

CYBERSÉCURITÉ ET SÛRETÉ DE FONCTIONNEMENT DANS LES SYSTÈMES INDUSTRIELS COHABITATION, ARTICULATION OU ANTAGONISME ?

5 NOVEMBRE 2019, ESTP CACHAN

Journée IMdR organisée par le groupe de
travail et de réflexion (GTR)
« Cybersécurité des installations
industrielles et IIoT »



DIRECTION GÉNÉRALE INDUSTRIELLE ET INGÉNIERIE



TRANSFORMATION
TECHNOLOGIE
& DIGITAL



VISION GÉRANT DE L'INFRASTRUCTURE TRANSPORT TERRESTRE

RETOUR D'EXPÉRIENCE SNCF RÉSEAU





Yseult GARNIER

Responsable CyberSécurité Industriel (RCS-I)

**SNCF RESEAU - DIRECTION GENERALE INDUSTRIELLE ET
INGENIERIE**

Département Transformation Technologie et Digital

12 rue Camille MOKE 93212 Saint Denis

MOBILE : +33 (0)6 15 62 20 22

MAIL : yseult.garnier@reseau.sncf.fr

AGENDA

1. HISTORIQUE DES 2 DÉMARCHES SÉCURITÉ ET CYBERSÉCURITÉ
2. LIEN ENTRE CES 2 DÉMARCHES
3. CONCLUSION
4. QUESTIONS

1. HISTORIQUE

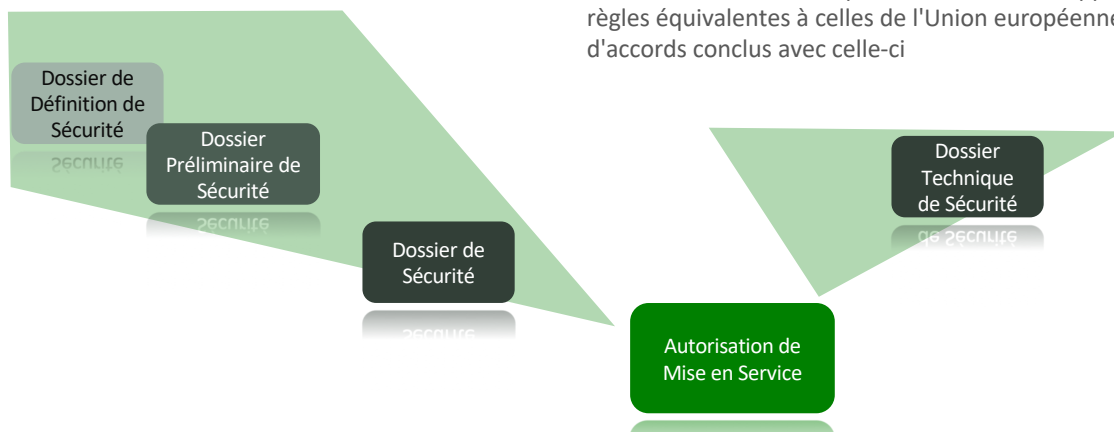
HISTORIQUE

AVANT 2014 :

1 seule démarche pour les systèmes de sécurité ferroviaire: principe de la démarche sécurité, imposée par la réglementation

