

# Colloque réseaux de données

D RTE 28100 Démonstration de la sécurité des réseaux de données

Safety et Security – Exemples pratiques

Berne, le 11 décembre 2024

# Bienvenue

## **Direction du colloque et organisation**

Robert Leemann, CFF

Urs Walser, UTP

## **Intervenants**

Thierry Bassani, CFF

Patrick Favre, OFT

Martin Gerber, RBS

Matthias Glock, CFF

Jean-Christophe Grandchamp, CFF

Emmerich Horvath, zb

Tobias Hubschmid, OFT

Andreas Klopfenstein, BLS

Kurt Maier, ex-CFF, chef de projet D RTE 28100

Markus Roth, RhB

Marcel Schmid, UTP

Patrick Waldburger, AB

# Bienvenue

**Bernhard Adamek**  
Vice-directeur de l'UTP

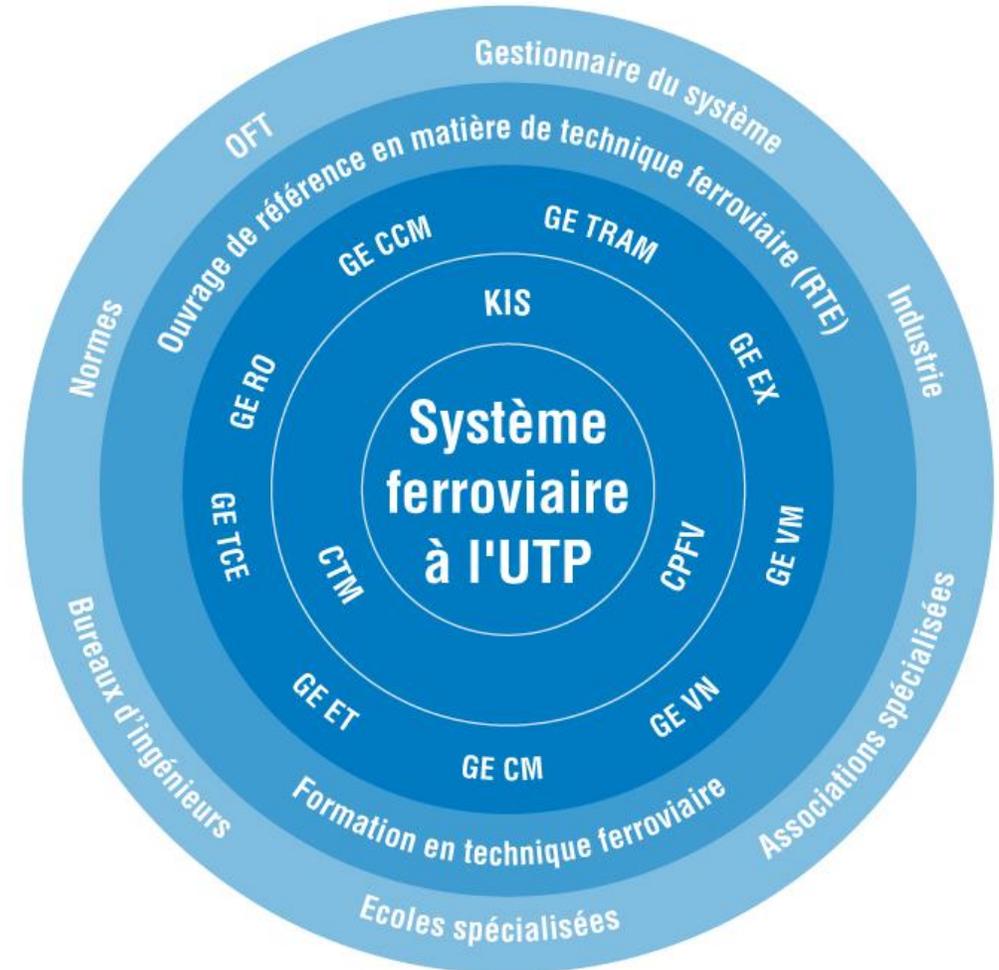


# Colloque réseaux de données

Organisé par le groupe d'experts  
Électrotechnique de l'UTP

en étroite collaboration avec

le groupe de projet D RTE 28100



# Colloque réseaux de données

## Remarques

- Programme transmis avec l'invitation (légèrement modifié)
- Pause-café et repas de midi propices à des échanges approfondis et des contacts plus étroits
- Les intervenants se tiennent à disposition pour répondre à toute question posée en plénum ou dans le cadre d'un échange bilatéral
- Interprétation simultanée allemand → français
- Les présentations peuvent être téléchargées → lien envoyé par courriel ce matin

# Colloque réseaux de données

## Retour sur le lancement du projet RTE

- Les groupes d'experts de l'UTP évaluent la nécessité de mettre en place de nouvelles réglementations RTE.
- Certains thèmes semblent intéressants, mais pas suffisamment pour mettre sur pied un groupe rapidement.
- Le phénomène inverse s'est produit pour le projet «Cybersécurité et réseaux de données»: de nombreux spécialistes se sont manifestés pour intégrer le groupe.
- C'est un grand jour pour le groupe d'experts!  
Le projet est publié et nous allons aujourd'hui présenté le produit dans le cadre de ce colloque.

# Programme de la matinée

dès 9h	<b>Arrivée des participants</b> Café-croissants
9h30	<b>Accueil et introduction</b> Robert Leemann
9h45	<b>Nouvelle réglementation RTE</b>
9h45	Actions nécessaires et prescriptions souveraines de base, Safety – Security Patrick Favre, Tobias Hubschmid
10h05	D RTE 28100 Démonstration de la sécurité des réseaux de données Introduction et principes RTE chap. 1-4 Kurt Maier
10h20	Questions Robert Leemann
10h35	<b>Pause</b>

# **D RTE 28100, Actions nécessaires et prescriptions souveraines - Safety et Security, 1ère partie**

Patrick Favre, Tobias Hubschmid

Berne, mercredi 11.12.2024

# Actions nécessaires et prescriptions souveraines

1ère partie:

- Quelles sont les installations que l'OFT doit approuver ?
- Quand utilisait-on des homologations de série dans le passé ?
- Comment les réseaux de données étaient-ils traités dans le passé?
- Le processus «Änderungsprozess Datennetze@SA» aux CFF
- Un processus pour les chemins de fer privés

2<sup>ème</sup> partie: Focus security

# Quelles sont les installations que l'OFT doit approuver ?

## **Loi sur les chemins de fer, Art. 18** Procédure d'approbation des plans (PAP)

<sup>1</sup> Les constructions et installations **servant exclusivement ou principalement à la construction et à l'exploitation d'un chemin de fer** (installations ferroviaires) ne peuvent être établies ou modifiées que si les plans du projet ont été approuvés par l'autorité compétente.

[...]

<sup>2</sup> L'autorité chargée de l'approbation des plans est l'OFT.

→ Il n'y a pas que les installations de haute importance pour la sécurité qui doivent être approuvées par l'OFT

## **Ordonnance sur les chemins de fer, Art. 7** Homologation de série (HdS)

<sup>1</sup> Une demande d'**homologation de série** conformément à l'art. 18x LCdF peut être déposée si elle **simplifie les procédures d'autorisation**.

→ L'homologation de série sert en principe à simplifier les PAP

# Quand utilisait-on des homologations de série dans le passé?

Dans passé et aujourd'hui:

- Dans le domaine des installations de sécurité, on homologuait principalement les systèmes de haute importance pour la sécurité (SIL 1-4).
- Les réseaux de données utilisés par ces systèmes étaient homologués.
- Les applications de faible importance pour la sécurité comme RCS (l'ancien TMS des CFF) passaient souvent «sous le radar».

Dans le futur:

- Les applications télématiques devraient systématiquement être approuvées, même si elles ne sont pas d'une haute importance pour la sécurité.

# Comment les réseaux étaient-ils traités dans le passé?

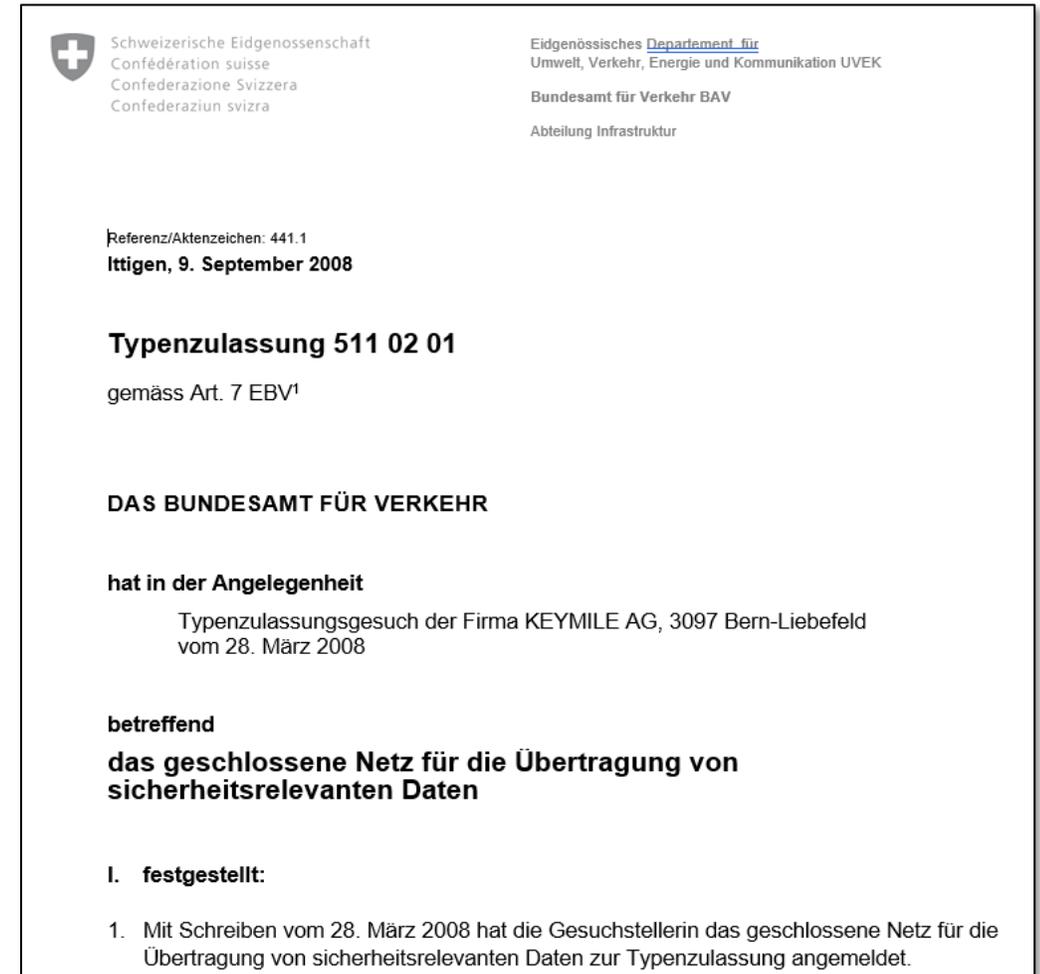
Homologations de série:

- Difonet (CFF)
- Rail IP (CFF)
- UMUX / XMC20  
(Ascom/Keymile/ABB/Hitachi)

Elles traitent le réseau et contiennent une liste d'applications autorisées.

Chaque modification aux applications doit être soumise pour approbation à l'OFT.

→ **Pas vraiment flexible ni dynamique**



# Le processus «Änderungsprozess Datennetze@SA» aux CFF

Seite 1/35 

Änderungsprozess Datennetze@SA

---

Dokumenten-Nummer	SA16-00351
Datum	02.09.2020

Version	Erstellt		Freigegeben	
3.3	Christine Kajtzovic I-NAT-NAT-SAZ-PLP-PJM	Dominik Hofer I-NAT-SAZ-APP-TAI	Johannes Scheuner I-NAT-SAZ-PLP-PJM	Name
	 Christine Kajtzovic I-NAT-NAT-SAZ-PLP-PJM 02.09.2020 14:00:00 02.09.2020 14:00:00	 Dominik Hofer I-NAT-SAZ-APP-TAI 02.09.2020 14:00:00 02.09.2020 14:00:00	 Johannes Scheuner I-NAT-SAZ-PLP-PJM 02.09.2020 14:00:00 02.09.2020 14:00:00	OE
	 Christine Kajtzovic I-NAT-NAT-SAZ-PLP-PJM 02.09.2020 14:00:00 02.09.2020 14:00:00			Visum

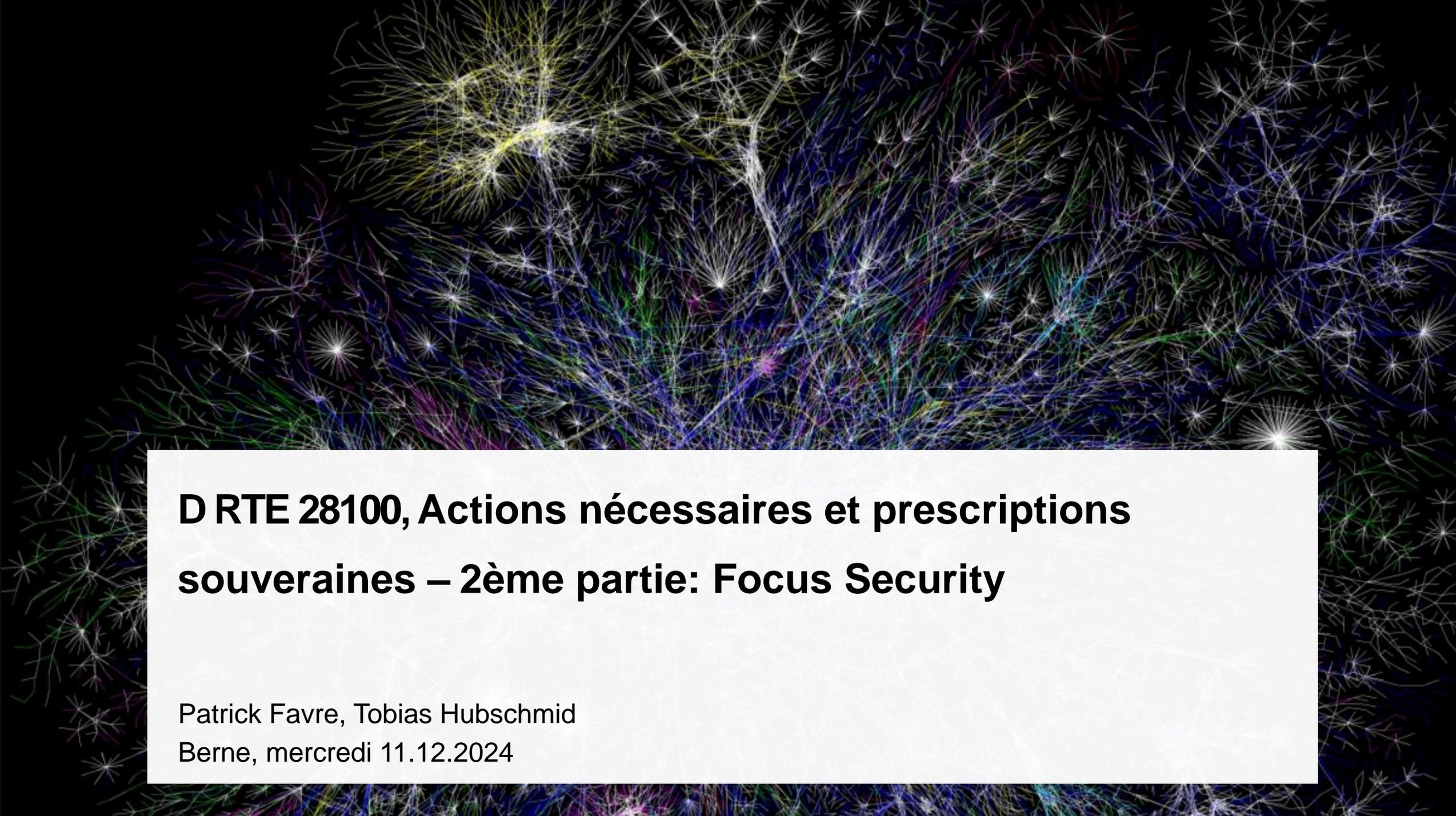
Eigner	I-NAT-SAZ
--------	-----------

Dieses Dokument ist urheberrechtlich geschützt. Jegliche kommerzielle Nutzung bedarf einer vorgängigen, ausdrücklichen Genehmigung.

- A l’occasion du remplacement du réseau SDH des CFF par un réseau MPLS, on a cherché une alternative plus flexible aux homologations classiques.
- Cette alternative devait correspondre à la tendance actuelle de donner plus de liberté, mais aussi plus de responsabilité aux entreprises de chemin de fer.
- Ainsi a été défini entre 2017 et 2020 le processus «Änderungsprozess Datennetze@SA» avec l’idée **de ne plus homologuer le réseau avec ses applications autorisées, mais plutôt le processus définissant comment ajouter une application.**
- Depuis, des dizaines d’applications ont passé par ce processus.

# La D RTE 28100: un processus pour les chemins de fer privés

- En 2021 l'UTP a lancé le groupe de travail D RTE 28100 dans le but de traiter pour les chemins de fer privés la question des réseaux de données modernes utilisés par des applications de haute importance pour la sécurité.
- Dès le début, une solution proche de l'«Änderungsprozess Datennetze@SA» des CFF était sur la table, mais le groupe de travail s'est longtemps cherché au sujet du périmètre à traiter.
- Finalement, la D RTE 28100 ressemble à une transposition de l'«Änderungsprozess Datennetze@SA» pour les chemins de fer privés et elle prend en compte les expériences faites par les CFF.



# **D RTE 28100, Actions nécessaires et prescriptions souveraines – 2ème partie: Focus Security**

Patrick Favre, Tobias Hubschmid  
Berne, mercredi 11.12.2024

# Actions nécessaires: focus security



1960 : Recherche le contrôle d'accès et les caméras de surveillance

Changement de société  
∞  
Changement de la culture  
de security



2024 : nouvelle porte tambour pare-balles à l'entrée principale du Palais Fédéral

# D RTE 28100 : Actions nécessaires - Security

## Passé

- Nombre **raisonnable** de réseaux IP dans le domaine TO.
- Les réseaux de données sont encore peu critiques en termes de safety et d'exploitation.
- Les connexions de données importantes pour la safety sont **séparées d'Internet** (réseaux fermés, surface d'attaque en premier lieu au niveau physique)
- TI et TO relativement bien séparées et **gérables**.
- Les réseaux de données ne sont guère segmentés, **la security n'est guère un sujet actuel**.
- Peu de **budget** (si tant est qu'il y en ait un) pour les mesures de security.

## Réseaux de données aujourd'hui

### ↗ Importance pour l'exploitation

- TI et TO se mélangent de plus en plus, **les réseaux interentreprises ne sont plus sous le contrôle total du GI**
- Industrie 4.0 (IoT, Clouds, etc.), "tout IP", **croissance exponentielle des appareils connectés au réseau**.
- Anciennes applications et services faiblement protégés toujours en service (on travaille encore en partie avec Telnet).
- **Menaces croissantes**
- **Exigences croissantes envers les réseaux**
- Plus (suffisamment) de **budget** pour les mesures de security disponible ???

GI: Gestionnaire d'infrastructure

# Prescriptions souveraines – DE-OCF 38.1

DISPOSITIONS D'EXÉCUTION	
Chapitre:	Ouvrages et installations
Section:	Installations de communication
Article:	Principes

<u>DE 38.1</u>	<u>Généralités</u>
1	Pour la spécification de fiabilité, disponibilité et d'appliquer les normes
1.1	Les exigences fonctionnelles de sécurité doivent être
1.2	Pour la communication, appliquer la norme S
1.3	La démonstration de conformité comprenant des fonctions doit être effectuées selon
1.3.1	Lorsque la norme SN EN 50129 est appliquée, il n'est pas nécessaire de tenir compte de la norme SN EN 50126-2, sauf quand celle-ci est explicitement référencée dans la norme SN EN 50129.
1.4	Les facteurs qui influencent les caractéristiques de fiabilité, de disponibilité, de maintenabilité et de sécurité (propriétés FDMS) doivent être respectés et contrôlés pendant toute la durée de vie des systèmes.
1.5	Pour les procédures d'approbation des plans et d'autorisation d'exploiter, l'OFT règle l'utilisation des normes SN EN 50126-1 et SN EN 50129 dans une directive.

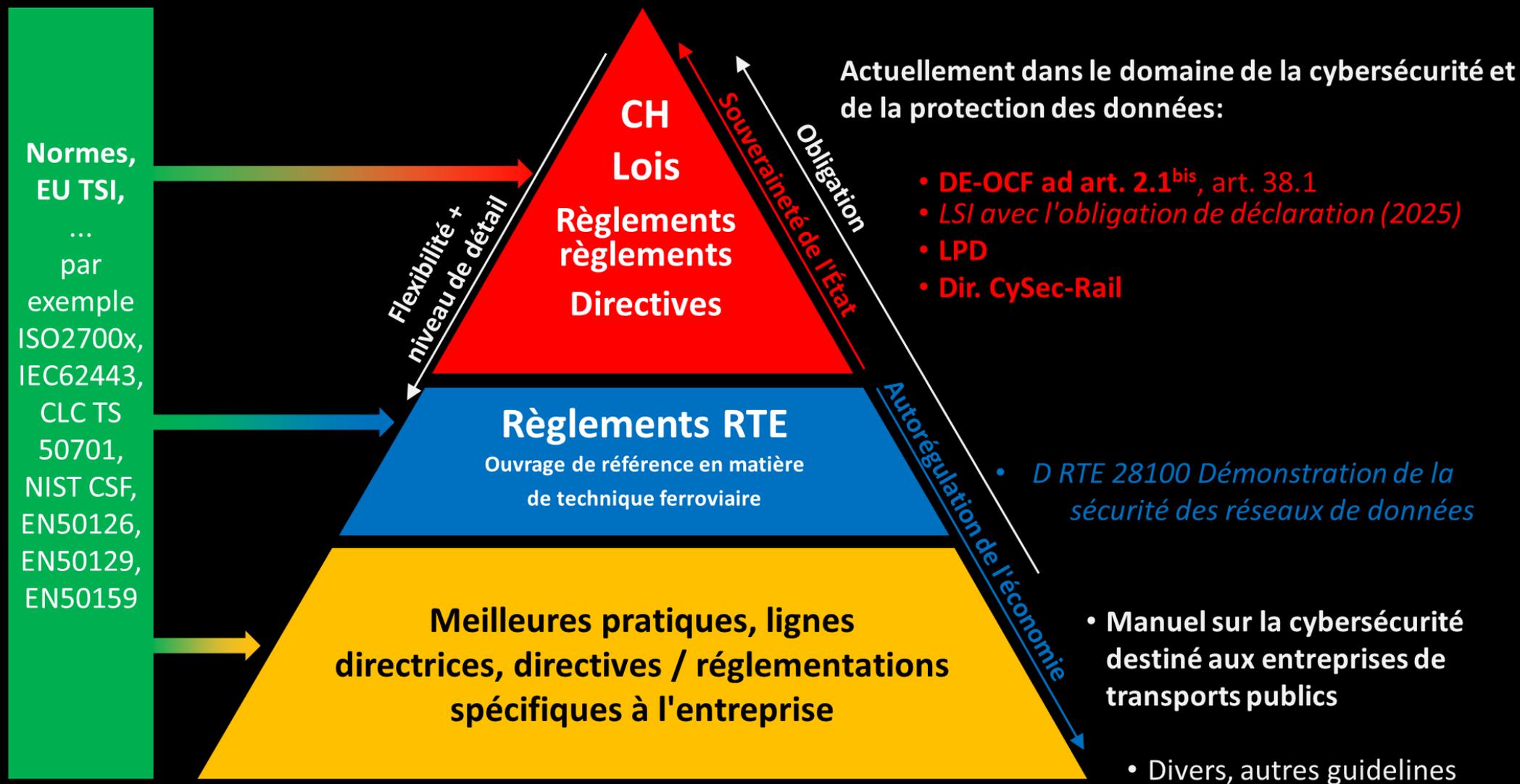
Les connexions et les réseaux de données doivent satisfaire aux exigences des installations, des systèmes et applications connectés en termes

- de fiabilité,
- de disponibilité,
- de la maintenabilité,
- de sécurité (exigences FDMS)
- et de cybersécurité.



- |   |   |
|---|---|
| 5 | Les DE-OCF ad art. 44, DE 44.b sont applicables aux exigences pour les câbles des installations de sécurité et des applications télématiques.   |
| 6 | <b>Nouveau</b> Les connexions et les réseaux de données doivent satisfaire aux exigences des installations, des systèmes et applications connectés en termes de fiabilité, de disponibilité, de maintenabilité, de sécurité (exigences FDMS) et de cybersécurité. |

# Prescriptions souveraines - Safety et Security



## D RTE 28100 : Pourquoi, en ce qui concerne la Security, ne pas simplement renvoyer à la Dir. CySec-Rail ou à une norme appropriée ?

