do-check-act
NIST	National Institute of Standards and Technology
ANSSI	Agence Nationale de la Sécurité des Systèmes D'Informations

Table 5 – Table des acronymes