SI le projet nécessite une autorisation de mise en service

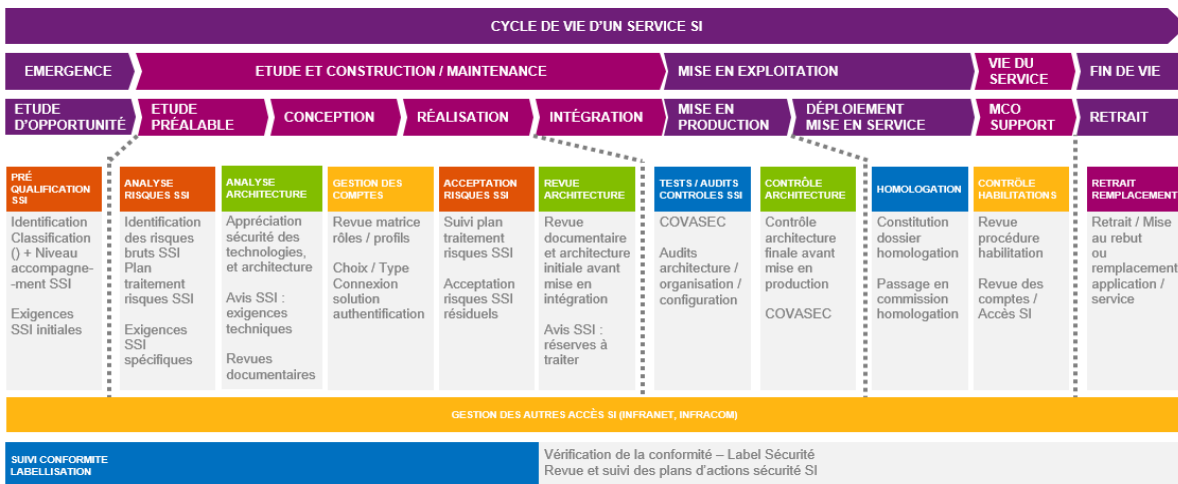
SI le projet est déjà autorisé sur un réseau d'un autre Etat membre de l'Union européenne ou d'un Etat appliquant des règles équivalentes à celles de l'Union européenne en vertu d'accords conclus avec celle-ci



HISTORIQUE

APRES 2014

Début 2014 : Mise en place d'un Responsable Cybersécurité Industriel à SNCF Réseau au sein des métiers
 → Mise en œuvre d'une démarche d'intégration de la cybersécurité pour tous les projets industriels



02. LIEN ENTRE CES 2 DÉMARCHES



02. LIEN ENTRE CES 2 DÉMARCHES

OBJECTIFS

Constat :

Pour les systèmes de sécurité ferroviaire, le risque cybersécurité a une part de plus en plus importante
Démarche sécurité ferroviaire bien intégrée dans les processus métiers et organisationnels
Démarche cybersécurité récente, et en cours d'intégration dans les processus métiers et organisationnels

Objectifs :

- Prendre en compte le risque cybersécurité dans la démarche de sécurité ferroviaire, en adaptant par rapport aux enjeux
- Fluidifier les 2 démarches afin que cette mise en place soit quasi transparente pour les projets



02. LIEN ENTRE CES 2 DÉMARCHES

COMMENT ?

- **Maintenir ces 2 démarches indépendantes**
 - Équipe sécurité ferroviaire et cybersécurité indépendante
 - Signataire différent pour les 2 livrables issus des démarches
- **Sensibiliser tous les acteurs des projets à la démarche cybersécurité**
 - Mise en place et animation de relais cybersécurité côté métier
 - Mise en place d'un guichet unique afin de fluidifier la prise en charge de la cybersécurité pour tous les nouveaux projets



02. LIEN ENTRE CES 2 DÉMARCHES

COMMENT ?

- **Identifier les jalons de rencontre entre les 2 démarches**
 - En émergence du projet, afin d'identifier les enjeux cybersécurité
 - En phase de spécification :
 - Lien entre l'analyse de risques SSI et l'analyse préliminaire de risques
 - Cohérence entre les exigences de sécurité ferroviaire et exigences de cybersécurité
 - En phase de validation : intégration des résultats des tests de cybersécurité
 - Avant l'autorisation de mise en service : cohérence et acceptation des risques résiduels issus des 2 démarches
 - Et pour chacun des jalons, identifier :
 - les documents d'entrée attendus de chacun
 - le timing par rapport au planning d'un projet
 - le livrable / avis attendu
- **Rencontre entre les 2 équipes sur un cas concret**

03. CONCLUSION

3. CONCLUSION

- Accord des 2 équipes et de la direction de maintenir ces 2 démarches indépendantes



- Accompagnement sécurité et cybersécurité de tous les projets informatiques
- industriels de sécurité ferroviaire



- Travaux en cours afin de finaliser les points de rencontre entre les 2 démarches



→ Bien s'assurer que les deux démarches sont cohérentes quant au résultat pour chacun des jalons nécessaires



MERCI.

AUTRES QUESTIONS ?