- Le D RTE 28100 aborde **de manière plus concrète et détaillée** la question de la Security dans les réseaux de données (groupe cible spécifique).
- La branche n'a pas émis le souhait d'omettre des parties des exigences et de renvoyer à la Dir. CySec-Rail ou à une norme.
- Développements indépendants de la RTE 28100 et de la Dir. CySec-Rail (lors du lancement de la RTE 28100, on ne savait pas encore qu'il y aurait la Dir. CySec-Rail). Les normes sont actuellement très dynamiques (p. ex. IEC 63452).
- **Avantage de la RTE actuelle:** un seul document contenant toutes les informations.

Il s'agit maintenant d'acquérir de l'expérience et de procéder à des ajustements si nécessaire !

# D RTE 28100: Introduction

Kurt Maier, chef de projet D RTE 28100

Bern, mercredi 11.12.2024

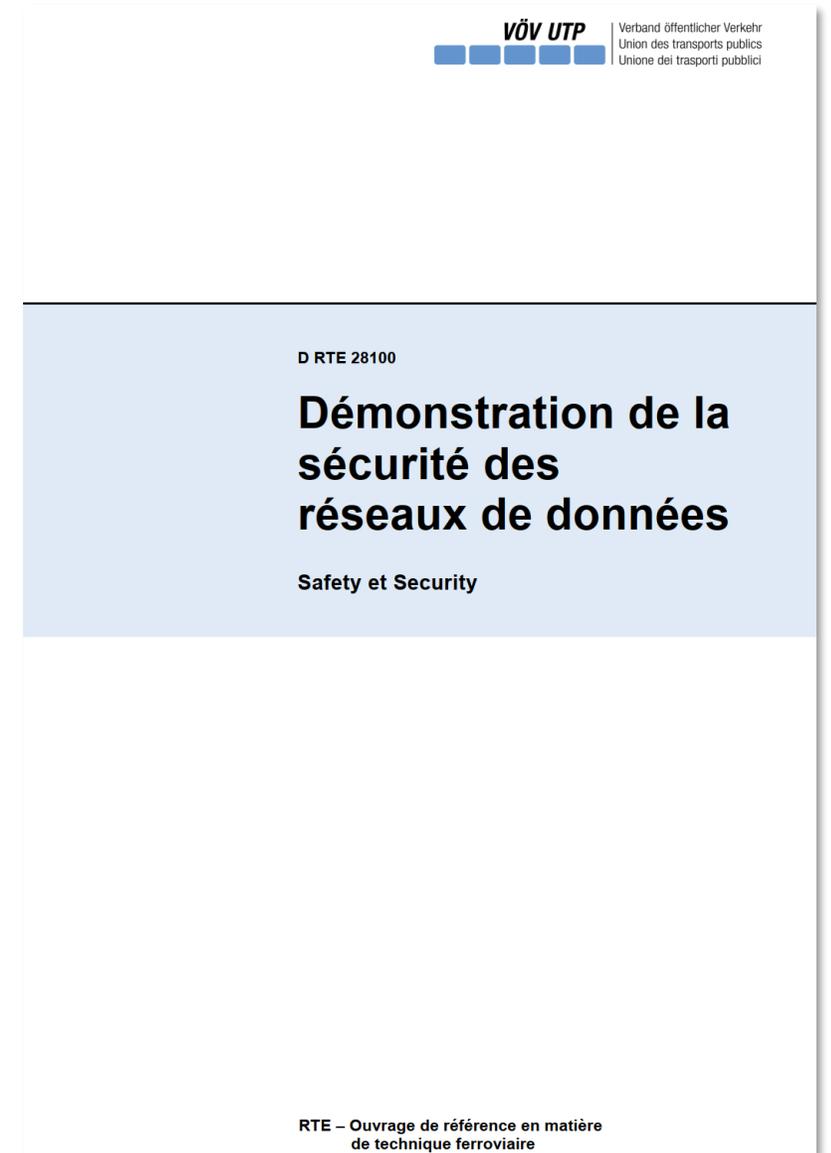
## Situation de départ pour la D RTE 28100

Lors d'un atelier du groupe d'experts Electrotechnique le **16.01.2020**, il a été constaté, entre autres, que :

- Le **remplacement des réseaux de données** existants est imminent.
- La **séparation des réseaux** fermés pour les applications liées à la sécurité devient plus difficile.
- Les **exigences de sécurité** des réseaux de données pour les applications liées à la sécurité et leur respect ne sont pas clairs.
- La **procédure correcte** pour l'appel d'offres, l'étude de projet, l'autorisation de l'OFT et l'exploitation des réseaux de données n'est pas claire.
- L'OFT estime qu'il faut clairement agir.
- La **cybersécurité** est également à prendre en compte.

# Qu'offre la réglementation D RTE 28100?

- Elle montre ce qu'il faut prendre en compte en matière de **Safety** et de **Security** lors de l'utilisation de réseaux de données d'infrastructure par les entreprises ferroviaires.
- Elle décrit comment les entreprises ferroviaires peuvent concevoir et exploiter leurs réseaux de données afin qu'ils répondent aux **prescriptions souveraines**.
- Les contenus sont à la pointe des prescriptions souveraines et des **normes**.



# Structure de la réglementation D RTE 28100

## Chapitres

1 Généralités

2 Bases

3 Abréviations et termes

4 Principes (informatif)

5 Exigences relatives aux réseaux de données (normatif)

6 Procédure d'homologation de série des réseaux de données (normatif)

7 Processus d'approbation des réseaux de données (normatif)

8 Projets de réseaux de données (informatif)

9 Applications ferroviaires (informatif)

10 Bibliographie

## Annexes (informatif)

A1 Prescriptions souveraines

A2 Normes relatives à la Safety et à la Security

A3 CLC/TS 50701

A4 SN EN 50159

A5 Sécurité des bâtiments pour la Safety et la Security

A6 Réseau de données Datacom-NG des CFF

Modèles V1-V7

Cœur de la RTE 28100

# Chapitres de la D RTE 28100

Chap. 1 Généralités, Chap. 2 Bases (normes etc.), Chap. 3 Abréviations et termes

Chap. 4 Principes (informatif)

→ Réseaux de données et applications (4.3), TI et TO (4.4), Safety et Security (4.5)

Chap. 5 Exigences relatives aux réseaux de données (normatif)

→ Catalogue d'exigences avec 12 sous-chapitres et 48 exigences

Chap. 6 Procédure d'homologation de série des réseaux de données (normatif)

→ Procédure simplifiée pour les nouveaux réseaux de données d'infrastructure

Chap. 7 Processus d'approbation des réseaux de données (normatif)

→ Processus de cycle de vie pour les réseaux de données

Chap. 8 Projets de réseaux de données (informatif)

Chap. 9 Applications ferroviaires (informatif)

## Annexes de la D RTE 28100

- A1 Prescriptions souveraines:** LCdF, OCF, DE-OCF, **Dir. CySec-Rail**, Dir. HdS
  - A2 Normes relatives à la Safety et à la Security**
    - SN EN 50126-1/2, SN EN 50129, **SN EN IEC 62443**, SN EN ISO/IEC 27000
  - A3 **CLC/TS 50701** Railway Applications – Cybersecurity**
    - **Introduction aux chapitres et aux annexes**
  - A4 **SN EN 50159** Communication de sécurité sur des systèmes de transmission**
    - classes de réseau, menaces et mesures de protection
  - A5 Sécurité des bâtiments pour la Safety et la Security**
    - Objectifs de protection, planification etc.
  - A6 Réseau de données Datacom-NG des CFF**
    - Homologation de série et processus de modification de Datacom-NG
- Modèles V1-V7** → «Liste des applications prévues» etc.

## Applications ferroviaires (Chap. 4.3.1)

### L'importance pour la sécurité:

Une application est **de haute importance pour la sécurité** ou **de faible ou sans importance pour la sécurité**.

La distinction se base sur le niveau d'intégrité de sécurité (SIL):

- **SIL 1 à SIL 4** → **de haute importance pour la sécurité**
- **intégrité de base** → **de faible ou sans importance pour la sécurité**

### L'importance pour l'exploitation:

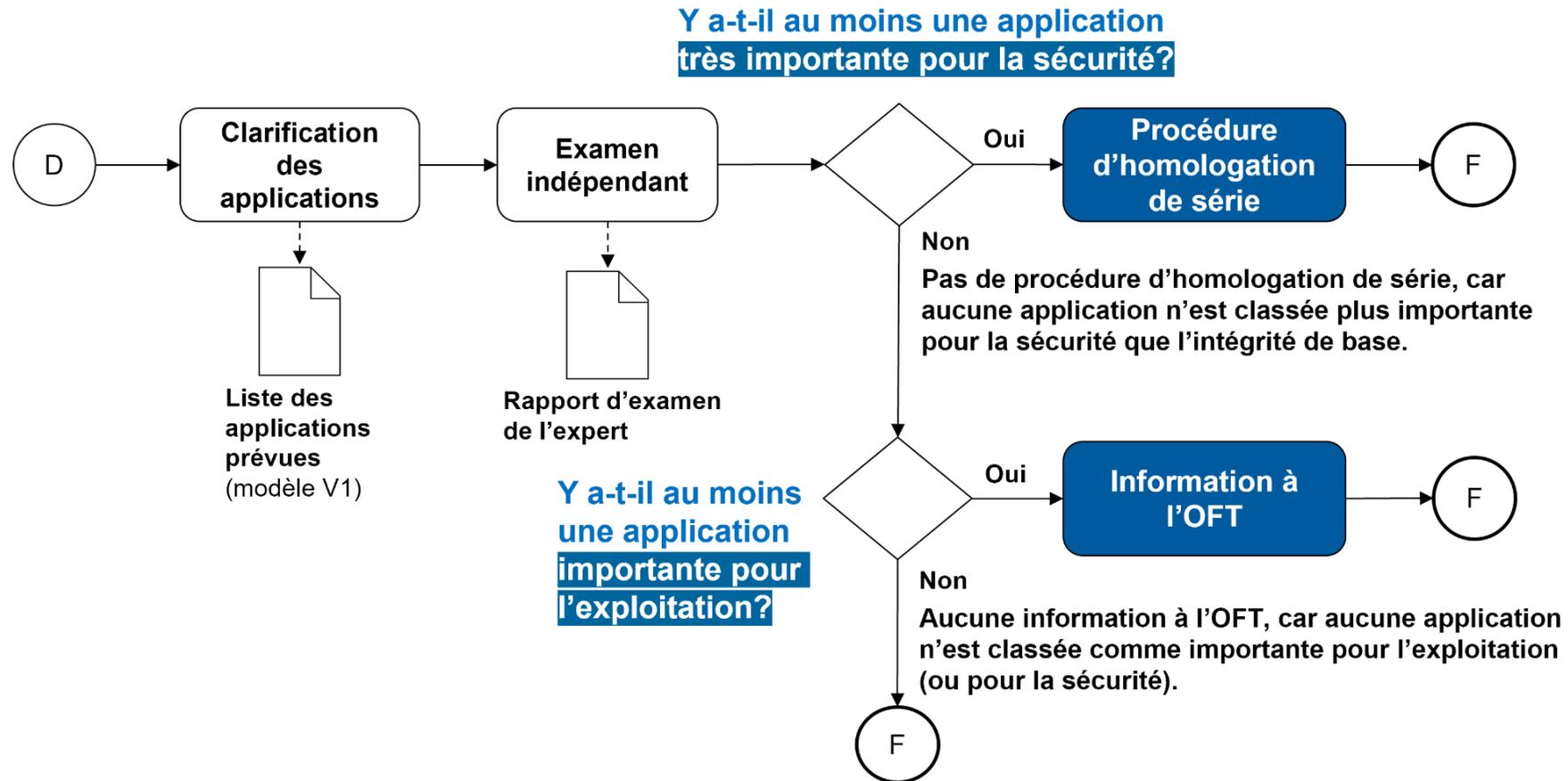
Une application est **importante pour l'exploitation** ou **pas importante pour l'exploitation**.

«Les systèmes ou installations importants pour l'exploitation sont déterminants pour le maintien de l'exploitation ferroviaire. Ils présentent des exigences accrues en matière de disponibilité afin de garantir une qualité de service et de transport élevée pour la clientèle.» Chap. 3.2 Termes

**L'importance des applications en termes de sécurité et d'exploitation détermine la procédure à mettre en œuvre conformément à la réglementation RTE 28100.**

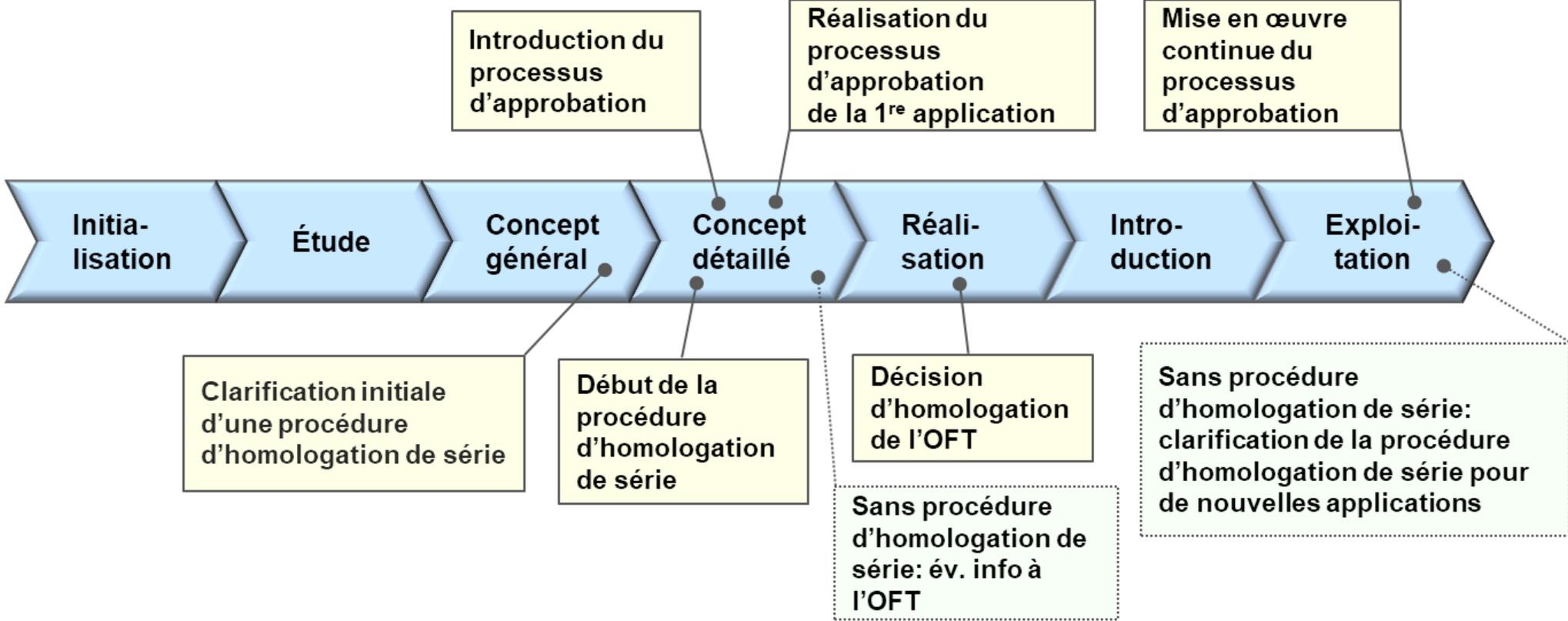
# Applications ferroviaires

Clarification avant une procédure d'homologation de série (cf. chap. 6):



# Projets de réseaux de données (Chap. 8)

La méthodologie de projet classique est appropriée pour montrer la procédure à suivre lors d'une homologation de série.



# Applications ferroviaires (Chap. 9)

## Appareils d'enclenchement

Fonctions:

- protection des itinéraires de manœuvre,
- protection des itinéraires de train.

Importance pour la sécurité: jusqu'à SIL 4

Important pour l'exploitation: oui

Exemples:

- enclenchements électroniques,
- enclenchements à relais.

<b>9</b>	<b>Applications ferroviaires (informatif) .....</b>
9.1	Installations de sécurité et applications télématiques .....
9.2	Conditions d'application liées à la sécurité .....
9.3	Exemples d'applications ferroviaires .....
9.3.1	Disposition, Traffic Management System (TMS).....
9.3.2	Technique de commande ferroviaire .....
9.3.3	Télécommande .....
9.3.4	Appareils d'enclenchement .....
9.3.5	Installations extérieures.....
9.3.6	Contrôle de la marche des trains, signalisation en cabine ..
9.3.7	Radio .....
9.3.8	Diagnostic .....
9.3.9	Maintenance à distance .....
9.3.10	Approvisionnement en énergie.....

Exemples de conditions d'application dans la technique de protection et de commande ferroviaire

- Les connexions réseau (LAN, WAN) au sein du système doivent satisfaire aux exigences d'un **réseau de classe 2** selon la norme SN EN 50159.
- Le réseau doit être conçu de sorte que le **temps de latence** de 25 ms maximum entre n'importe quel port d'accès soit respecté en cas de sollicitation de la bande passante garantie.

## D RTE 28100: Introduction

Merci beaucoup.

## Démonstration de la sécurité des réseaux de données

Safety et Security



# Questions



**Boissons et collation au foyer**

**Merci de regagner votre place pour 10h55, la prochaine présentation commencera à 11h00**



# Programme de la matinée

11h	<b>Contenu de la réglementation RTE</b> <b>D RTE 28100 Démonstration de la sécurité des réseaux de données</b>
11h	Exigences RTE chap. 5 (part Security élevée, points sensibles, application pratique, y c. V7 évent. avec exemples des AB) Markus Roth, Emmerich Horvath, Kurt Maier
11h15	Procédure d'homologation de série RTE chap. 6 Processus d'approbation RTE chap. 7 avec documents correspondants Patrick Favre, Kurt Maier
11h45	Questions Robert Leemann
12h	<b>Dîner</b>

# **D RTE 28100, Exigences relatives aux réseaux de données**

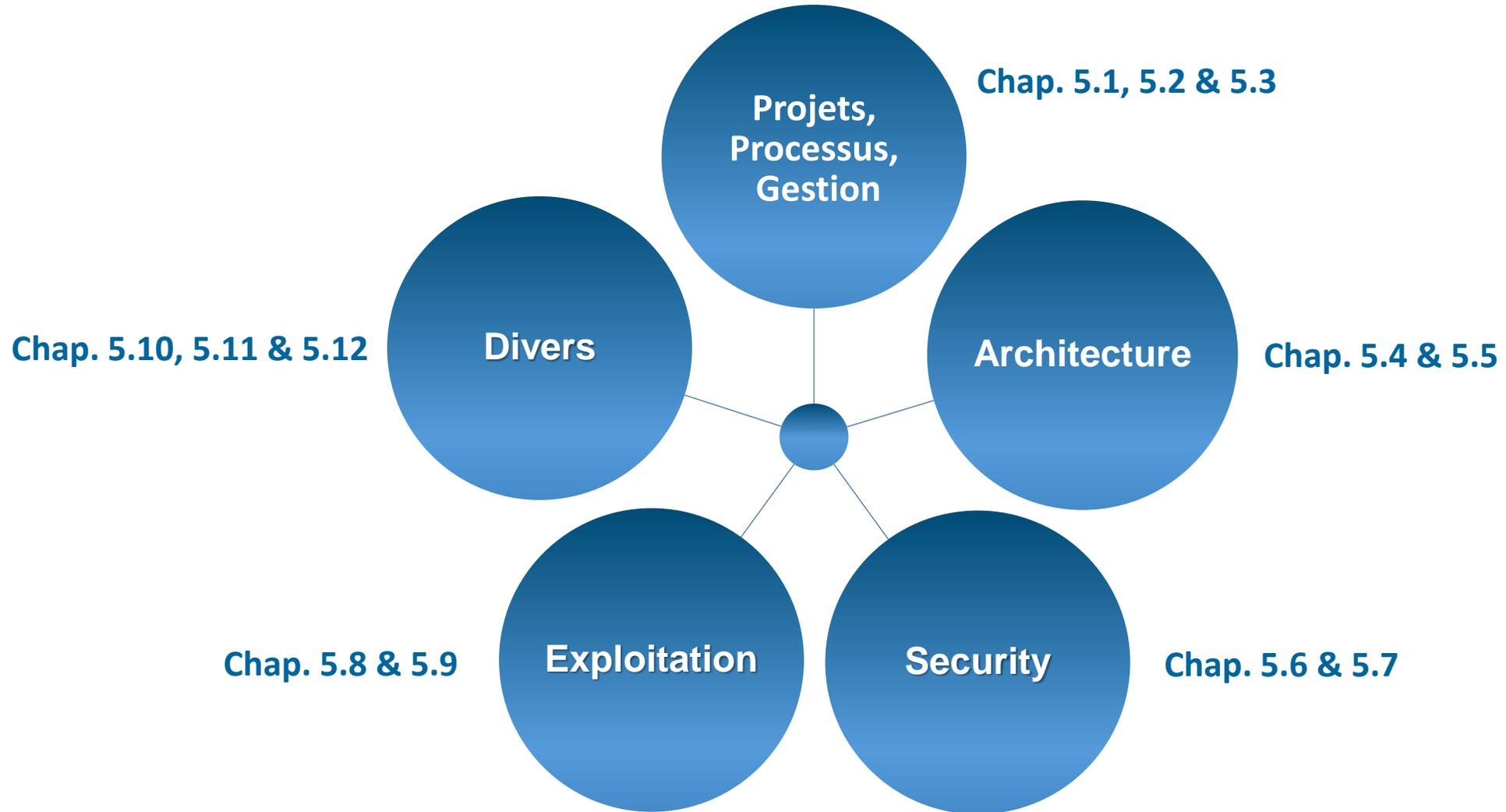
Emmerich Horvath, Markus Roth, Kurt Maier

Bern, mercredi 11.12.2024

# Exigences relatives aux réseaux de données (chap. 5)



# Subdivision du chap. 5



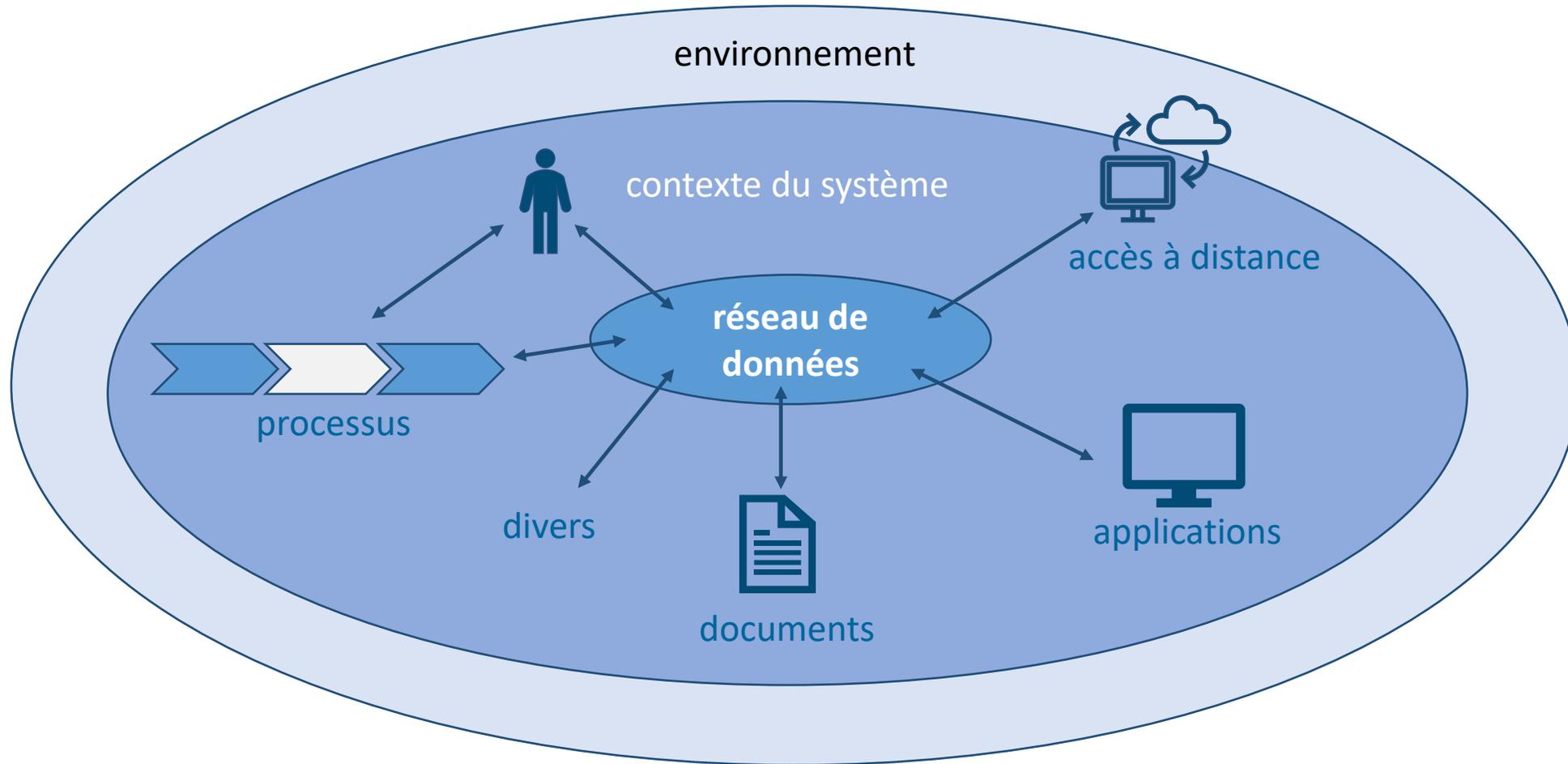
# Subdivision des exigences

Chap. 5.1	Exigences de projet relatives à la Safety	<b>Projets, Processus, Gestion</b>
Chap. 5.2	Exigences de projet relatives à la Security	
Chap. 5.3	Information Security Management System (ISMS)	
Chap. 5.4	Exigences relatives à l'architecture et au zonage	<b>Architecture</b>
Chap. 5.5	Redondances et disponibilité	
Chap. 5.6	Exigences relatives à l'analyse des risques de Security	<b>Security</b>
Chap. 5.7	Target Security Level minimal selon la CLC/TS 50701	
Chap. 5.8	Exigences relatives à l'administration et la configuration du système	<b>Exploitation</b>
Chap. 5.9	Exigences relatives au concept d'exploitation du réseau de données	
Chap. 5.10	Exigences relatives à la documentation	<b>Divers</b>
Chap. 5.11	Exigences relatives aux experts	
Chap. 5.12	Exigences relatives à la sécurité des bâtiments	

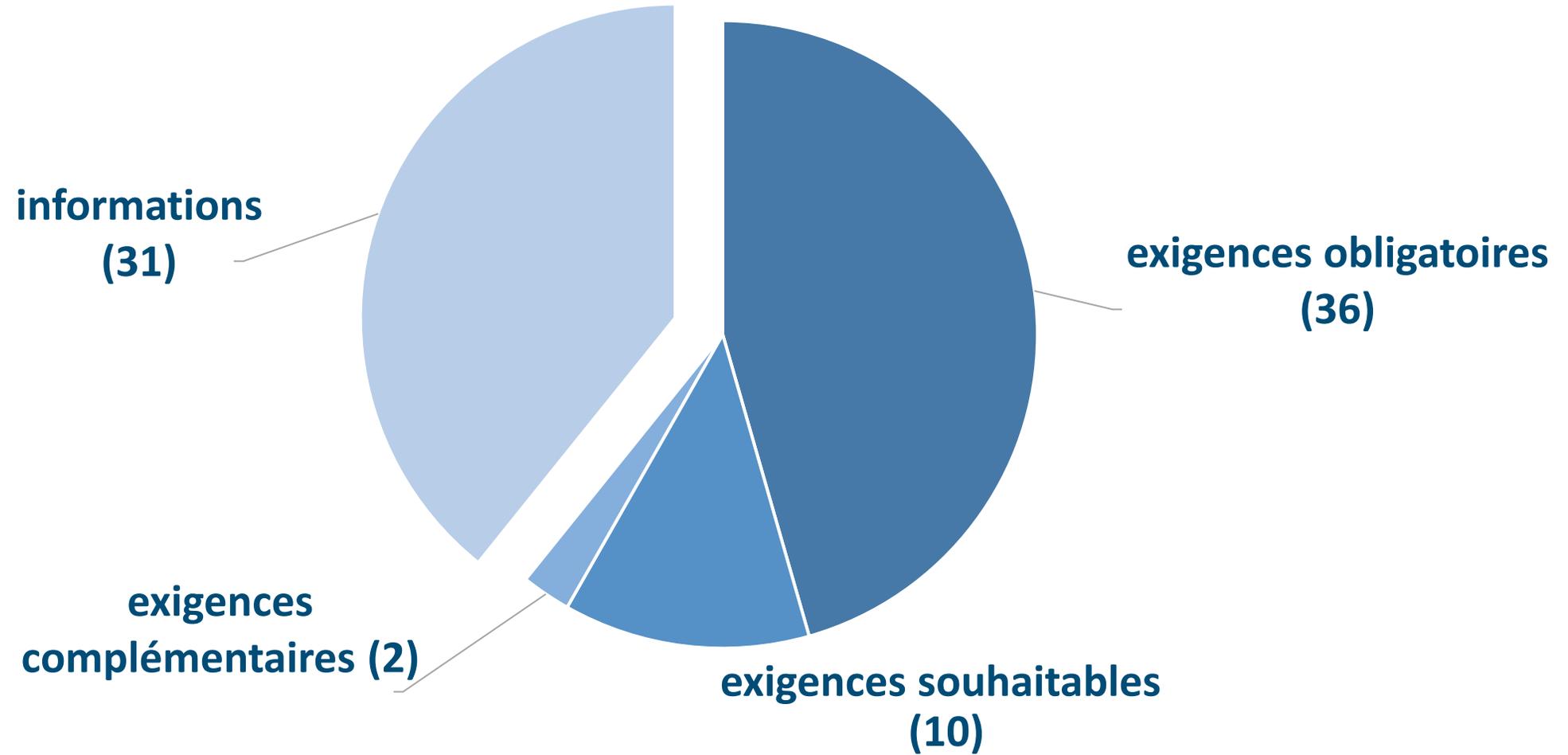
## D RTE 28100: Exigences relatives aux réseaux de données



# Exigences: Système, contexte du système, environnement



# Catégorisation des exigences au chap. 5



## Catégorisation des exigences au chap. 5

Les **exigences obligatoires (O)** doivent être mises en œuvre dans le cadre de l'application de la D RTE 28100.

Les **exigences souhaitables (S)** expriment des préoccupations importantes, mais ne doivent pas nécessairement être mises en œuvre dans tous les cas. Ils sont traités en fonction des risques.

Les **exigences complémentaires (C)** peuvent être satisfaites dans la mesure où les circonstances et les ressources le permettent.

Les **informations (I)** sont des compléments aux exigences.

# Identification des exigences

## Identification Rx.y

**R** signifie «Requirement» (exigence),  
**x** correspond à la numérotation du **sous-chapitre 5.x**,  
**y** étant la **numérotation continue** au sein du sous-chapitre.

### 5.1 Exigences de projet relatives à la Safety

---

(O, R1.1) La Safety doit être prise en compte dès le début de la planification d'un réseau de données si ce dernier est également destiné à des applications de haute importance pour la sécurité (fonctions de sécurité SIL 1 à SIL 4).

(O, R1.2) Les rôles et responsabilités en matière de Safety doivent être déterminés. L'utilisation d'un réseau de données dans un environnement d'applications de haute importance pour la sécurité nécessite que le gestionnaire d'infrastructure possède des connaissances spécialisées approfondies et détaillées sur le réseau de données et les applications. Si les connaissances spécialisées en matière de Safety font défaut, des mesures doivent être prises le plus tôt possible.

(O, R1.3) Une procédure d'homologation de série conforme à la présente réglementation RTE sera mise en œuvre si les conditions l'exigent (cf. section 6.3.1).

Exemple: (O, **R1.1**)  
→ au chap. **5.1**, la **1ère exigence**  
(exigence obligatoire)

# Modèle Excel D-RTE-28100-V7

GI (en abrégé)/GI (en toutes lettres)

Exigences relatives aux réseaux de données selon la réglementation D RTE 28100, chapitre 5

Projet de réseau de données

Il n'est pas nécessaire de traiter chaque exigence O ou S séparément. Il est également possible de prendre position pour chaque sous-chapitre du chapitre 5. (Éventuellement avec des compléments individuels pour les exigences)

Type	Texte de l'exigence du chapitre 5	Situation, risques, mesures, mise en œuvre	Statut	Commentaires/compléments
T	<b>5.1 Exigences de projet relatives à la Safety</b>			
O	(O, R1.1) La Safety doit être prise en compte dès le début de la planification d'un réseau de données si ce dernier est également destiné à des applications de haute importance pour la sécurité (fonctions de sécurité SIL 1 à SIL 4).			
O	(O, R1.2) Les rôles et responsabilités en matière de Safety doivent être déterminés. L'utilisation d'un réseau de données dans un environnement d'applications très importantes pour la sécurité nécessite que le gestionnaire d'infrastructure possède des connaissances spécialisées approfondies et détaillées sur le réseau de données et les applications. Si les connaissances spécialisées en matière de Safety font défaut, des mesures doivent être prises le plus tôt possible.			
O	(O, R1.3) Une procédure d'homologation de série conforme à la présente réglementation RTE sera mise en œuvre si les conditions l'exigent (cf. section 6.3. 1).			
O	(O, R1.4) Le respect des conditions d'application des applications importantes pour la sécurité sur le réseau de données doit être garanti tout au long de leur cycle de vie. Le processus d'approbation tel qu'il est défini dans la présente réglementation RTE sert, entre autres, de preuve.			

# Exigences en matière de Safety et Security

- Les exigences se rapportent aux réseaux de données avec lesquels les applications ferroviaires importantes pour l'exploitation et de haute importance pour la sécurité sont mises en réseau.
- Les exigences indiquent la voie à suivre, sans que chaque détail soit prédéfini.
- Pour le traitement des exigences du chapitre 5, il existe le modèle Excel D-RTE-28100-V7.
- **Dans tous les cas, la responsabilité de l'évaluation et de la mise en œuvre des exigences incombe aux gestionnaires d'infrastructure.**



# D RTE 28100: Exigences relatives aux réseaux de données

## Démonstration de la sécurité des réseaux de données

Safety et Security

Merci beaucoup.



# **D RTE 28100, Homologation de série et processus d'approbation, 1ère partie**

Kurt Maier, Patrick Favre

Berne, mercredi 11.12.2024

# Homologation de série (Chapitre 6)

1ère partie:

- Pourquoi une homologation de série ?
- Une homologation de série n'est pas toujours nécessaire
- Liste des applications prévues
- Procédure d'homologation de série
- Procédure en cas d'information à l'OFT (sans procédure)
- Cas sans d'interaction avec l'OFT
- Information périodique à l'OFT

# Pourquoi une homologation de série ?

Deux variantes envisageables pour l'approbation des réseaux de données ont été comparées:

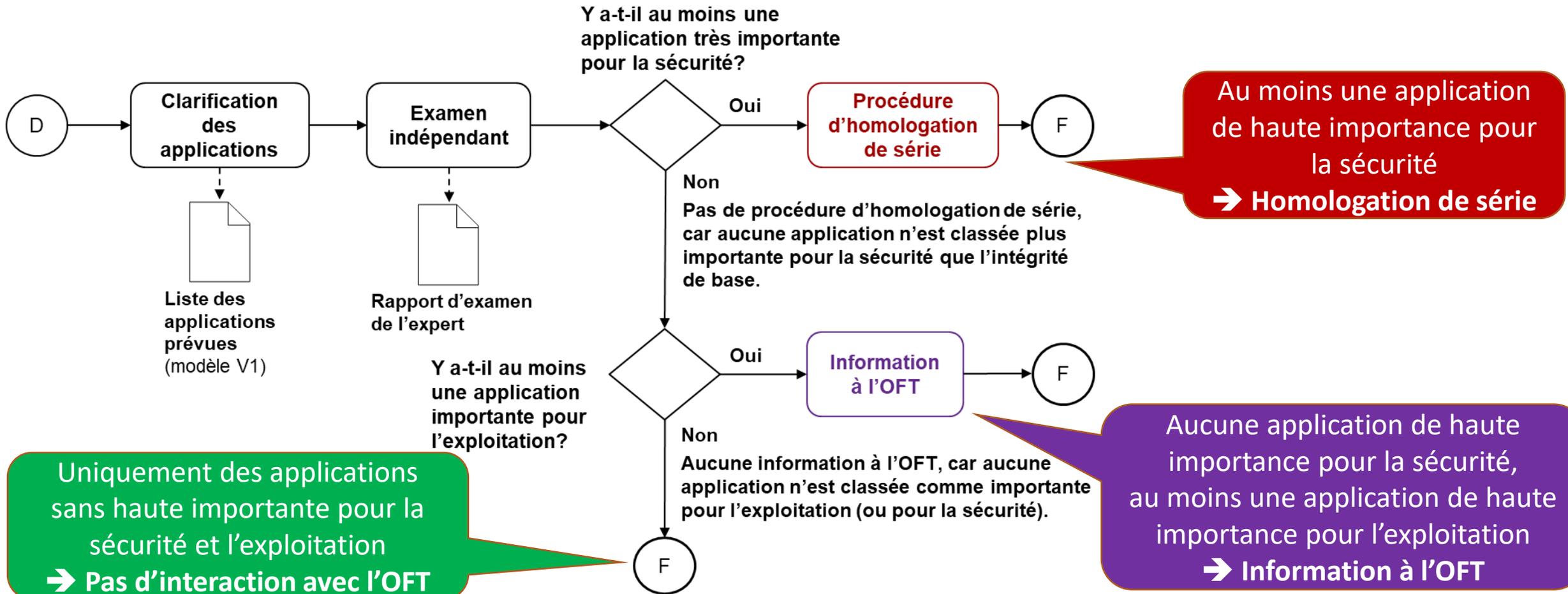
Procédure d'approbation des plans générique	Homologation de série
Une PAP par GI et par réseau de données	Une HdS par GI et par réseau de données
100% conforme aux prescriptions souveraines	Dans l'esprit des prescriptions souveraines
Ne rentre pas vraiment dans le moule des PAP classiques, implique un «nouveau genre» de PAP	Moins formaliste, très flexible, dynamique
	Utilisée jusqu'à lors pour les réseaux de données

→ La variante de l'homologation de série a été choisie pour sa flexibilité et sa simplicité.

*REMARQUE: Dans la prochaine directive «Démonstration de la sécurité des installations de sécurité», on utilisera probablement une PAP ad hoc pour les installations télématiques.*

# Une homologation de série n'est pas toujours nécessaire

→ On juge l'importance pour la sécurité **des applications qui utilisent le réseau** ←



# Liste des applications prévues (modèle V1)

- La liste contient toutes les applications à connecter au réseau de données avec leur importance pour la sécurité et l'exploitation.
- Après son établissement, elle doit être contrôlée par un expert.
- La liste doit être tenue actuelle pendant toute la durée de vie du réseau de données.

Liste des applications prévues  
GI (en abrégé)/GI (en toutes lettres)  
Projet de réseau de données

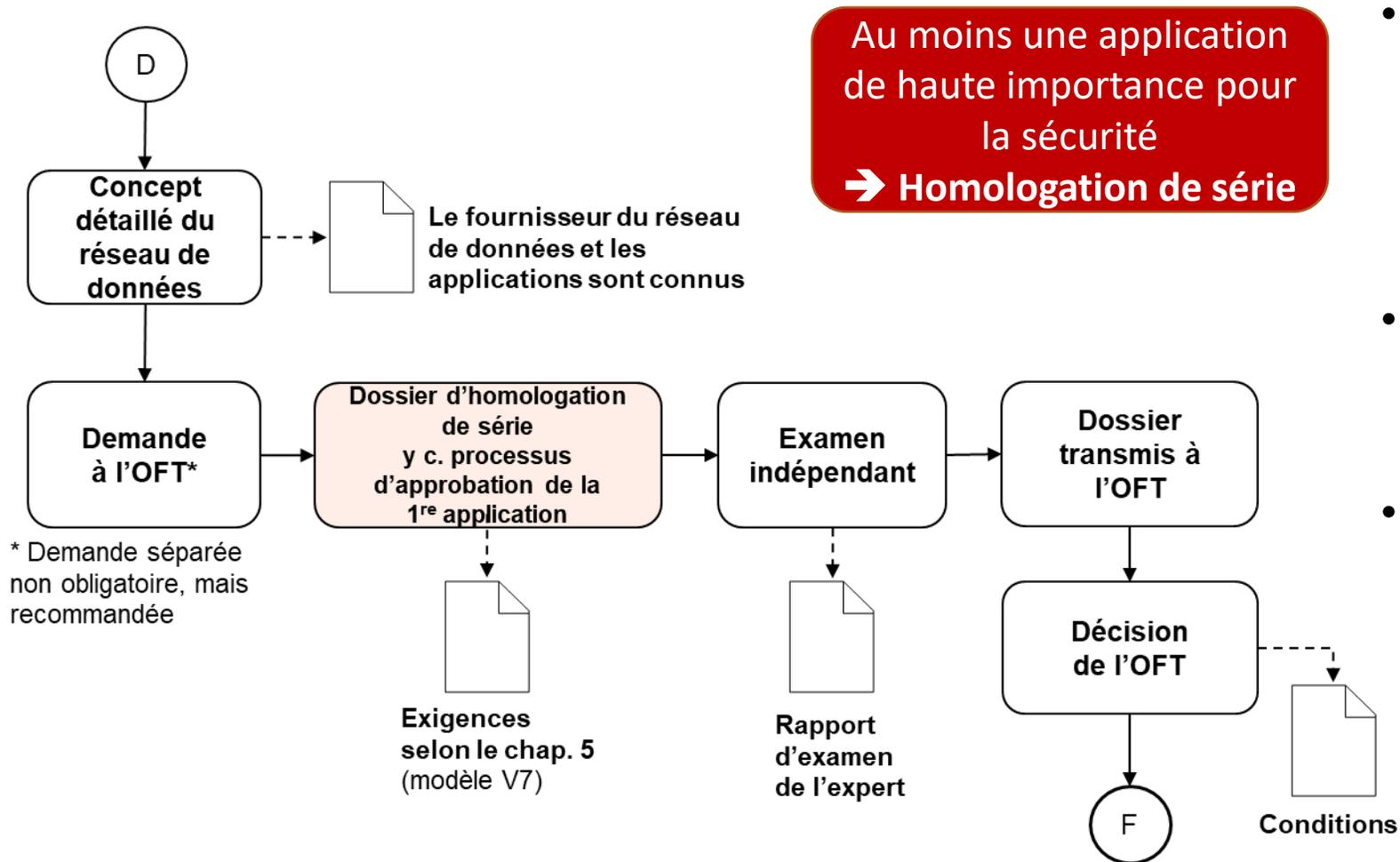
Insérer le logo du GI

## 2. Applications prévues

Les applications qui seront mises en ligne sur le réseau de données doivent être saisies dans le tableau ci-après.

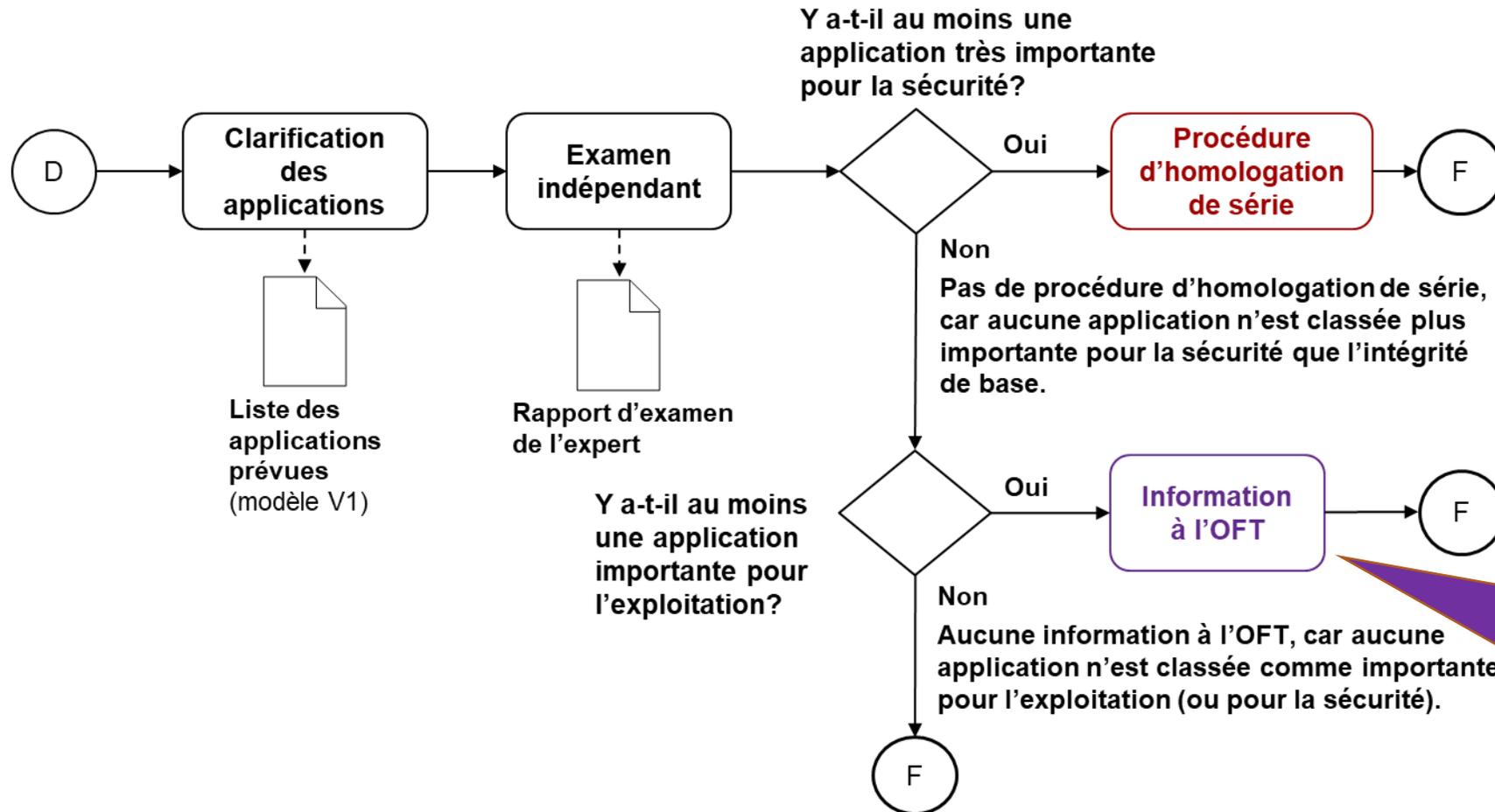
Application	Version (principale)	Fournisseur	Fonction, domaine d'utilisation, caractéristiques	Classe EN 50159 [Classe n°]	Importante pour la sécurité? [SIL n°, BI]	Importante pour l'exploitation? [oui, non]
Système de commande et d'information			Technique de commande ferroviaire	Classe 2	SIL 2	Oui
RCI			Technique de commande ferroviaire, télétransmission à l'Er	Classe 2	SIL 2	Oui
rcs95			Technique de commande ferroviaire, télétransmission à l'Er	Classe 1	SIL 2	Oui
Elektra 2 (CC) – Elektra 2 (EC)			Connexion encl.-encl. avec le site distant	Classe 1	SIL 4	Oui
Elektra 2 (CC) – Elektra 2 (CC)			Connexion encl.-encl. avec l'appareil d'enclenchement voisin	Classe 2	SIL 4	Oui

# Procédure d'homologation de série



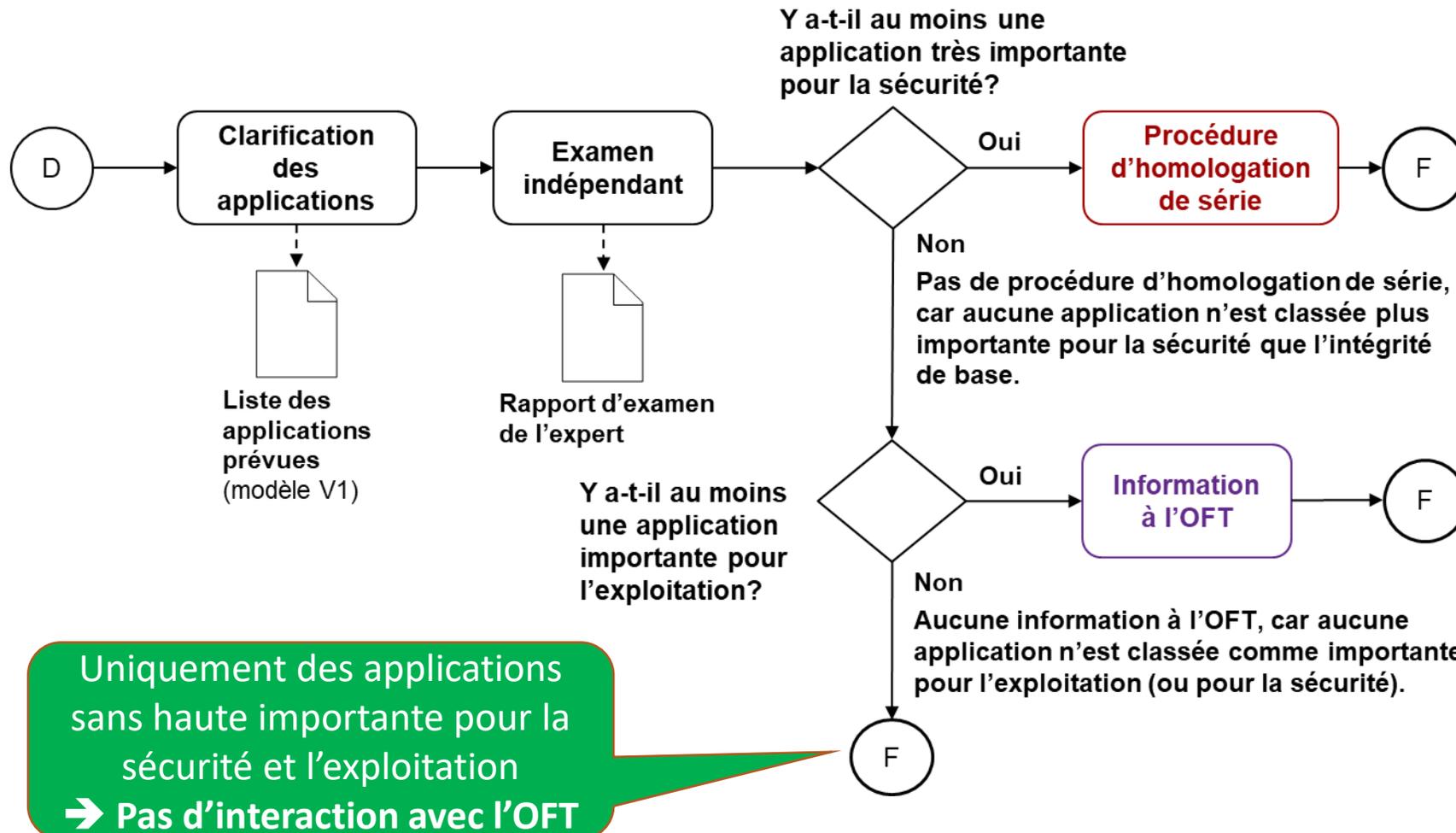
- Pour au moins une application de **haute importance pour la sécurité**, le gestionnaire d'infrastructure (GI) prouve qu'elle peut être branchée au réseau en toute sécurité.
- Le GI prouve aussi qu'il a **mis en œuvre et pérennisé les processus nécessaires dans son entreprise**.
- Après que l'OFT ait accordé l'HdS, le GI peut établir la conformité d'autres applications de manière indépendante, sans plus en référer à l'OFT.

# Procédure en cas d'information à l'OFT (sans procédure)



- Au branchement nouvelles applications, ce processus doit être mis en œuvre.

# Cas sans interaction avec l'OFT



- Même si l'OFT n'est pas impliqué, le GI doit conserver la documentation établie.
- A chaque nouvelle application, ce processus doit être mis en œuvre.

# Activités durant le cycle de vie du réseau

Dans les cas où une homologation de série a été accordée:

- L'OFT est à **informer annuellement** sur l'utilisation du processus d'approbation (listes actuelles des applications autorisées et des modifications autorisées au réseau de données).
- Le **processus d'approbation doit être exécuté** à nouveau lors de **modifications significatives** aux applications connectées ou au réseau de données.

Dans les autres cas:

- Si une information à l'OFT a été nécessaire, la liste actuelle des applications prévues est à lui fournir **annuellement**.
- Le **processus de clarification doit être exécuté** à nouveau lors de **modifications significatives** aux applications connectées. Selon le résultat, une homologation de série ou une information à l'OFT peuvent être nécessaires.

# **D RTE 28100: Homologation de série et processus d'approbation, 2ème partie**

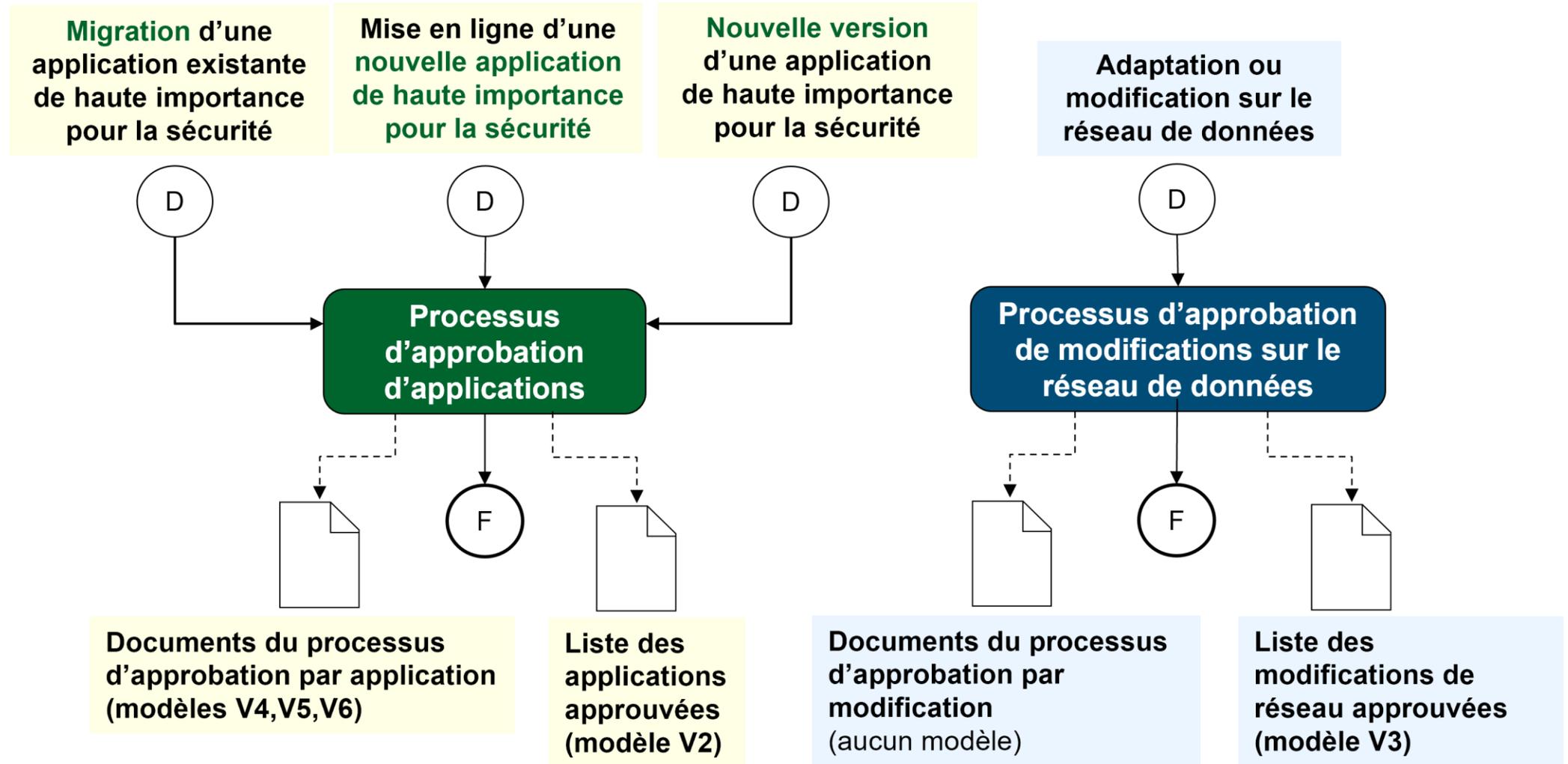
Kurt Maier

Bern, mercredi 11.12.2024

## D RTE 28100: Concept du processus d'approbation

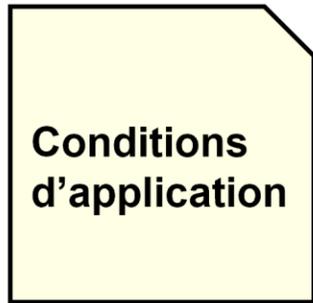
- Lorsque des **applications de haute importance pour la sécurité** sont connectées à un réseau de données, il faut éviter les risques inacceptables en matière de Safety et de Security.
- Il convient de vérifier systématiquement si le réseau de données peut respecter les **conditions d'application** d'une application de haute importance pour la sécurité en termes de Safety et Security.
- Le **processus d'approbation** permet de vérifier et de documenter que les exigences relatives au réseau de données sont respectées tout **au long de son cycle de vie**.
- Il y a deux processus distincts:
  - **Processus pour applications de haute importance pour la sécurité** avec trois points de départ
  - **Processus pour modifications sur le réseau de données** avec un point de départ

# Points de départ de processus d'approbation



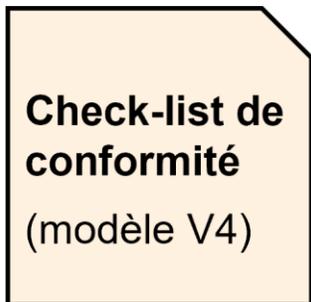
# Processus d'approbation d'applications

Fournisseur du réseau de données

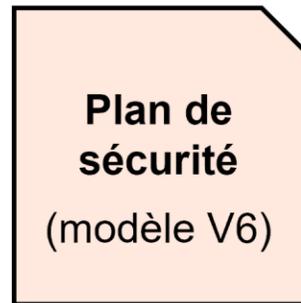
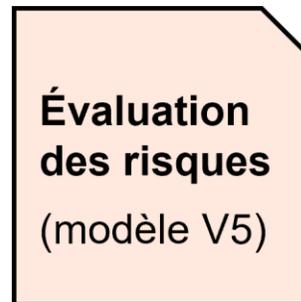


Fournisseur de l'application IS

Gestionnaire d'infrastructure & fournisseur de l'application IS



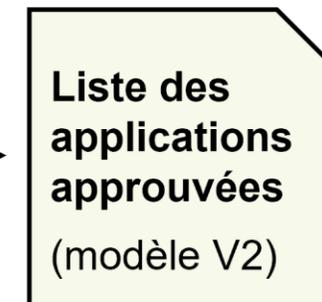
Gestionnaire d'infrastructure



Expert



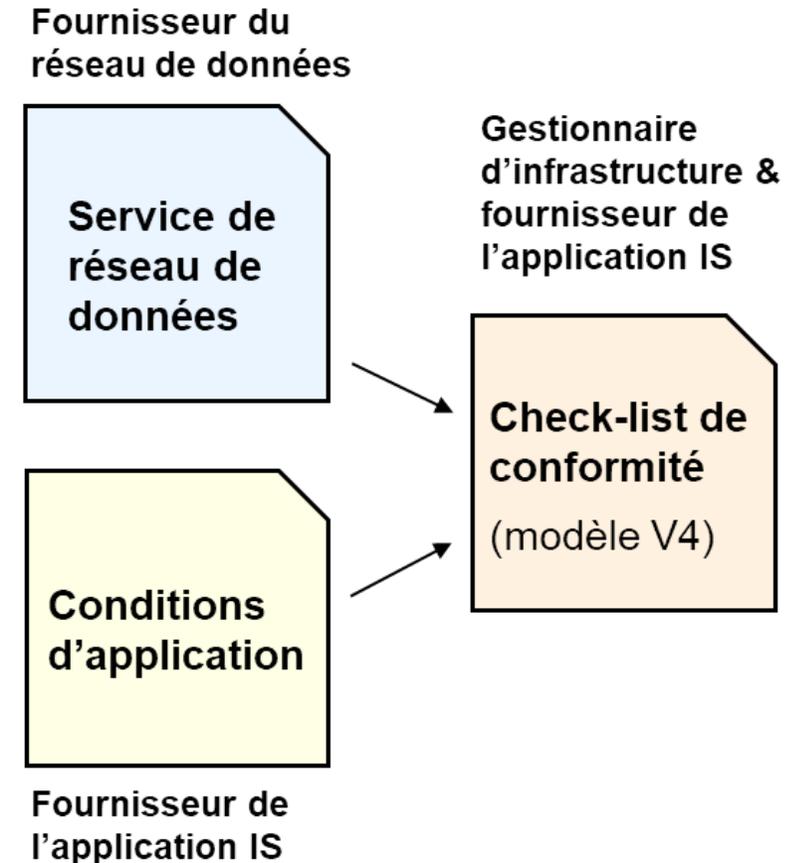
Gestionnaire d'infrastructure



applications ayant été soumises au processus d'approbation

# Check-list de conformité

- La Check-list de conformité permet de vérifier si, dans **l'interaction entre le réseau de données et une application IS donnée**, les conditions d'application sont connues et peuvent être respectées.
- Le document donne une vue d'ensemble des **caractéristiques, restrictions et limites pertinentes d'une application** en relation avec un réseau de données.
- La Check-list de conformité est établie **par le gestionnaire d'infrastructure avec le fournisseur de l'application**.
- Elle est implémentée dans le modèle D-RTE-28100-V4, qui contient un **aperçu des caractéristiques des applications** et une **liste de contrôle des menaces selon la SN EN 50159**.



## 2.1. Caractéristiques de l'application

Le fabricant/fournisseur doit vérifier les informations contenues dans le tableau ci-après. Des commentaires peuvent être ajoutés ou des corrections peuvent être effectuées dans le tableau ou au chap. 0 (en les signalant par un surlignage ou en activant le suivi des modifications).

Item	Caractéristique/valeur	Remarque/évaluation
<b>Identification</b>		
Application	Système de commande et d'information	
Version du système		
Groupe d'applications	Technique de commande ferroviaire	
Type de connexion		
Connexion au niveau du système		
SIL	SIL 2	
Homologation de série		
Statut de planification/d'exploitation	Planifiée/En cours d'examen/En exploitation	
<b>Système de communication de l'application</b>		
Protocole de transmission	Propriétaire	
Protocole sur la couche OSI 4	TCP	
Protocole sur la couche OSI 3	IP	
Protocole sur la couche OSI 2/1	Ethernet	
<b>Conformité à EN 50159</b>		
Aptitude à la classe selon EN 50159 [1]	Classe 1/classe 2	

# Check-list de conformité, modèle V4

## 3. Check-list

Le fabricant/fournisseur doit remplir la check-list de ce chapitre. Des remarques peuvent être apportées au chap. 3.8.

Case cochée = critère rempli

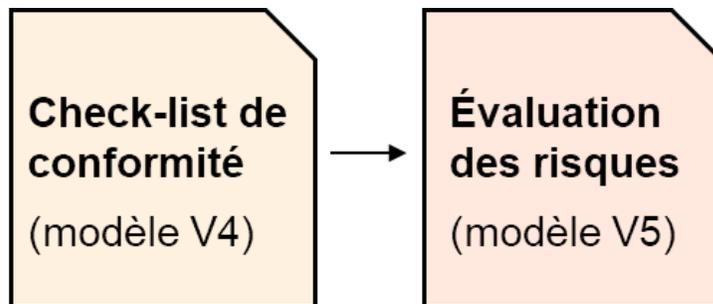
Case non cochée = critère non rempli

### 3.1. Menace de «répétition» selon la norme EN 50159

- Le réseau de données peut générer un nombre indéfini de répétitions, car celles-ci peuvent être interceptées par les mesures de protection de l'application.
- Il n'existe pas de conditions d'application contre cette menace pour le réseau.
- ou
- Contre la menace de «répétition», il existe des conditions d'application ou des restrictions pour le réseau de données:
- conditions d'application ou valeur limite maximale: .....

# Évaluation des risques

- L'évaluation des risques doit montrer que le réseau de données peut remplir les **conditions d'application** recensées par la Check-list de conformité.
- Dans le cadre de l'évaluation des risques, la **sécurité informatique (Security)** est également évaluée.
- Pour l'évaluation des risques, il existe le modèle D-RTE-28100-V5.



## 2.2. Satisfaction des exigences

Les exigences et les conditions d'application, ainsi que leur satisfaction par le réseau de données, sont listées ci-après.

Condition d'application/ID	Exigence (partielle)	Remarque	Satisfaite?
[Condition d'application 1]			
[Condition d'application 2]			
V_Netzw_01	<b>Conditions pour le système de transmission</b>		
V_Netzw_01.A	La qualité de transmission du LAN et du WAN doit...		
V_Netzw_01.B	Le système de transmission fournit suffisamment de bande passante.		
S_System_03	<b>EN 50159 – preuve de conformité</b>		
S_System_03.A	Les connexions réseau (LAN, WAN) doivent satisfaire aux exigences d'un réseau de classe 1 selon la norme EN 50159 ou		
S_System_03.B	aux exigences d'un réseau de classe 2 selon la norme EN 50159 avec la restriction suivante: ...		

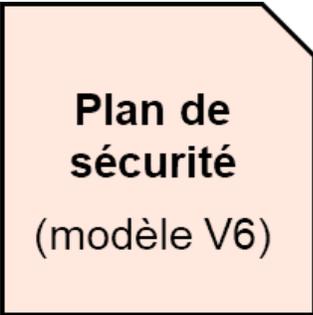
## 2.3. Conflits

Des conflits surviennent lorsque des exigences ne peuvent pas être (intégralement) satisfaites. Sur la base des exigences détaillées énoncées au chap. 2.2, les conflits identifiés sont les suivants:

N°	ID de l'exigence partielle	Problème pour la satisfaction des exigences	Menace
1	S_System_03.B	Des erreurs techniques ou humaines (diaphonie, mauvaise configuration, etc.) peuvent entraîner des communications avec d'autres calculateurs que ceux prévus.	Insertion
2			

# Plan de sécurité

- Le plan de sécurité décrit le contenu du projet, les installations concernées, les rôles et les responsabilités.
- Pour le plan de sécurité, il existe le modèle D-RTE-28100-V6.
- Le chapitre 3 «Garantie de la sécurité» du modèle V6 comprend divers points de contrôle:
  - Évaluation des risques
  - Maturité des spécifications et homologation des produits
  - Utilisation des produits
  - Vérification des documents



### 3.1. Évaluation des risques

N°1	Question		
1	L'évaluation des risques [9] aboutit à des mesures ou à des exigences importantes pour la sécurité.  Si oui: description détaillée	<input type="checkbox"/> Oui	<input type="checkbox"/> Non

### 3.2. Maturité des spécifications et homologation des produits

Les points de contrôle suivants indiquent si la maturité des spécifications et l'homologation des produits sont assurées. S'il est impossible de répondre à tous les points par un oui (= OK), il convient d'indiquer comment la maturité des spécifications et l'homologation des produits seront atteintes.

N°	Question	OK	NOK
2	Le projet concerne exclusivement des produits homologués de série de l'installation de sécurité.	<input type="checkbox"/> Oui	<input type="checkbox"/> Non
	Référence de l'homologation de série OFT: – HdS 512 04 01		
3	La maturité des spécifications est assurée, car aucune ou uniquement <ul style="list-style-type: none"> <li>– des fonctionnalités techniques,</li> <li>– des possibilités de planification,</li> <li>– des processus d'exploitation</li> </ul> ayant été soit <ul style="list-style-type: none"> <li>– explicitement homologués dans le cadre d'une application générique sur la base d'un dossier de sécurité chez le GI, soit</li> <li>– ayant déjà fait leurs preuves dans le cadre d'une application pluriannuelle et à grande échelle chez le GI, sont utilisés.</li> </ul>	<input type="checkbox"/> Oui	<input type="checkbox"/> Non

# Rapport d'examen de l'expert

- Avant la mise en service de l'application, l'expert examine les documents et les justifications concernant le respect des conditions d'application.
- L'approbation de l'application sur le réseau de données n'est autorisée que si les éventuelles conditions du rapport de contrôle des experts sont remplies resp. prises en compte.
- Un rapport d'examen d'expert est établi
  - lors de la clarification préalable à une procédure d'homologation de série
  - avant la soumission des documents d'homologation de série
  - **durant le processus d'approbation**
  - lors de la mise en ligne ultérieure d'autres applications
- Il n'existe pas de modèle pour le rapport d'examen d'expert.



# Liste des applications approuvées

- Le **résultat du processus d'approbation** est repris dans le document «Liste des applications approuvées».
- «La liste des applications approuvées» est envoyée **chaque année à l'OFT** sous la forme d'une mise à jour, mais uniquement si de nouvelles approbations ont eu lieu au cours de l'année écoulée.
- Pour ce document, il existe le modèle D-RTE-28100-V2.

Liste des applications approuvées  
(modèle V2)

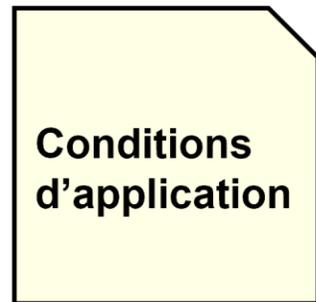
## 2. Applications

### 2.1. Application xy

Identification	
Application	Système de commande et d'information
Version du système	
Fournisseur	
Description de l'application	
Références	Documents complémentaires pertinents
Caractéristiques	
SIL	SIL 2
Aptitude à la classe selon EN 50159 [1]	Classe 2
Conditions d'application	
Résultats du processus d'approbation	
Service de réseau de données	
Check-list de conformité	
Évaluation des risques	
Plan de sécurité	

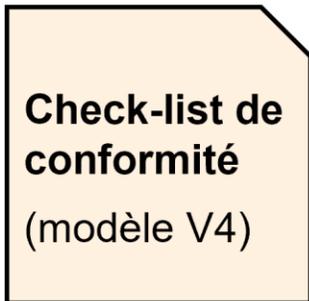
# Processus d'approbation d'applications, récapitulatif

Fournisseur du réseau de données

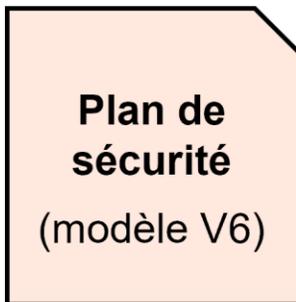
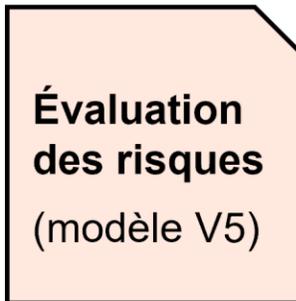


Fournisseur de l'application IS

Gestionnaire d'infrastructure & fournisseur de l'application IS



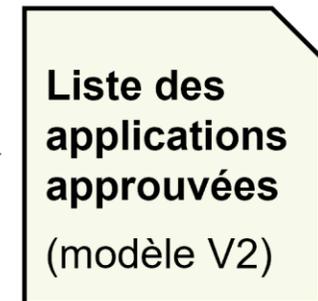
Gestionnaire d'infrastructure



Expert



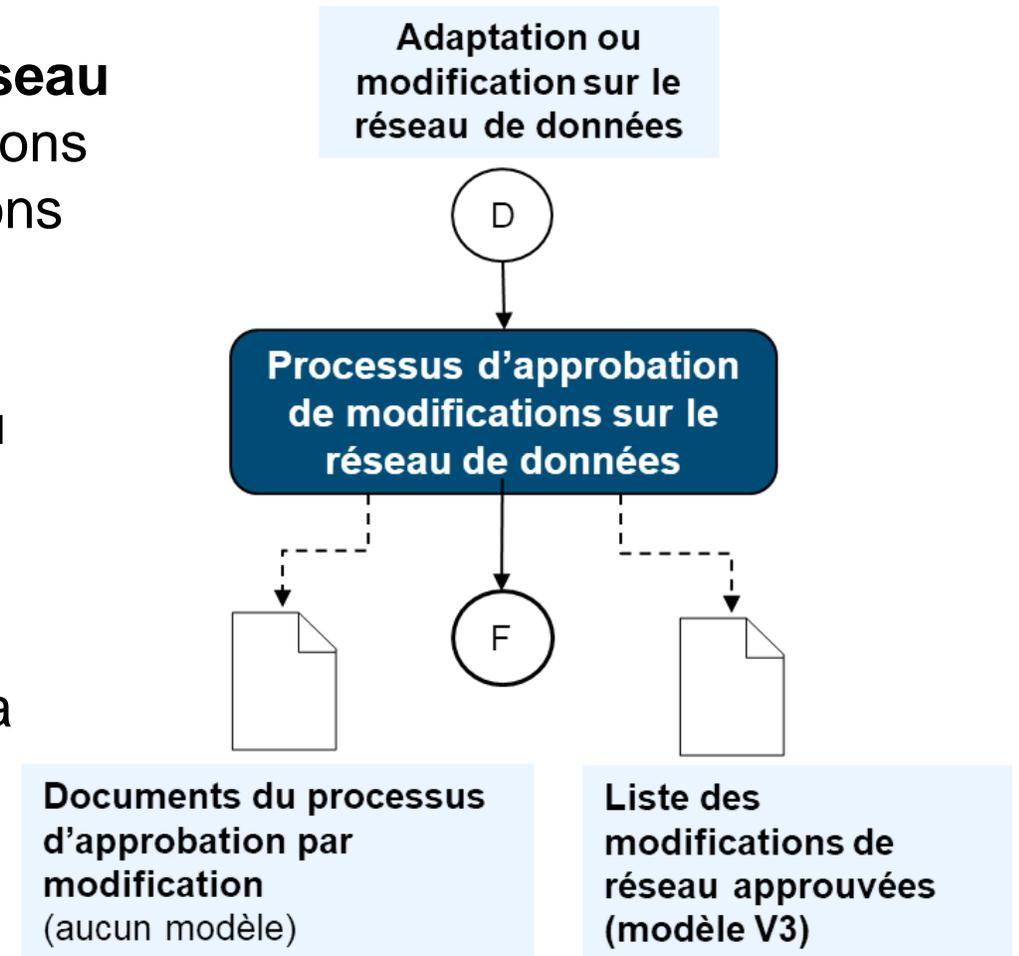
Gestionnaire d'infrastructure



applications ayant été soumises au processus d'approbation

# Processus d'approbation de modifications sur le réseau de données

- Si une **adaptation ou une modification sur le réseau de données** est susceptible d'avoir des répercussions négatives sur la Safety et la Security des applications importantes pour la sécurité, une **évaluation des risques** doit être effectuée pour cette modification.
- Exemples de modifications avec mise en œuvre du processus d'approbation: modification du concept architectural, nouvelle interface vers l'extérieur.
- Il n'existe pas de modèle spécifique pour cette évaluation des risques. Les points de contrôle de la feuille suivante servent de point de départ à l'évaluation des risques.



# Processus d'approbation de modifications sur le réseau de données

## Points de contrôle selon le modèle V3, «Liste des modifications de réseau approuvées», chap. 2.1.2

Une clarification est nécessaire pour tous les points de contrôle auxquels il n'est pas possible de répondre clairement par un «oui».

- a)  Oui  Non Il n'y a pas de répercussions négatives sur la **cybersécurité**.
- b)  Oui  Non Il n'y a pas de répercussions négatives sur la **séparation du réseau** (ou sur la segmentation du réseau).
- c)  Oui  Non Il n'y a pas de répercussions négatives concernant les **menaces selon la norme EN 50159** (répétition, suppression, insertion, reséquencement, corruption, retard, mascarade).
- d)  Oui  Non Il n'y a pas de répercussions négatives sur les **conditions d'application** pour les systèmes importants pour la sécurité ou pour l'exploitation.
- e)  Oui  Non Il n'y a pas de répercussions négatives sur les **retards** (Delays) pour les systèmes importants pour la sécurité ou pour l'exploitation.
- f)  Oui  Non Il n'y a pas de répercussions négatives sur la **disponibilité** pour les systèmes importants pour la sécurité ou pour l'exploitation.

# Liste des modifications de réseau approuvées

- La **modification de réseau vérifiée** et le résultat du processus d'approbation sont repris dans le document «Liste des modifications de réseau approuvées»
- «La liste des modifications de réseau approuvées» est envoyée **chaque année à l'OFT** sous la forme d'une mise à jour, mais uniquement si de nouvelles approbations ont eu lieu au cours de l'année écoulée
- Pour ce document, il existe le modèle D-RTE-28100-V3.

Liste des  
modifications  
de réseau  
approuvées  
(modèle V3)

## 2.1. Modification de réseau xy

### 2.1.1. Aperçu des modifications

Identification	
Titre de la modification	Mise à niveau du logiciel des routeurs MPLS
Description de la modification	Il s'agit d'une mise à niveau du cycle de vie po MPLS. Mise à niveau de .... vers
Objectif de la modification	Le support du fabricant pour le réseau de don Les erreurs sont corrigées. Les failles de sécu traitées. De nouvelles fonctionnalités sont disp
Composants du réseau concernés	Routeurs MPLS
Réseau/sous-réseau concerné	
Documentation de la modification	Notes de mise à jour, analyses d'impact
Références	Documents complémentaires pertinents
Organisation	
Requérant	
Fournisseur de la modification	
Chef de projet du fournisseur	
Chef de projet du GI	
Engineering du fournisseur	
Engineering du GI	
Résultats	
Évaluation des risques séparée (éventuellement)	

# D RTE 28100: Processus d'approbation

## Démonstration de la sécurité des réseaux de données

Safety et Security

Merci beaucoup.



# Questions



# Repas de midi de 12h00 à 13h20

- Menu et boissons non alcoolisées compris dans le prix
- Menu végétarien/végan: voir carte sur la table

## Reprise à 13h30

**En Guete**  
**Bon appétit**



# Programme de l'après-midi

13h30	<b>Pratique</b>
13h30	Projets de réseaux de données des CFF (AiNET) Thierry Bassani
13h45	Projets de réseaux de données du BLS Andreas Klopfenstein
13h55	Projets de réseaux de données des AB Patrick Waldburger
14h05	Projets de réseaux de données du RBS Martin Gerber
14h15	Expériences de l'OFT avec les PAP Patrick Favre, Tobias Hubschmid
<hr/>	
14h25	<b>Pause</b>

# Renouvellement du réseau de données CFF

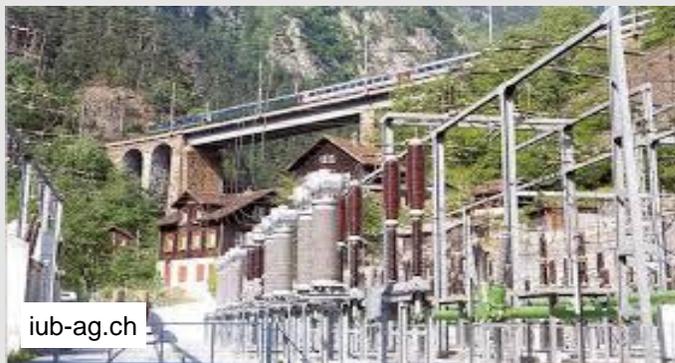
**Mercredi, 11.12.2024**

Thierry Bassani, Jean-Christophe Grandchamp

# Le réseau est au centre de la digitalisation



[mydelade.com.au](http://mydelade.com.au)



[iub-ag.ch](http://iub-ag.ch)



[magiskater.ch](http://magiskater.ch)



[forum.spur-n-schweiz.ch](http://forum.spur-n-schweiz.ch)

# Pourquoi le renouvellement ?

- Le réseau de données en service aujourd'hui nécessite des mesures de rallongement du cycle de vie. Les composants périmés devront être remplacés en 2029 après environ 9 ans de service.
- En raison du développement des centres de calculs et des solutions de sécurité, CFF IT a besoin d'une bande passante accrue (100 Gbit/s et plus).
- Le futur contrôle ferroviaire avec FRMCS (Future Railway Mobile Communication System) et EESA (ERTMS Evolution Sicherungsanlagen) nécessite des nouvelles fonctionnalités dans le réseau de données.



# Le programme AiNET (Intelligent Network)

## Objectifs du programme AINET

- Extension fonctionnelle évolutive et maintien de la substance de l'infrastructure actuelle du réseau de données grâce à des technologies éprouvées, orientées vers l'avenir, évolutives et compatibles avec plusieurs fournisseurs.
- Satisfaction des besoins de CFF IT, FRMCS et EESA
- Mise à disposition des moyens d'exploitation nécessaires/systèmes de gestion pour une exploitation efficace, pour l'amélioration de la qualité du service et la garantie de la disponibilité exigée dans l'exploitation ferroviaire.
- Transition des services du réseau existant vers le nouveau sans perturbations.

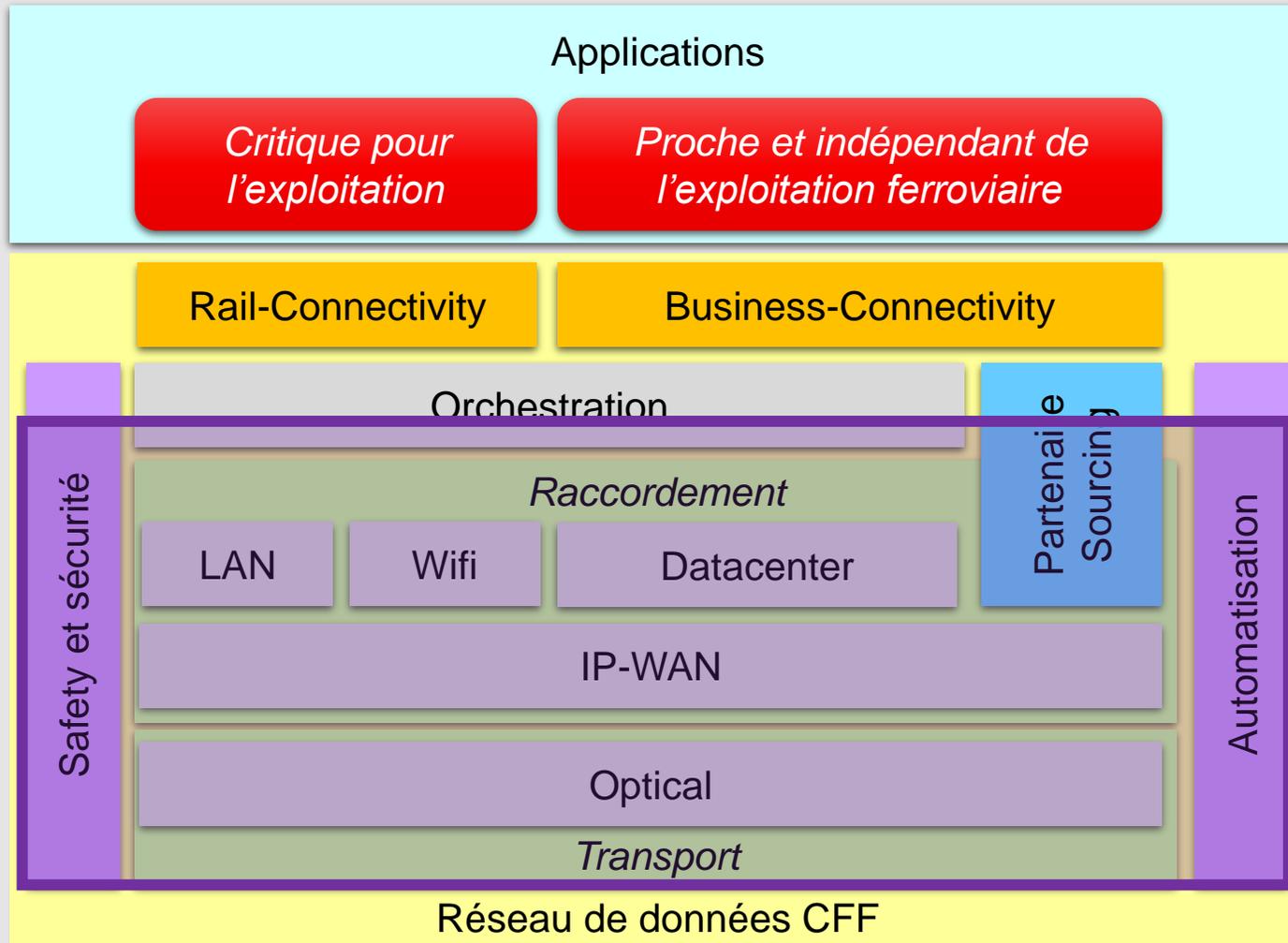
Si le programme AINET n'est pas mis en œuvre, cela aura des conséquences

- Les composants du réseau actuel arrivent à la fin de leur cycle de vie et tombent en panne, ce qui signifie que le réseau de données n'est plus disponible.
- Il n'est pas possible de fournir de nouvelles fonctions pour le contrôle ferroviaire et l'informatique.

L'objectif est donc de **continuer à développer le réseau de données des CFF** et de s'assurer qu'il répond aux exigences actuelles et futures.



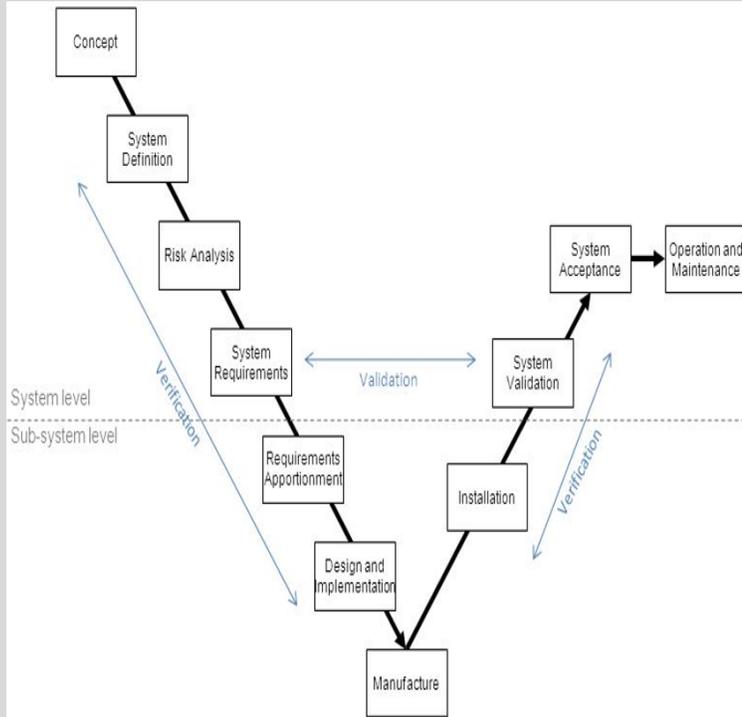
# Architecture





# Gestion des questions de sécurité (safety)

## EN 50126



## EN 50159

electrosuisse >>> Schweizer Norm Norme Suisse Norma Svizzera **SN**

Fachbereich Elektrotechnik **EN 50159**

ENGETRAGENE NORM DER SCHWEIZERISCHEN NORMENVEREINIGUNG SNV NORME ENREGISTRÉE DE L'ASSOCIATION SUISSE DE NORMALISATION

**Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante Kommunikation in Übertragungssystemen**

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission

Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

Diese Norm ist die deutsche Fassung EN 50159:2010

Die Europäische Norm EN 50159:2010 hat den Status einer Schweizer Norm. Sie gilt in der Schweiz als anerkannte Regel der Technik.

Die EN 50159:2010 gilt seit: 01.09.2010.

Für die vorliegende Norm ist das Schweizerische Elektrotechnische Komitee (CES), Technisches Komitee 9 - Elektrische und elektronische Anwendungen für Bahnen - zuständig.

Referenznummer / No. de référence: SNEN 50159:2010(D) Herausgeber / Vertrieber / Editeur / Distributeur: Electrosuisse, Luppenstrasse 1, CH-8320 Fehraltorf, © Electrosuisse 2010-9

## Processus Safety@TC

Seite 1/26

**Änderungsprozess**  
Datennetze@SA

**VÖV UTP** | Verband öffentlicher Verkehr  
Union des transports publics  
Unione dei trasporti pubblici

D RTE 28100

**Nachweisführung**  
**Datennetze**

Safety und Security



## Les thèmes «safety» dans le programme AiNET

1. De quoi a besoin le programme AiNET concernant la «safety» ?
2. Sur quoi le programme AiNET peut compter ?
3. Que doit élaborer le programme AiNET ?



## De quoi a besoin le programme AiNET concernant la «safety» ?

- Processus de validation
- Preuve de la conformité aux exigences des normes et de applications
- Plan «safety», plan RAM, vérification, validation
- Rapport d'examen par un expert en «safety»
- Décision de l'OFT (homologation)

# Sur quoi le programme AiNET peut compter ?

(Déjà grandement élaboré dans le programme Datacom-NG)

- Processus de validation («Processus de modification des réseaux de données@IS»)
- (Pré)contrôle de sécurité pour les phases d'exploitation/cycle de vie (Jalons / Tollgates)
- Analyse des risques pour les nouvelles technologies (Segment-Routing,...)
- Analyse des risques liés aux processus d'exploitation (principe des 4 yeux, ...)

## Que doit élaborer le programme AiNET ?

- Analyse des risques et preuves concernant les nouvelles technologies et la mise en œuvre des solutions
- Preuve selon EN 50159 pour le nouveau réseau de données CFF
- Adaptation des processus d'exploitation pour la Business-Connectivity (sans effets négatifs pour la Rail-Connectivity)
- Adaptation des processus de cybersécurité en cas de modifications de Rail-Net
- Adaptation du «Processus de modification des réseaux de données@IS»

**Danke, merci, grazie**

**Mercredi, 11.12.2024**

Thierry Bassani, Jean-Christophe Grandchamp

A decorative blue vertical line with two white circles at the top and bottom, positioned on the left side of the slide.

# Projet SA-EVO BLS Netz AG

D RTE 28100 Réseaux de données, 11 décembre 2024  
Andreas Klopfenstein, gestionnaire des technologies  
Réseaux et Security

# —○ Programme

1. Contexte  
Technologie SDH en fin de vie  
Réseaux
2. Objectifs visés  
SA-EVO  
Exigences  
Ressources en fibre optique
3. Difficultés
4. Conclusion

# —○ 1. Contexte – Technologie SDH en fin de vie

## Points forts

- Technologie robuste (SDH)  
Topologie en anneau, haute disponibilité

## Points faibles

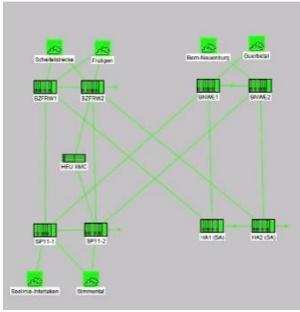
- **Technologie SDH en fin de vie**
  - Matériel de remplacement parfois plus disponible
  - Manque comblé par des démantèlements/limitations
- **Conceptions multiples**
  - Aucune redondance modulaire au niveau du shelf sur le réseau Emme
  - Concept d'alimentation électrique variable en fonction des régions
- **Utilisation de matériel de diverses générations**
  - UMUX 1500/XMC/MileGate
  - Conséquence: complexité et dépendances accrues



# 1. Contexte – Réseaux

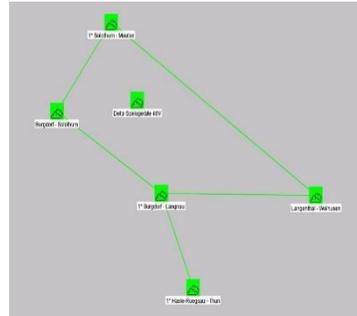


# 1. Contexte – Réseaux

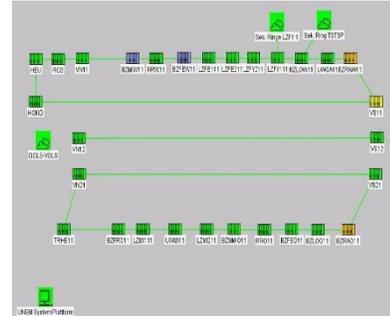


**SA**

Ittis, encl., RCI, rcs95, EC-CC

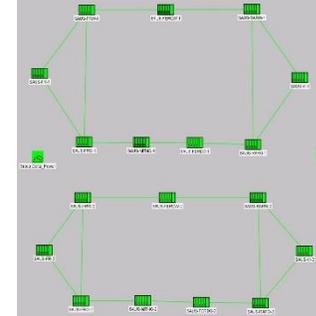


**Emme**



**DT**

GSM-R/BTS



**SAUS**

RBC, encl., etc.

**MileGate**

Convertisseur de sous-débits TKN (v.24, x.35, etc.)

# Objectifs visés

## SA-EVO

Un réseau pour tous les services déterminants pour la sécurité

Ittis

Enclenchement

GSM-R/BTS

Sous-débits

## Exigences

Processus d'homologation RTE 28100 OFT

Dir. CySec-Rail OFT

Fournisseur sécurité de l'information BLS

Fournisseur sécurité de base/projets BLS



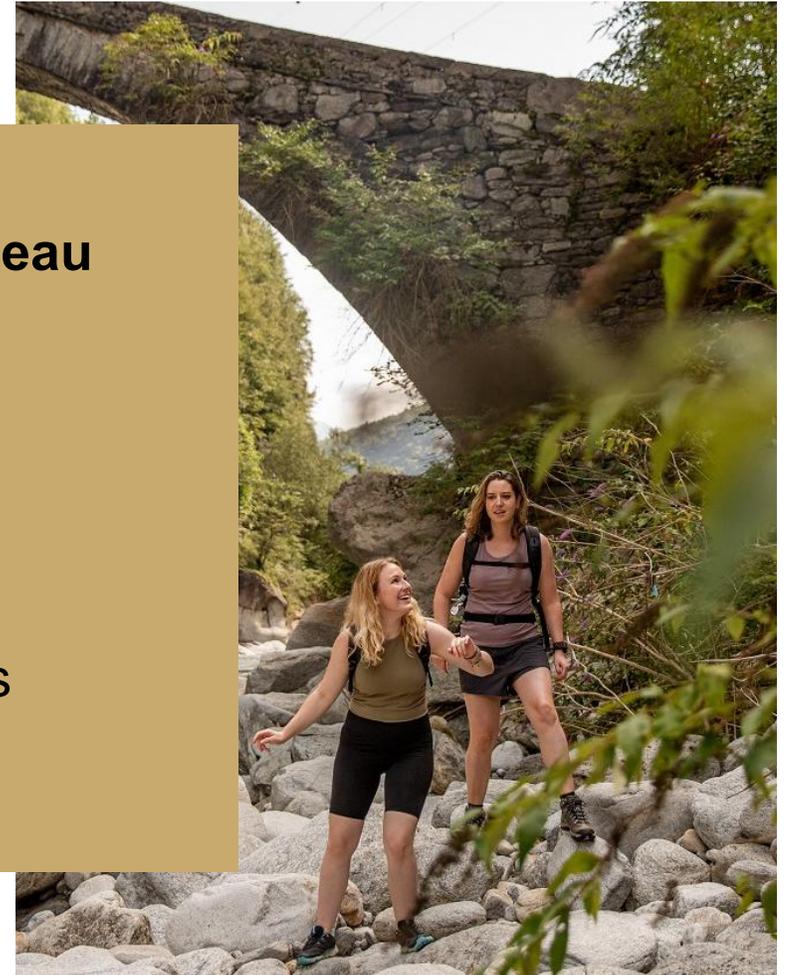
# Objectifs visés

**Appel d'offres indépendant de la technologie du réseau**

MPLS-TP ou IP/MPLS

**Ressources en fibre optique**

- Raccordement défini des sites Access
- Fibre optique avec module BIDI SFP dans les chaînes Access, si possible



# Difficultés

## Sur le plan réglementaire

- Processus d'homologation par service selon la RTE 28100 avec l'OFT
- Respect de la dir. CySec-Rail de l'OFT
- Respect des dispositions du manuel sur la cybersécurité destiné aux entreprises de transports publics de l'OFAE

## Sur le plan technique

- Services de catégorie 1 sur les réseaux orientés paquets (EN 50159)  
EC-CC, rcs95 non autorisés (selon CFF-OFT)



# Conclusion



**Charge administrative très importante pour démontrer la sécurité et satisfaire aux exigences requises dans le cadre des projets**

**«Explosion» des exigences de sécurité dans l'environnement TO**

**Nécessité de posséder ou d'acquérir un savoir-faire**

**La gestion des assets, une opération clé dans un environnement hétérogène (cycle de vie des applications ferroviaires!)  
Qu'y a-t-il dans le réseau?**

**Évaluation des risques basée sur les assets des différentes applications**

A vertical blue line with two white circles at the top and bottom, extending from the left edge of the slide.

# Merci!

BLS SA  
Genfergasse 11  
CH-3001 Berne  
bls.ch

A large, solid pink circle containing white text.

Des  
questions?

# Rapport d'expériences sur le renouvellement du réseau de données

Colloque Réseau de données,  
le 11 décembre 2024

Patrick Waldburger,  
spécialiste Numérisation et réseaux



# Bienvenue!



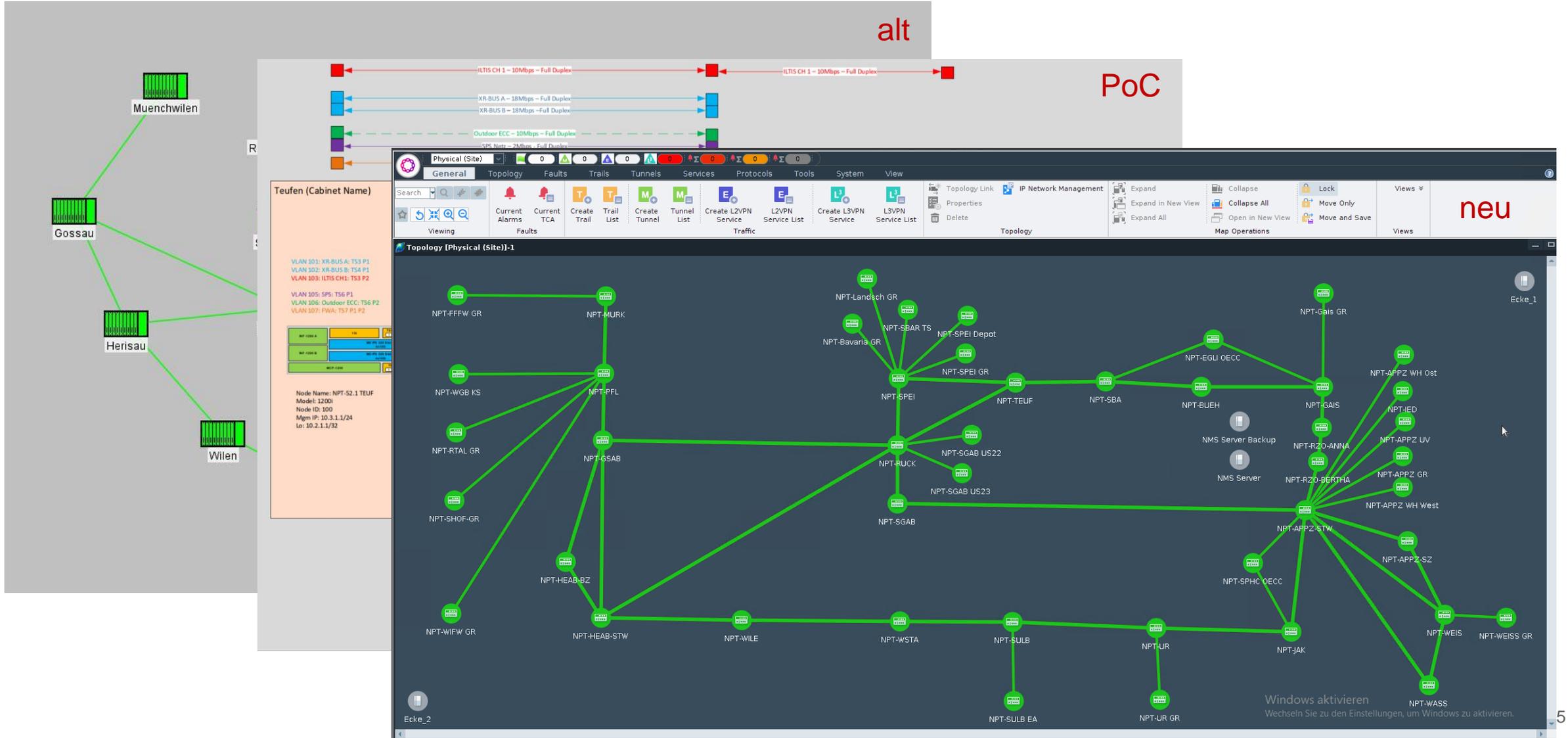
# Plan

- 1. Notre réseau de lignes**
- 2. Réseau de données: processus de mise en œuvre, chiffres et applications**
- 3. RTE 28100: processus et déroulement de projet**
- 4. Conclusions**



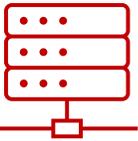


# Réseau de données: processus de mise en œuvre de l'ancien au nouveau



# Réseau de données en chiffres

**6**  
machines  
virtuelles



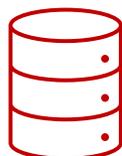
**340**  
points  
finaux de  
services



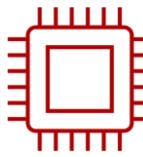
**404**  
tunnels MPLS-TP



**286 GB**  
capacité de  
stockage



**46**  
nœuds de  
réseau



**64**  
services



# Réseau de données: applications

## Réseau de données



### Très important pour la sécurité



Connexions  
entre les postes  
d'enclenchement



Système de  
commande  
intégral



Systèmes de  
comptage des  
essieux



### Base d'intégrité



Information à la  
clientèle, vidéo et  
technique



Guidage à distance de  
la lumière et du  
chauffage des aiguilles



Radio et  
annonces

# RTE 28100 Démonstration Réseaux de données

RTE 28100 pas encore publiée – Homologation de série des Appenzeller Bahnen à titre de projet pilote afin d’acquérir une première expérience dans l’application de la réglementation RTE 28100 – Processus d’approbation défini pour vérifier et documenter le respect de toutes les conditions d’application par le réseau de données tout au long du cycle de vie – Réglementation et aide à la planification et à l’exploitation de réseaux de données pour répondre aux prescriptions souveraines

## Applications ferroviaires

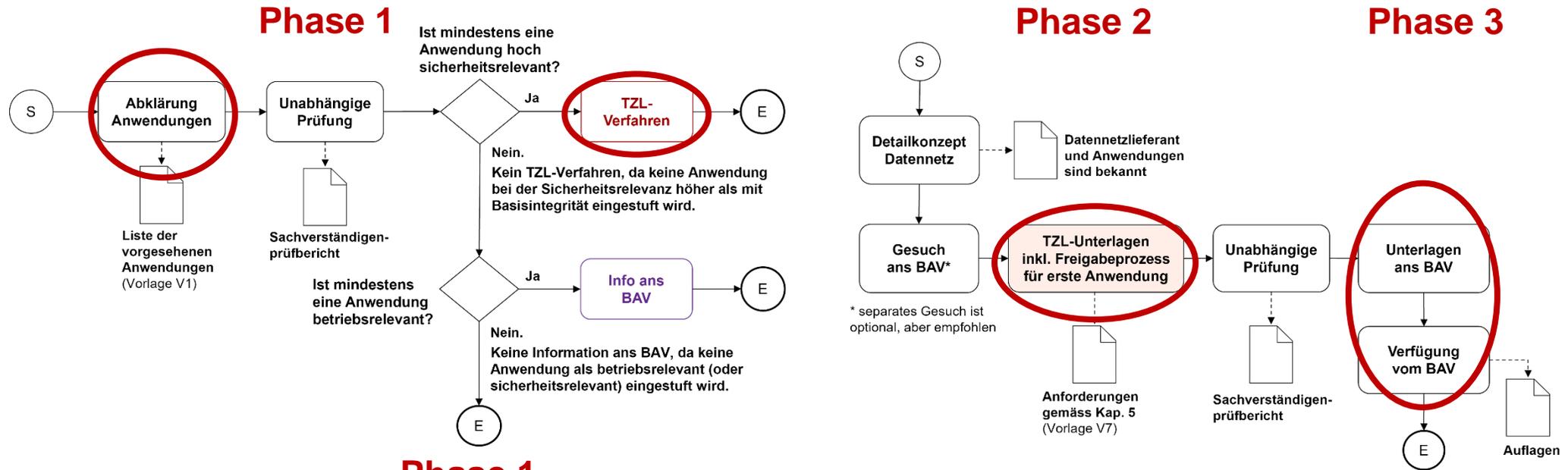


Conditions d’application du fournisseur de l’application ferroviaire au réseau de données



Réseau de données

# RTE 28100: processus



## Phase 1

- Liste des applications → modèle M1
- Examen des applications Homologation de série oui/non → expert

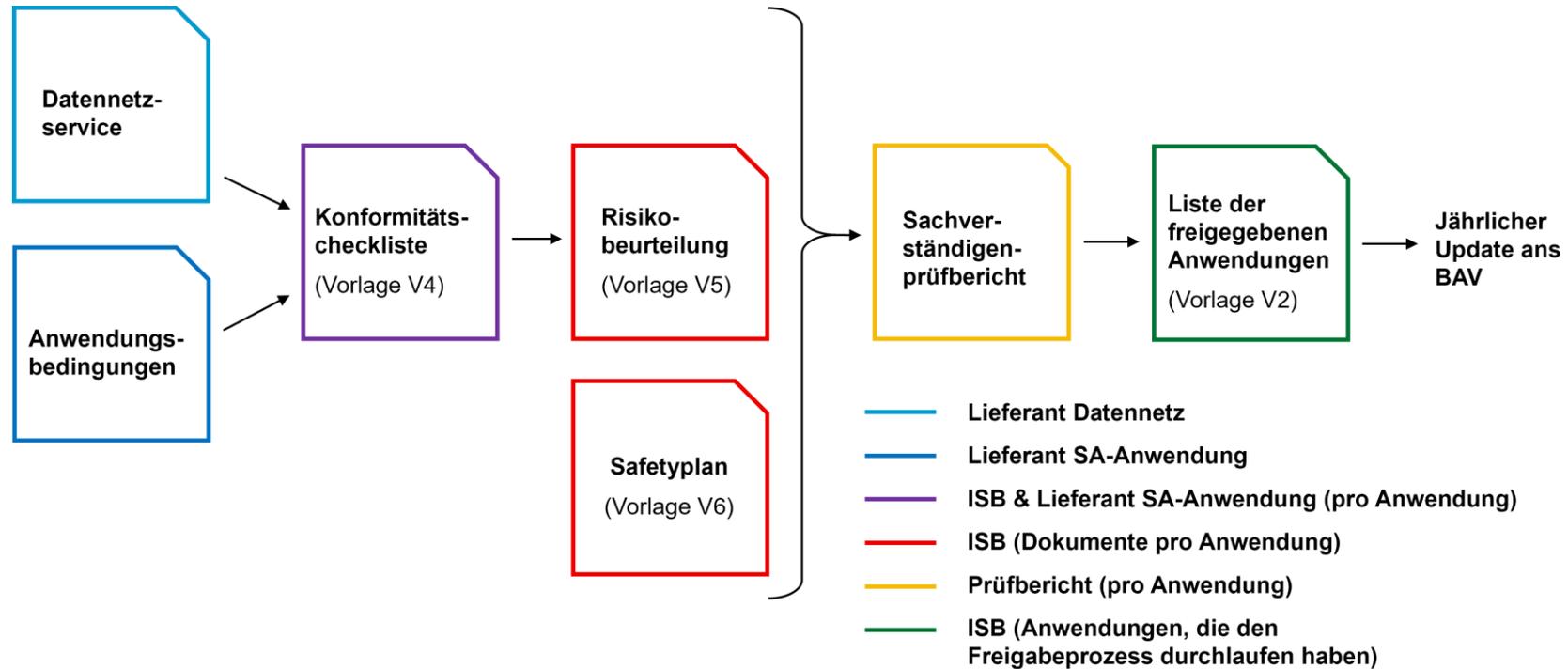
## Phase 2

- Processus d'approbation de la 1<sup>re</sup> application (homologation de série) → modèles M4 à M7

## Phase 3

- Rapport d'examen de l'expert → décision de l'OFT → modèles M2 et M3

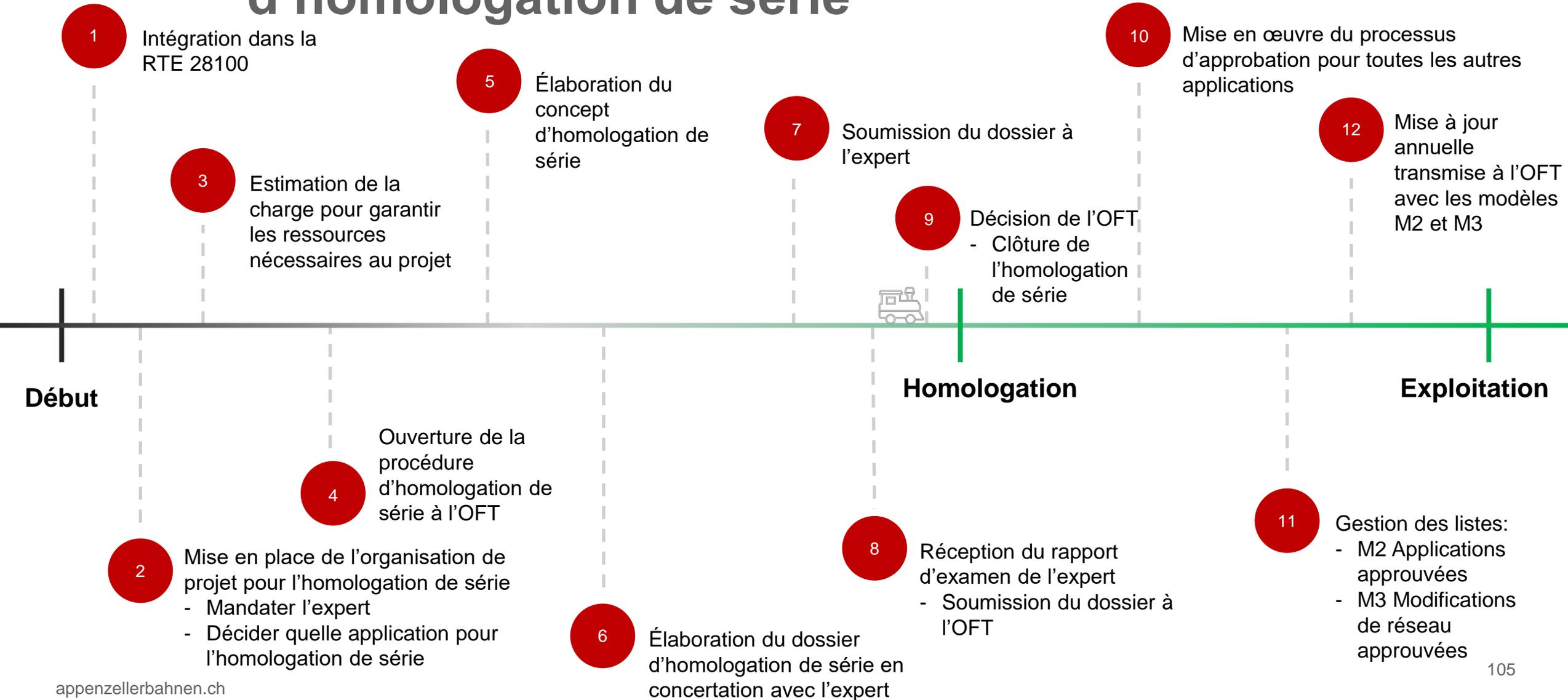
# RTE 28100: processus



## Phase 4

- Processus d'approbation des applications restantes

# RTE 28100: déroulement des projets d'homologation de série



# Expérience de l'application de la RTE 28100

Rapport d'examen de l'expert nécessaire pour lancer la procédure d'homologation de série?

Chapitre 5: exigences normatives relatives au réseau de données

→ Redondance avec la directive sur la cybersécurité ferroviaire

Granularité de l'appréciation des risques et plan de sécurité

Peu d'experts en «réseau de données»

→ Pénurie de ressources à l'avenir?

Des ressources supplémentaires sont nécessaires chez les GI pour mettre en place les processus lors de l'introduction.

Les compétences doivent être assurées en interne par les GI! **Important!**

Coordination des interfaces: spécialiste – application – preuve

**Les applications sont centrales et définissent les exigences relatives au réseau de données.**

Les check-lists de conformité entraînent un surcroît de charge pour les fournisseurs d'applications.

Le processus d'approbation doit être mis en œuvre et consigné chez chaque GI.

Estimation de la charge pour l'homologation de série et le processus d'approbation

La RTE 28100 offre une base complète.

Aide permettant de s'assurer que rien n'a été oublié

Uniformisation de la démonstration





# Des questions?



# Réseau de données RBS

Martin Gerber, chef de projet RBS  
Mark Bischofberger, chef de projet Nokia



# Réseau de données - Projet RBS

**Renouvellement de l'infrastructure 'Réseau de donnée' d'une architecture SDH à une architecture MPLS (protocole MPLS-TP ou IP/MPLS)**

**Calendrier :**

- Appel d'offres: Juillet 2020 (publication)
- Offres: Novembre 2020
- PoC/Pilote: 2021
- Rollout: 2022 à 2024
- Migration: 2023 à 2025

**Spécifications-clés:**

- Réseau de paquets utilisant un contrôle centralisé (MPLS-TP) ou un plan de routage sous-jacent (Base Routing IP/MPLS)
- Disponibilité identique à celle du réseau SDH, temps de basculement en cas d'erreurs similaire à la technologie SDH (50ms)
- Réseau moderne, durée d'exploitation: 12 à 15 ans minimum.

**Migration de toute les applications de RBS pour l'exploitation, y.c. télécontrôle des postes d'enclenchement VBBa**

1. Applications liées à l'exploitation
2. Applications relevant de la sécurité: télécontrôle des postes d'enclenchements

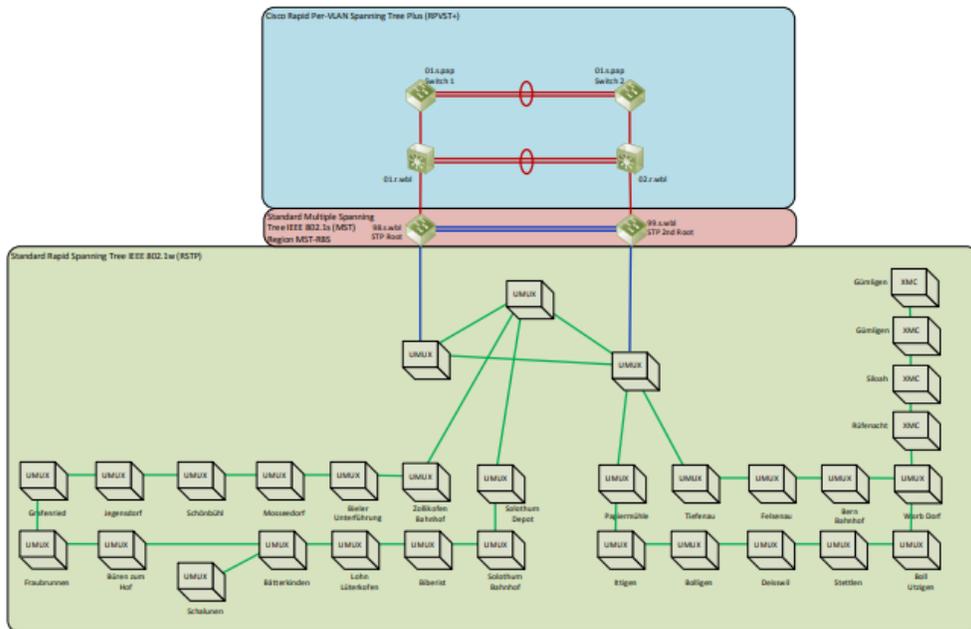
# Réseau de données - Projet RBS – Schéma du réseau

## ❑ Ancien réseau SDH

- ❖ Interfaces E1
- ❖ EoS sur E1/VC12 pour le trafic Ethernet

❑ 2 anneaux 622M (Soleure et Worb, y.c. un anneau de Worb à Muri)

❑ Connexions redondantes vers les 2 DC



## Réseau 'paquets' moderne

❑ Implémentation du protocole IP/MPLS

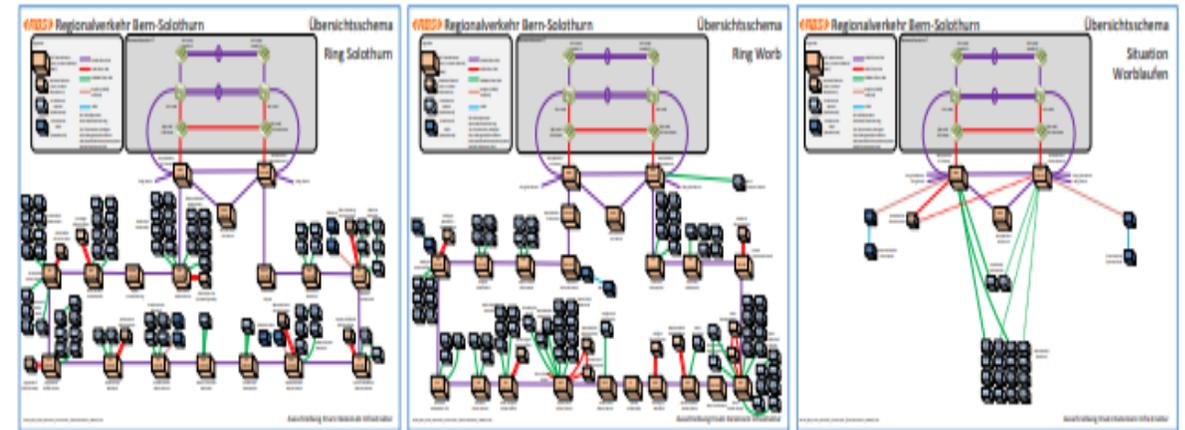


❑ Interfaces Ethernet:  
Transmission du trafic L2 et L3

❑ Réseau 'Postes d'enclenchements' acheminé séparément sur fibres nues (EN550195 Cat1)

❑ 2 anneaux 10G: Solothurn et Worb, retour via Berne

❑ Redondance via des fibres louées



# Réseau de données - RBS – Choix des NEs



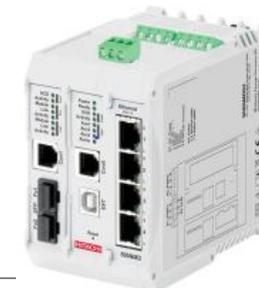
## □ IP/MPLS Routers

- ❖ **3 noeuds principaux (passerelles vers DC):**  
3 x 7250 IXR-R6 avec contrôleurs redondants
- ❖ **Gares:**  
32 x 7705 SAR-8 avec contrôleurs redondants



## □ Switches L2

- ❖ **Switches vers sous-stations DC:**  
~30 Switches L2 durcis pour la connexion des sous-stations de traction 1500VDC
- ❖ **Switches durcis (cabinets):**  
Interopérabilité (ERPS) avec les ~450 switches 'Linerunners' déjà en service



# Réseau de données - RBS

## Caracteristiques & Migration des applications



### ❑ Réseau IP/MPLS

- ❖ Tous les NE redondants, alimentation DC redondante (batteries)
- ❖ Base Routing: IS-IS -> temps de basculement (Switchover): 0 à 50ms avec protocole IP/MPLS FRR

### ❑ Réseau Switches L2

- ❖ Tous les Switches L2 vers les sous-stations DC sont alimentés de manière redondante.
- ❖ Max 4 Unités dans un anneau -> Basculement (switchover): max. 50ms par protocole ERPS oder LAG

## Migration des applications - Calendrier

VBBa Enclenchement s	Télécontrôle Enclenchements SPS	Radio TETRA	Radio Tunnel	Radio KAIROS	Téléphonie SIP	Haut-Parleurs IP KIS	Panneaux affichage IP KIS	Alimentation Traction	Alarmes UPS et Alimentation	Technique (Aiguillages Lumières, etc.)	Video
Sécurité	Exploitation	Exploitation	Exploitation	Exploitation	Exploitation	Exploitation	Exploitation	Exploitation	Exploitation	Exploitation	Exploitation
LAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN
eigene Glasfaser	2024	2025	2024	2024	2023	2023/24	2024/25	2024	2023	2023	2023

# Daten Réseau de données - RBS

## Exploitation et Maintenance



### ❑ Exploitation et Maintenance par RBS et Nokia

- ❖ Support premier niveau géré l'organisation de piquet RBS
- ❖ Support deuxième niveau par Nokia Suisse – Contrat de support et de maintenance 7x24h
- ❖ Support troisième niveau par groupe Nokia – Intégré dans contrat de support 7x24h

### ❑ Délais d'intervention

- ❖ Critical - réaction: 15min - solution: 4h
- ❖ Major - réaction: 1h - solution: 12h
- ❖ Minor - réaction: prochain jour ouvrable

# **D RTE 28100, Expériences de l'OFT avec les PAP, 1<sup>re</sup> partie**

Patrick Favre, Tobias Hubschmid

Berne, mercredi 11.12.2024

# Expériences de l'OFT avec les PAP

## 1<sup>ère</sup> partie:

- «Anciennes» homologations de série Difonet, Rail IP, UMUX/XMC20
- Processus «Änderungsprozess Datennetze@SA» des CFF
- Première utilisation de la D RTE 28100 aux chemins de fer Appenzellois

## 2<sup>ème</sup> partie: Focus security

## «Anciennes» homologations de série

A l'exemple de DIFONET CFF, Rail IP CFF et UMUX/XMC20:

- Le contrôle systématique de la compatibilité des applications avec le réseau avait été formalisé et se faisait de manière **relativement conséquente**.
- L'**implication (théoriquement) systématique de l'OFT** dans la décision de brancher une application au réseau était **peu adéquate**.
- Dans le cas d'UMUX/XMC20, c'est le fournisseur qui s'occupe de l'homologation de série, ce qui peu transparent pour les gestionnaires d'infrastructure.

Il est à supposer qu'un certain nombre de réseaux et d'applications soient passés «sous le radar».

## Processus «Änderungsprozess Datennetze@SA» des CFF

- **Le processus d’approbation a fait ses preuves** et assure un traitement systématique du branchement de nouvelles applications.
- L’investissement jusqu’à l’homologation de série a été très élevé, probablement en raison de la longue phase de recherche de la voie optimale.
- **L’effort pour l’exécution du processus d’approbation** après l’homologation de série est relativement grand. Il est justifié par l’ampleur de la coordination entre les acteurs impliqués (télécom, installations de sécurité, fournisseurs, expert).
- **L’application du processus d’approbation demande beaucoup de compétences techniques**, autant du côté des applications que du réseau.

## Première utilisation de la D RTE 28100 aux chemins de fer Appenzellois

Retour d'expérience après l'utilisation de la D RTE 28100 (aspect safety, en particulier le processus d'approbation):

- **La première utilisation a été couronnée de succès.**
- Les modèles V1 – V7 remplis et le rapport de l'expert permettent à l'OFT de juger le dossier en un temps et avec un coût raisonnables.
- **Une évaluation des risques fondée et bien documentée est fondamentale** si toutes les exigences d'une l'application ne sont pas remplies à 100%.
- Il est fondamental que **le processus d'approbation soit mis en œuvre et pérennisé** par le GI.

# **D RTE 28100, Expériences de l'OFT avec les PAP**

## **2ème partie: Focus Security**

Patrick Favre, Tobias Hubschmid

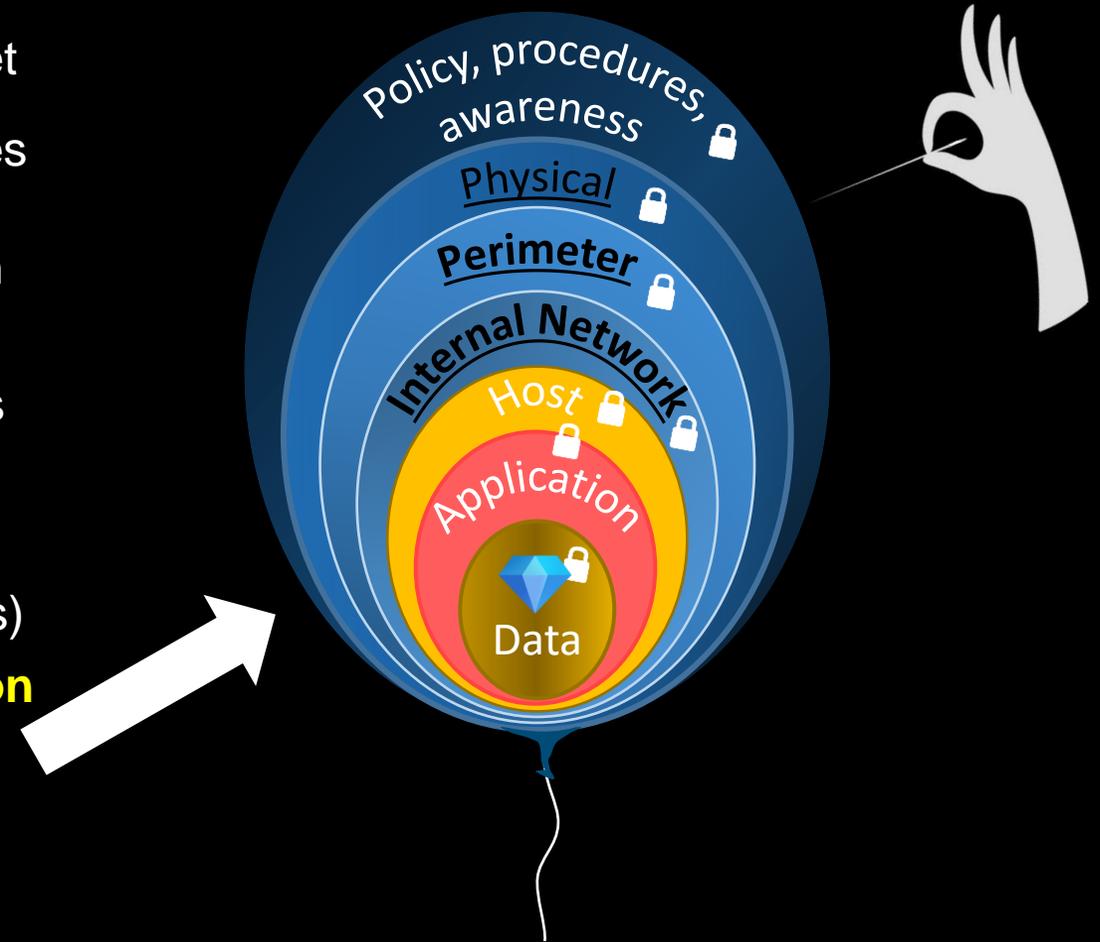
Berne, mercredi 11.12.2024

# Focus Security : Expériences de l'OFT en matière d'activités de surveillance (PAP, HdS, audits)

- 👍 **Sensibilisation** croissante à la cybersécurité dans le secteur. On investit de plus en plus dans la security.
- 👉 **Chantier SMSI**: difficulté de délimiter les activités/mesures dans le projet et les activités SMSI.
- 👉 **Compréhension commune entre la safety** ("never touch a running system") **et la security** (éliminer rapidement les vulnérabilités) souvent encore inexistante.
- 👉 **La gestion des fournisseurs** reste un grand défi. Les rôles et les responsabilités entre le GI et le prestataire de services sont souvent insuffisamment clarifiés et pas assez contraignants.

# Potentiel d'amélioration identifié et facteurs critiques de succès :

- **Compétences et collaboration**: définition claire et communication, y compris documentation des tâches, compétences et responsabilités au sein des différents secteurs.
- La "**visibilité**" a encore un potentiel d'amélioration dans de nombreux réseaux de données, en particulier dans le domaine TO. C'est-à-dire la capacité de pouvoir reconnaître les cyber-attaques en temps réel et d'isoler rapidement les segments de réseau concernés.
- Demander de **l'aide** à des experts techniques expérimentés (promouvoir des experts compétents)
- **Gestion des fournisseurs - c'est ensemble qu'on y arrive !**
- Security : appliquer systématiquement **le principe de «Defense-in-Depth»** (implique «Security by design»). L'infrastructure du réseau de données revêt une grande importance à cet égard.



# Take home message



## Le timing est essentiel :

Se défendre contre les cyberattaques est une question de timing. Cela demande une détection rapide, une limitation des dommages et des procédures de récupération efficaces.\*

Soyez prêt !

Les réseaux de données ont un rôle important à jouer dans la détection des cyber-attaques et dans la limitation des dommages !

\*Lockbit, le ransomware le plus rapide à ce jour, peut selon CISCO Talos crypter 100'000 fichiers de test - soit 53 gigaoctets - en seulement 5 minutes et 50 secondes.

## COURTE PAUSE (15 min)



... reprise à 14h40

# Programme de l'après-midi

14h40	<b>Nouvelles du domaine des installations de sécurité et de la cybersécurité</b>
14h40	Réglementations relatives aux installations de sécurité Urs Walser
14h50	Normes Security - Safety (IEC, CENELEC) Jean-Christophe Grandchamp
15h00	Informations de l'UTP Marcel Schmid
15h10	<b>Clôture</b> Robert Leemann
15h30	<b>Fin du colloque / échanges informels avec les intervenants</b> (trains à prendre dès 16h)

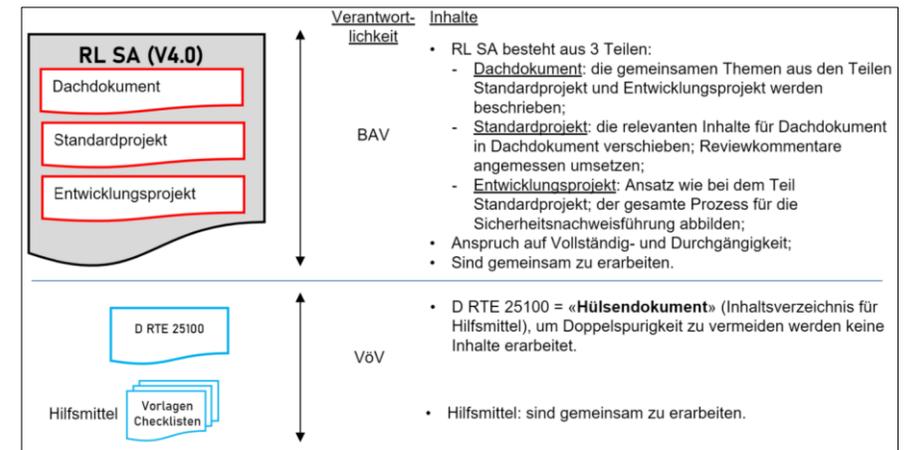
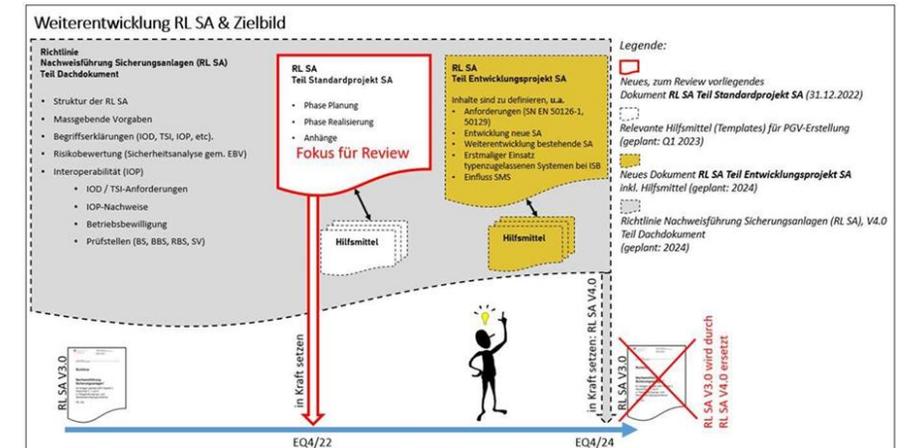
# Règlementations relatives aux installations de sécurité / à la formation en technique ferroviaire

Urs Walser, responsable de projet RTE

Mercredi 11 décembre 2024

# Directive sur les installations de sécurité – D RTE 25100 Démonstration de la sécurité des installations de sécurité

- Développement continu nécessaire
  - Directive de l'OFT «Démonstration de la sécurité: Installations de sécurité», V 3.0, 23 octobre 2015
  - D RTE 25100 «Démonstration de la sécurité des installations de sécurité», 1.5.2016
  - Information de l'OFT sur la directive relative aux installations de sécurité (dir. IS) V 4.0 dans le GE ET au 3<sup>e</sup> trimestre de 2022
  - Consultation d'un projet de l'OFT Directive sur les installations de sécurité 4.0 partie du projet standard au 4<sup>e</sup> trimestre de 2022
  - Mandat de projet commun entre l'OFT et l'UTP sur le développement continu de la directive sur les installations de sécurité et de la D RTE 25100 au 1<sup>er</sup> trimestre de 2023



# Directive sur les installations de sécurité – D RTE 25100

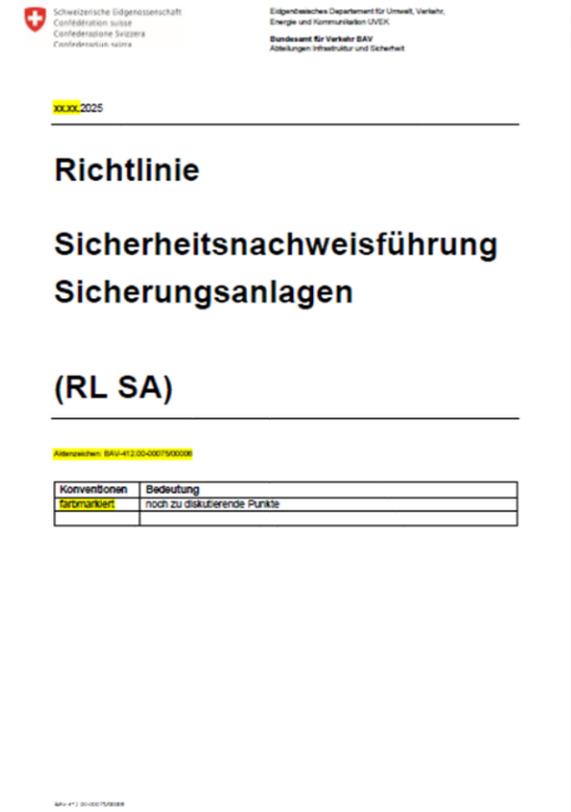
## Démonstration de la sécurité des installations de sécurité

- Direction du projet
  - Dir. IS Martin Gusset, OFT
  - RTE Anne Lehnert, BB
- Groupe de projet composé:
  - de l'OFT
  - d'acteurs de la branche (ferroviaire et industrie)
  - de l'UTP/RTE
- Sous-groupes
  - Projet standard
  - Projet de développement
  - Postes d'aiguillage
  - Cybersécurité

Name	Vorname	Unternehmen		RTE
Bartlome	Marcel	BAV		
Guritanu	Violeta	BAV		
Gusset	Martin	BAV	PL BAV	
Hubschmid	Tobias	BAV		
Studer	Andreas	BAV		
Benz	David	SBB		
Boucher	Adrien	SBB		X
Einer	Stefan	SBB		
Ferrari	Flavio	SBB		
Grünig	Ernst	SBB		
Kajktazovic	Christine	SBB		X
Montani	Mauro	SBB		
Ruch	Peter	SBB		X
Theurillat	Raphael	SBB		
Tomas	Daniel	SBB		
Wermelinger	Roger	SBB		
Hauswirth	Jürg	SOB		
Hofstetter	Roland	Geste		
Huber	Michael	Siemens		
Hurni	Marcel	BLS		X
Lehnert	Anne	Bahnberatung	PL RTE	X
Schenk	Dominic	RBS		X
Veja	Julien	STASIG		
Walser	Urs	VöV		X

# Directive Démonstration de la sécurité: installations de sécurité

- Objectifs du développement continu
  - Cette directive a pour but de répondre aux exigences de l'OCF (chap. 1) relatives à la planification et à la construction des installations de sécurité, qui doivent être approuvées en procédure d'approbation des plans et d'autorisation d'exploiter.
  - Cette directive définit une procédure uniforme pour la démonstration de la sécurité avec les installations de sécurité, et explique
    - quelles directives sont déterminantes;
    - quelles pièces justificatives sont nécessaires pour les installations de sécurité;
    - à quelles exigences ces pièces justificatives doivent répondre en termes de contenu;
    - quelles pièces justificatives doivent être fournies à l'OFT, et quand.



# Directive Démonstration de la sécurité: installations de sécurité

## • Contenu:

- Généralités (document de base)
- Projet standard
  - Une grande partie du contenu de la 1<sup>re</sup> édition de la D RTE 25100 est reprise dans la partie projet standard de la réglementation sur les installations de sécurité.
- Projet de développement
  - Cette partie est nouvelle.
- Annexes

RL SA (V4.0)		
Einleitung über die Struktur und Inhalte der RL SA		
Teil Dachdokument	Teil Standardprojekt	Teil Entwicklungsprojekt
<b>Kapitel</b> <b>1</b> Nennung des Zwecks, Anwendungsbereichs und der Abgrenzung der RL SA. <b>2</b> Beschreibung des Vorgehens zur Projekteinstufung. <b>3</b> Nennung der massgebenden Vorgaben. <b>4</b> Erläuterungen zu den Rollen und Verantwortlichkeiten der Beteiligten. <b>5</b> Erläuterungen zu den Kernthemen des PGV: <ul style="list-style-type: none"><li>• Verfahrensarten und Fristen;</li><li>• PGV-Dokumente und inhaltliche Anforderungen;</li><li>• Risikoanalyse und -beurteilung;</li><li>• Notwendigkeit der Sachverständigenprüfung;</li><li>• Abweichungen von Vorgaben;</li><li>• Bauphasen und Provisoren;</li><li>• Technisch-betriebliche Integration;</li><li>• Signifikante Änderungen;</li><li>• Cybersicherheit.</li></ul> <b>6</b> Konkretisierung zur Notwendigkeit des BbV.	<b>Kapitel</b> <b>7</b> Einleitung und Beschreibung der Phasen und des Ablaufs des Standardprojekts. <b>8</b> Erläuterungen zu den Kernthemen für die Phase Planung des Standardprojekts: <ul style="list-style-type: none"><li>• Anwendungskategorien;</li><li>• Notwendigkeit des PGV und die Art der Sicherheitsachseverfüllung;</li><li>• Sachverständigenprüfung Phase Planung</li><li>• Inhaltliche Anforderungen an die PGV-Dokumente;</li><li>• <b>Plangenehmigungsverfügung.</b></li></ul> <b>9</b> Erläuterung zu den Kernthemen für die Phase Realisierung des Standardprojekts: <ul style="list-style-type: none"><li>• Projektänderungen;</li><li>• Unterlagen und inhaltliche Anforderungen;</li><li>• Projektierung und Montage;</li><li>• Werkprüfung;</li><li>• Sachverständigenprüfung Phase Realisierung;</li><li>• Inbetriebnahme;</li><li>• Abschlussarbeiten;</li><li>• Einzuziehende Unterlagen und Fristen.</li></ul> <b>Anhänge Standardprojekt (S)</b> <b>S1</b> Prüfauftrag an den Sachverständigen für die Phasen Planung und Realisierung. <b>S2</b> Entscheidungshilfe für die Zuordnung der Anwendungskategorie. <b>S3</b> Farbkennzeichnung in den Dokumenten für die Phase Planung. <b>S4</b> Farbkennzeichnung in den Dokumenten für die Phase Realisierung.	<b>Kapitel</b> <b>10</b> Einleitung <ul style="list-style-type: none"><li>• Beschreibung der Phasen und des Ablaufs des Entwicklungsprojekts</li><li>• Erläuterungen zu Gesamtprojekthierarchie, Projektvorbereitung und -vorstellung</li></ul> <b>11</b> Erläuterungen zu den Kernthemen für die Phase Planung des Entwicklungsprojekts: <ul style="list-style-type: none"><li>• <b>Konzept und Systemdefinition.</b></li><li>• <b>Risikoanalyse und -beurteilung.</b></li><li>• <b>Gefährdungsbeherrschung;</b></li><li>• <b>Abweichungen von Vorgaben;</b></li><li>• <b>Produkt Entwicklungsphasen 1 - 4;</b></li><li>• <b>Inhaltliche Anforderungen an die PGV-Dokumentation;</b></li><li>• <b>Planenehmigungsverfügung.</b></li></ul> <b>12</b> Erläuterungen zu den Kernthemen für die Phase Realisierung des Entwicklungsprojekts: <ul style="list-style-type: none"><li>• <b>Projektänderungen;</b></li><li>• <b>Produkt Entwicklungsphasen 5 - 9;</b></li><li>• <b>Technisch-betriebliche Integration der eingesetzten Produkte;</b></li><li>• <b>BbV-Dokumente und inhaltliche Anforderungen;</b></li><li>• <b>Betriebsbewilligung;</b></li><li>• <b>Inbetriebnahme;</b></li><li>• <b>Betriebsprüfung;</b></li><li>• <b>Abschlussarbeiten;</b></li></ul> <b>13</b> Schnittstelle zum Typenzulassungsverfahren <b>Anhänge Entwicklungsprojekt (E)</b> <b>E1</b> Prüfauftrag an den Sachverständigen Stufe Entwicklungsprojekt für die Phasen Planung und Realisierung. <b>E2</b> Prüfauftrag an den Sachverständigen Stufe Produkt für die Phasen Planung und Realisierung.
<b>Begriffserläuterungen und Abkürzungen</b>		

# D RTE 25100 Démonstration de la sécurité: installations de sécurité

- Objectif et contenu
  - Approfondissement pratique de la directive sur les installations de sécurité
  - Informations détaillées concernant les termes et les processus de la démonstration de la sécurité
  - Conseils pratiques pour une documentation correcte et efficace
  - Aides
- Aides concernant la dir. IS
  - Aides adaptées à la nouvelle dir. IS
  - Check-lists:
    - Code couleur
    - Documents projet de développement
  - Modèles:
    - Rapport de sécurité
    - Preuve de sécurité
    - Validation pour la mise en exploitation
    - Déclaration de conformité IOP

# D RTE 25096 Processus de planification des installations de sécurité

- Objectifs
  - Place des installations de sécurité dans des projets ferroviaires et des interfaces possibles avec d'autres corps de métier
  - Classement de la planification de projets d'installations de sécurité dans les processus de planification
  - Définition d'un processus de planification générique pour les projets d'installations de sécurité
  - Meilleure compréhension de la planification des installations de sécurité ainsi que des particularités et de la nécessité d'une coordination avec les autres domaines spécialisés
  - Formation de personnes qui débutent dans ce domaine
  - Aide à la navigation grâce aux principales directives, aux ouvrages de référence en matière de technique ferroviaire connexes et aux processus de planification existants
- Groupe cible
  - Planificatrices, planificateurs et personnes issues d'autres domaines spécialisés qui touchent à des domaines spécifiques aux installations de sécurité

# D RTE 25096 Processus de planification des installations de sécurité

- Contenu
  - Processus de planification générique des installations de sécurité
  - Lot de travail 1: concept
  - Lot de travail 2: définition du système
    - Acquisition et vérification des bases
    - Organisation du projet
    - Description de l'environnement technique et opérationnel
    - Analyse des interfaces
    - Définition d'itinéraires, de vitesses et de signalisation
    - Exigences en termes d'infrastructure
  - Lot de travail 3: projet de construction / projet de construction et de mise à l'enquête
    - Acquisition d'autres bases
    - Planification technique et opérationnelle

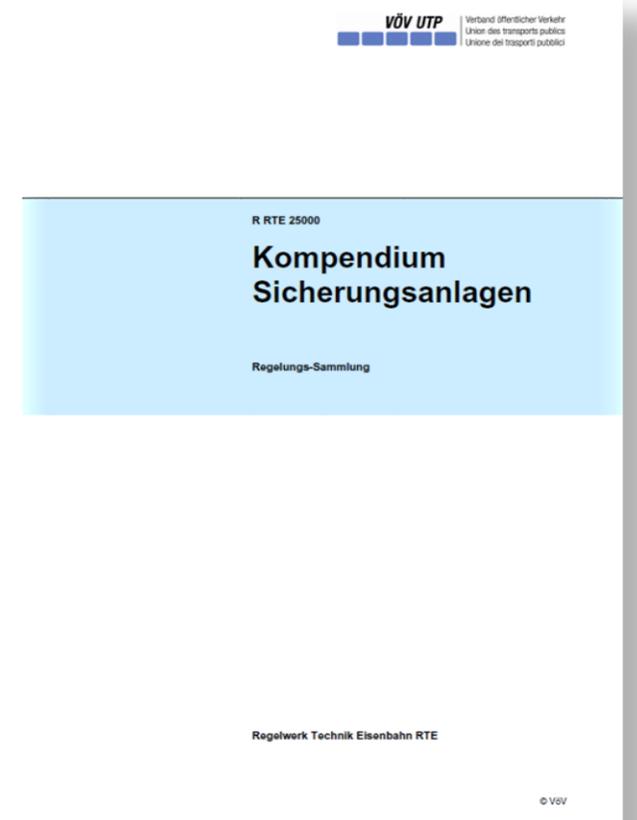


# Autres étapes

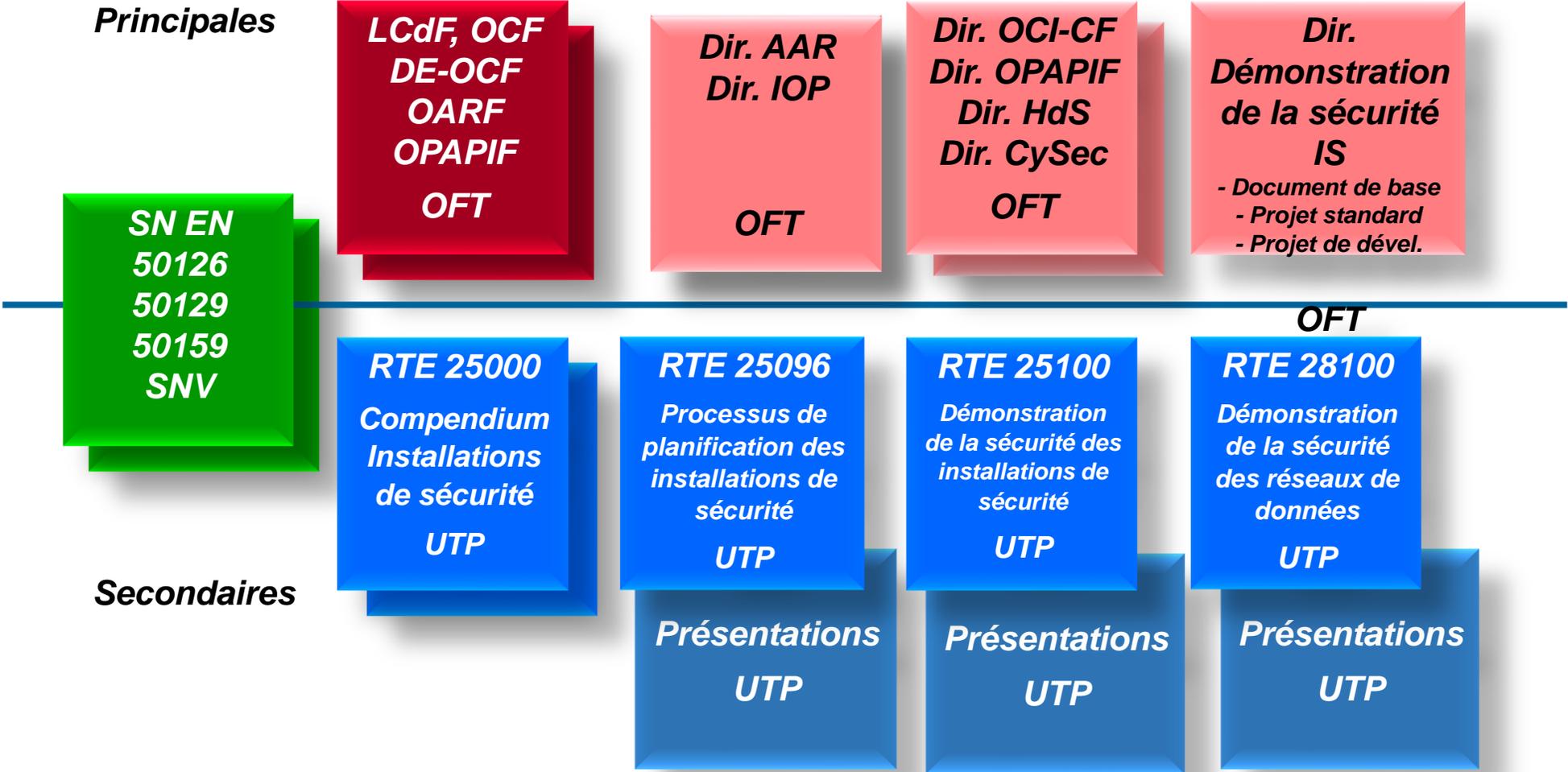
- Calendrier:
  - 1<sup>er</sup> trimestre 2025 Finalisation et révision dans des groupes de projet
  - 2<sup>e</sup> trimestre 2025 Consultation de la directive sur les installations de sécurité 4.0 avec lecture des D RTE 25100 et 25096
  - 2<sup>e</sup> trimestre 2025 Colloque de l'UTP parallèle dir. IS / D RTE 25100
  - 3<sup>e</sup> trimestre 2025 Publication de la dir. IS 4.0  
Publication de la D RTE 25100  
Publication de la D RTE 25096

# R RTE 25000 Compendium Installations de sécurité

- Adaptations dans la 13<sup>e</sup> édition:
  - Sujets plus importants (R RTE 25053, 25056 et 25063)
  - Petites modifications dans 21 autres réglementations
- État:
  - 2<sup>e</sup> lecture au 3<sup>e</sup> trimestre de 2024
  - En cours de finalisation
  - Publication prévue pour le 1<sup>er</sup> mars 2025



# Aperçu des réglementations sur les installations de sécurité



# Formation en technique ferroviaire

- Offre actuelle

Bildung Technik Eisenbahn BTE  
**Bildungsangebote 2024 / 25**

CAS Mechanische Schienenfahrzeugtechnik ZHAW	9/2024
Modul Finanzierung und Abgeltung im öV HSLU	9/2024
CAS en Système ferroviaire HEIA-FR	9/2024
CAS Railway Signalling FHNW	9/2024
CAS Fahrbahn HEIA-FR	9/2024
CAS Bahnbau BFH	10/2024
CAS System Eisenbahn BFH	1/2025
CAS Elektrische Triebfahrzeuge FHNW	2/2025
Lehrgang Projektleitende Fahrstrom SBB	8/2025
MAS Bahnsysteme BFH	

  
voev.ch/bildung-bte

**VÖV UTP**  
Verband öffentlicher Verkehr  
Union des transports publics  
Unione dei trasporti pubblici

[www.utp.chformation-ferroviaire](http://www.utp.chformation-ferroviaire)

# CAS Railway Signalling à la FHNW

- Nouvelle offre de la Haute école spécialisée du nord-ouest de la Suisse (FHNW), à Windisch, en collaboration avec eduRail et l'UTP
- La première édition est en cours, avec 14 participants
  - STADLER 3, STASIG 2, Ing.Büros2
  - BLS 3, RhB 1, SOB 1, SZU 1, VBZ 1
- Les préparatifs pour la 2<sup>e</sup> édition (2025/26) ont commencé.
  - Transmettre l'information aux personnes que cela pourrait intéresser

[www.fhnw.ch/cas-railway-signalling](http://www.fhnw.ch/cas-railway-signalling)



## Inhalte

- **Aufbaumodul Bahnsicherung**  
Sicherheit im Bahnbetrieb, Planungs- und Realisierungsprozesse, Bahnsicherungsgrundlagen, ERTMS, Zulassungs- und Nachweisprozesse.
- **Vertiefungsmodul Zugbeeinflussung**  
ETCS und ZBMS-Systemfunktionen, ETCS On-boardausrüstung und Streckeninfrastruktur, Migration und Zulassung, ERTMS-Strategie, ATO, CBTC und weitere Zukunftsthemen.
- **Vertiefungsmodul Stellwerktechnik**  
Stellwerke und Aussenanlagen, Leittechnik, Spezialanlagen, Assetmanagement, Digitalisierung und Zukunftsthemen.

# Questions sur les présentations



## Normes Security-Safety (IEC, CENELEC)

Matthias Glock, SBB, Infrastructure, NAT, IISO

Jean-Christophe Grandchamp, SBB, Infrastructure, NAT-Telecom

Robert Leemann, Président Groupe d'experts électrotechnique

Mercredi, 11.12.2024

# Normes Security-Safety (IEC, CENELEC)

- Informations générales
- Développement EN 50159
- Développement IEC 63452
- Informations sur EN 50126 et CENELEC TS 50701

R. Leemann

J.-Ch. Grandchamp

M. Glock

R. Leemann

# Normes: Informations générales

- **NORME**

*«Une norme est un document établi par consensus et validé par une institution reconnue. . . .» [SN EN 45020]*

- **Domaine de l'électrotechnique:**

**IEC**

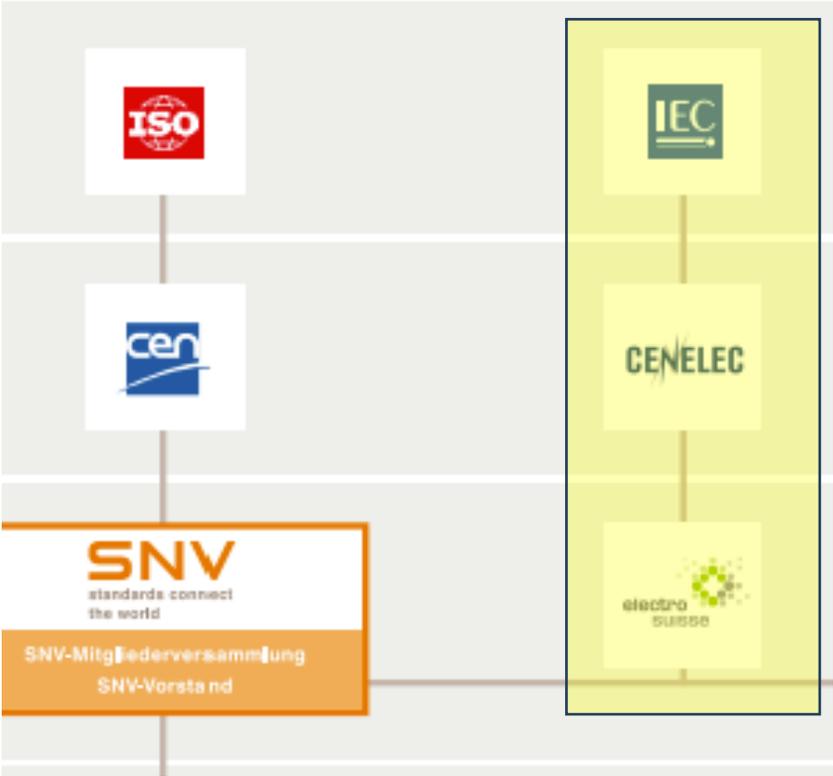
**International** Electrotechnical Commission

et

**CENELEC**

Comité **Européen** de Normalisation Électrotechnique

# Normes: Informations générales



<b>mondial</b>	IEC – TC9	Technical committee 9
<b>à l'échelon européen</b>	CENELEC – TC9X	Technical committee 9X
<b>à l'échelon de la Suisse</b>	TK 9	Comité technique 9 Comité miroir CH

# Normes: Informations générales

- La Suisse, représentée par le CES d'electrosuisse, est membre de la IEC et du CENELEC
- Experts avec affiliation à la branche electrosuisse  
→ Participation aux groupes de travail et aux commissions de la IEC et du CENELEC
- Toutes les normes d'électronique ferroviaire sont gérées au sein de l'IEC TC 9 ou du CENELEC TC9X.  
Le comité miroir est le TK 9.
- TK 9
  - recherche et désigne les experts
  - consolide les retours CH en une prise de position
  - communique les prises de position et les "noms" à Bruxelles ou Genève

# Développement EN 50159 «Communication de sécurité sur des systèmes de transmissions»

Jean-Christophe Grandchamp,  
SBB, Infrastruktur, TC

Membre de CENELEC WG 16 IT-Security

# Développement EN 50159

## État de révision EN 50159

### TC 9X/SC 9XA/WG 16:

2023-05	“Decision to revise -> WG16”
2023-09	“NWIP for EN 50159 Maintenance”*
<b>2024-11-20</b>	<b>“Delivery of ENQ draft”</b>
2025-02-19	“Submission of enquiry draft”
2025-05-14	“Closure of enquiry”

# Développement EN 50159

## Objectif de la révision de la norme CENELEC EN 50159

1. Adaptations à la norme EN 50129
2. Adaptations / Externalisation des sujets de cybersécurité (CLC/TS 50701)
3. Harmonisation des termes techniques pour EN 50129 & TS 50701

# Développement EN 50159

## Les changements de la révision en cours du Cenelec EN 50159 (Non officiel!)

- Les définitions ont été ajustées
- Thèmes de cybersécurité adaptés ou «à l'état de la technologie»
- Référence aux sujets de la TS 50701
- L'architecture de référence a été révisée, orientée vers la pratique
- Des exigences plus compréhensibles de la catégorie 3 (notamment sur la cybersécurité)
- Mise à jour, améliorant la compréhensibilité du «code de sécurité»

# Développement

## IEC 63452 «Railway applications – Cybersecurity»

Matthias Glock,  
SBB, Infrastructure, NAT-TO-SEY,  
Infrastructure Information Security Officer

Membre de CENELEC WG 26 et de IEC PT 63452

# Développement IEC 63452: centre de gravitation

Ce document propose une approche cohérente de la gestion de la cybersécurité des systèmes ferroviaires. Il s'applique à tous les domaines relevant du champ d'application de l'IEC TC 9.

Ce document transpose et adapte les exigences des normes CEI 62443 au domaine des applications ferroviaires et à l'environnement opérationnel, et explique comment ces exigences sont appliquées dans ce contexte.

Il fournit des conseils sur la manière de relier le processus de sécurité au cycle de vie générique pour la fiabilité, la disponibilité, la maintenabilité et la sécurité (RAMS) des normes CEI 62278.

# Développement IEC 63452: Objets de livraisons typiques

- Plan de gestion de la cybersécurité (CSMP)
- Analyse initiale des risques (IRA)
- Analyse détaillée des risques (DRA)
- Système sous considération (SuC)

Rôles, tâches, responsabilités:

- Opérateur, Intégrateur de systèmes, Prestataire de services, Détenteur de droits ferroviaires, ..

# Développement IEC 63452: Discussions

Exemples:

- Intégration de la cybersécurité dans le modèle RAMS (pas judiciaire)
- Responsabilités des fabricants pour les installations existantes
- Rôles multidimensionnels (l'opérateur est aussi un intégrateur de systèmes)
- La cybersécurité n'est pas un add-on à la sécurité (Principles CLC)

Introductions (actuellement par les CFF et l'OeBB) :

- Points de déclenchement de la cybersécurité et de la réglementation
- Clarification Taxonomy (Solution, Application, System) ne correspond pas à SUC

**Merci.**

**In the world of OT Cybersecurity, being ready isn't enough—  
you must be On Time!**



# Informations EN 50126 und TS 50701

Robert Leemann,  
Président, Groupe d'experts électrotechnique

(SBB, Regulation)

Membre CT 9 (SC9XA)



# Questions sur les présentations



# Informations de l'UTP

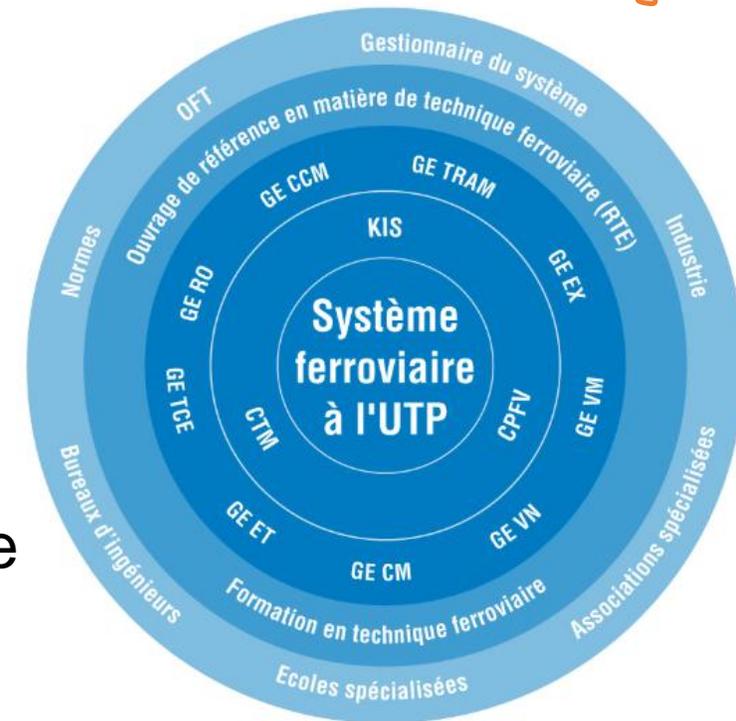
Marcel Schmid, Chef de projet système ferroviaire

**Mercredi 11 décembre 2024**

# Informations de l'UTP

Publication  
mi-décembre 2024

- **Newsletter Système ferroviaire**
- Manifestations: agenda de l'UTP, colloque sur la cybersécurité 2025, cours de construction de voies ferrées à crémaillère, etc.
- Programme d'encouragement de l'OFT
- Plateforme de normes de l'UTP
- Réglementations des CFF
- Gestionnaire de système Communication ferroviaire  
Désactivation du réseau mobile 3G!
- etc.



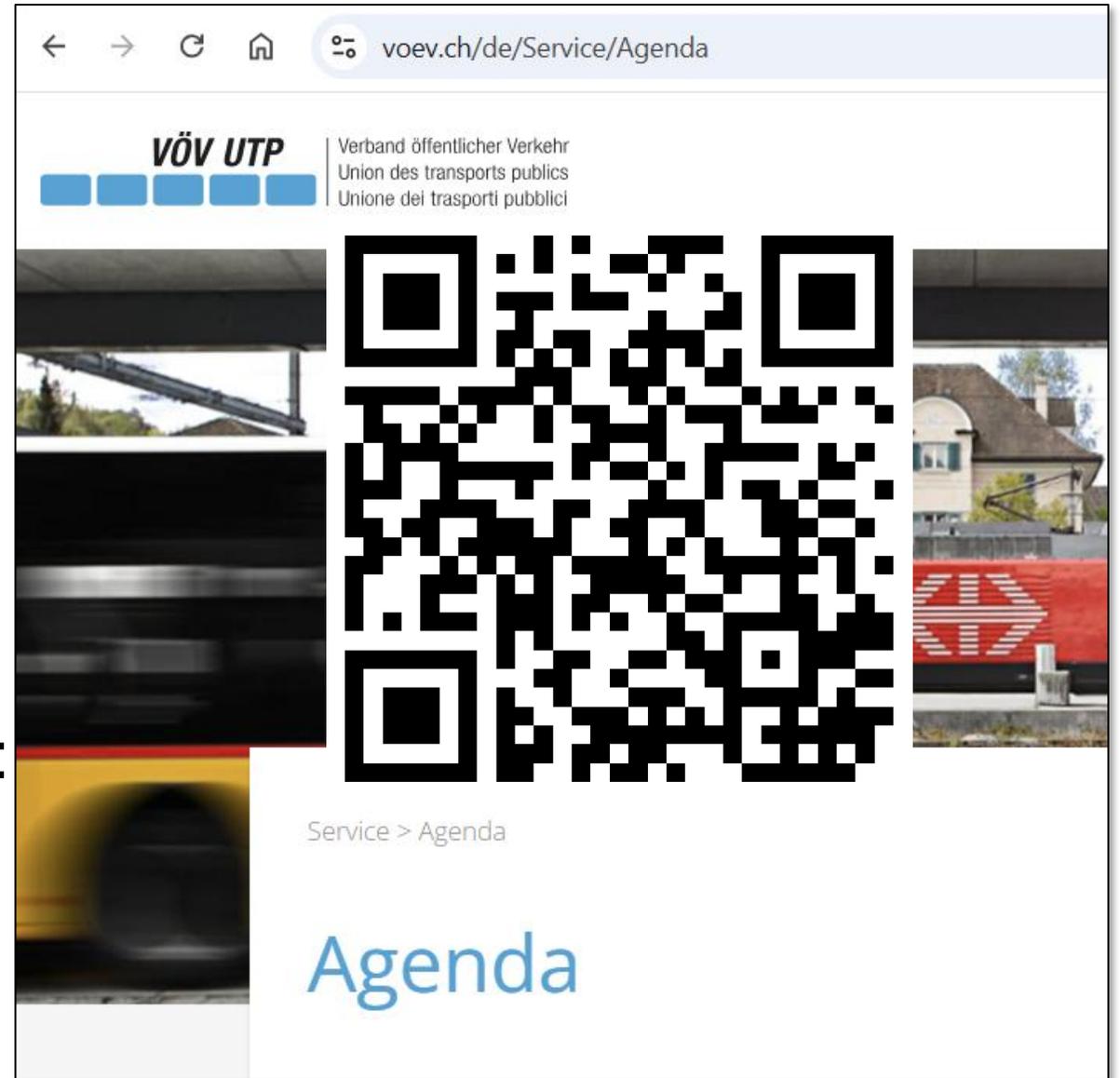
# Dates à retenir

## Agenda de l'UTP

- Colloques
- Cours
- Autres manifestations

Aperçu des dates importantes ici:

[www.utp.ch/manifestations](http://www.utp.ch/manifestations)



# Agenda de l'UTP

- Réserver
  - Ajoutez la date à votre calendrier Outlook.
- Liste d'invitation
  - Inscrivez-vous sur la liste des personnes intéressées et vous recevrez un e-mail dès que les inscriptions sont ouvertes.
- Inscription
  - Lien direct vers la plateforme d'inscription

## Colloque réseaux de données

D RTE 28100 Démonstration de la sécurité Safety et Security, exemples pratiques

> Inscription

## La mobilité et les transports publics de demain

> Réserver < Liste d'invitation

# Colloque sur la cybersécurité des technologies de l'information et des technologies opérationnelles

- L'organisation du colloque 2025 a commencé.

- Date: **le 25 juin 2025**
- Lieu: **dans la région de Berne**

- Programme sommaire / participants

**Matinée: Présentations (ouvertes à tous)**

**Après-midi: Ateliers pour les employés des chemins de fer**

- Sujets: **Feed-back sur le colloque de 2024 et actualité 2025**

*Réservez la date  
et notez-la dans  
votre agenda UTP.*



# Séances de groupes d'experts élargies à d'autres participant(e)s

- Ponctuellement, des séances de groupes d'experts sont ouvertes à un cercle élargi de participant(e)s.
- Généralement, une fois par année
- **Les expert(e)s des entreprises ferroviaires sont invité(e)s à participer à ces séances élargies.**
- **Une occasion à saisir!**
- **Donne un aperçu direct du travail du groupe d'expert(e)s en question**



# Séances de groupes d'experts élargies à d'autres participant(e)s

## Groupe d'expert(e)s Électrotechnique

Sujets touchant aux domaines suivants:

- courant de traction,
- 50 Hz,
- et techniques des installations de sécurité
  
- GT Éclairage, Passages à niveau, Cybersécurité des technologies de l'information et des technologies opérationnelles (en planification)

Une «séance ouverte» est prévue.

- Date: le 23 janvier 2024
- Où: à Wallisellen

Condition de participation: Employé d'une entreprise ferroviaire (membre de l'UTP)

- En cas d'intérêt, écrire à: [Marcel.schmid@utp.ch](mailto:Marcel.schmid@utp.ch)



# Séances de groupes d'experts élargies à d'autres participant(e)s

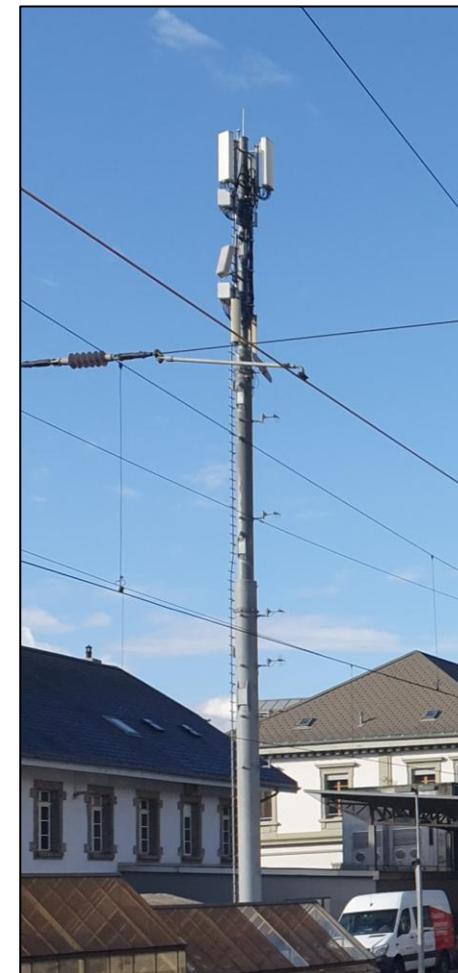
## Groupe d'experts en communication mobile

Sujets touchant aux domaines suivants:

- Communication ferroviaire mobile
- Gestionnaire de système Communication ferroviaire
- Radios dans les tunnels
- ERTMS – FRMCS
- GSM-R
- Autres systèmes radio

Une «séance ouverte» est prévue

- le 23 janvier 2024, au secrétariat de l'UTP, à Berne.
- Condition de participation: Employé d'une entreprise ferroviaire (membre de l'UTP)
- En cas d'intérêt, écrire à: [Marcel.schmid@utp.ch](mailto:Marcel.schmid@utp.ch)



# Questions sur les présentations



# D RTE 28100 Démonstration de la sécurité des réseaux de données

- Tâches accomplies
  - Publication: 1<sup>er</sup> septembre 2024
  - Colloque: 11 décembre 2024
- Prochaines étapes selon les besoins de la branche
  - Formation RTE (groupe cible, contenu, étendue, etc.)
  - Groupe d'échange d'expériences UTP (échange périodique)
  - Groupe de projet RTE
    - Adaptation des modèles à court terme
    - Adaptation de la réglementation à moyen terme
  - RTE Réseaux de données dans les véhicules, y compris les interfaces
  - ...



# Remerciements

- ✓ Merci à Monsieur F. Fellay, ingénieur en électricité diplômé de l'EPF, d'avoir remarquablement traduit les textes
- ✓ Merci à tous les intervenants d'avoir préparé et présenté les thèmes
- ✓ Merci aux membres de l'UTP en charge de l'organisation Nicole Reinhard, Marcel Schmid, Urs Walser et tous les autres pour l'image, le son, la nourriture et les boissons!
- ✓ Merci à toutes les personnes qui ont participé à ce colloque pour leur attention et leur engagement

# Trois requêtes pour conclure

## 1. **Feed-back – nous cherchons à nous améliorer en permanence**

Vous recevrez un sondage par courriel

- Nous invitons toutes les personnes insatisfaites à nous expliquer précisément ce qui leur a déplu sans en parler autour d'elles
- Nous invitons toutes les personnes satisfaites à en parler autour d'elles, y compris à nous

## 2. **Casques**

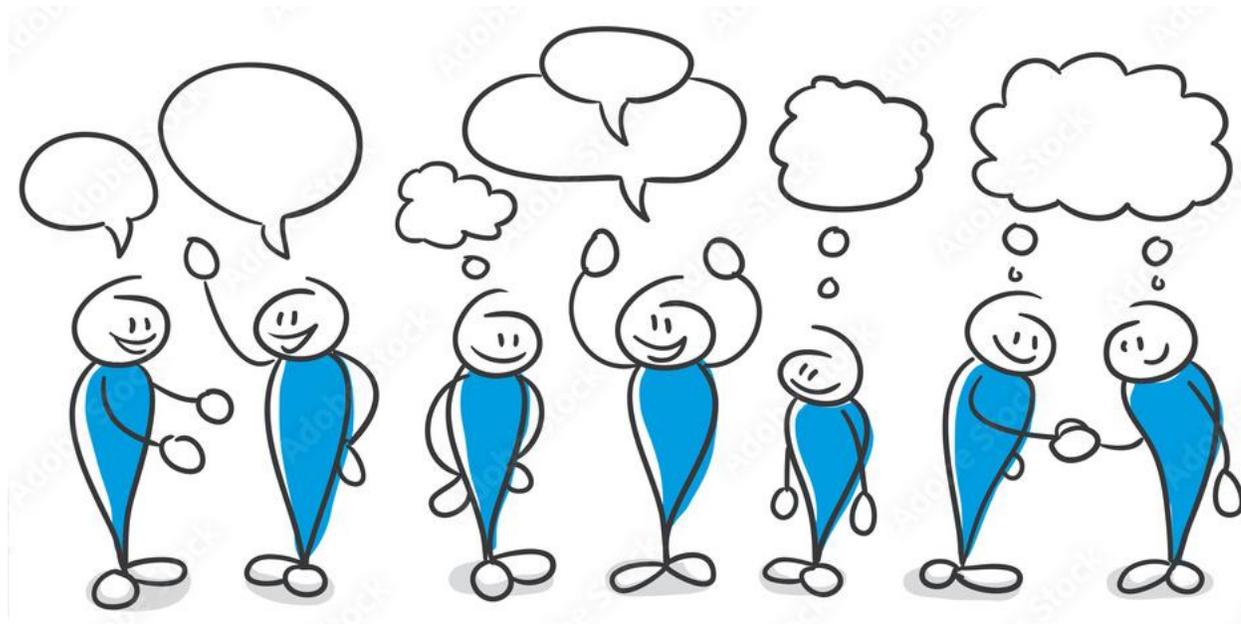
Merci de les déposer à l'entrée

## 3. **Poursuite des échanges**

De nombreux experts sont présents parmi nous aujourd'hui. Profitez de l'occasion pour leur parler et leur poser des questions.

Beaucoup de trains circulent encore à 16h30 et 17h00 au départ de Berne...

# Invitation à un temps d'échange informel autour d'un café et d'une part de gâteau



... puis bon retour chez vous

**RÉSERVE**

# Caractère contraignant des réglementations RTE

- ❖ Principe  
Les réglementations RTE sont des recommandations non contraignantes de l'UTP à l'intention des entreprises membres.  
→ Le choix est laissé aux directions pour chaque édition.
- ❖ Des réglementations RTE peuvent être convenues dans le cadre des contrats.
- ❖ Un office peut également déclarer une réglementation RTE contraignante.