SBB CFF FFS

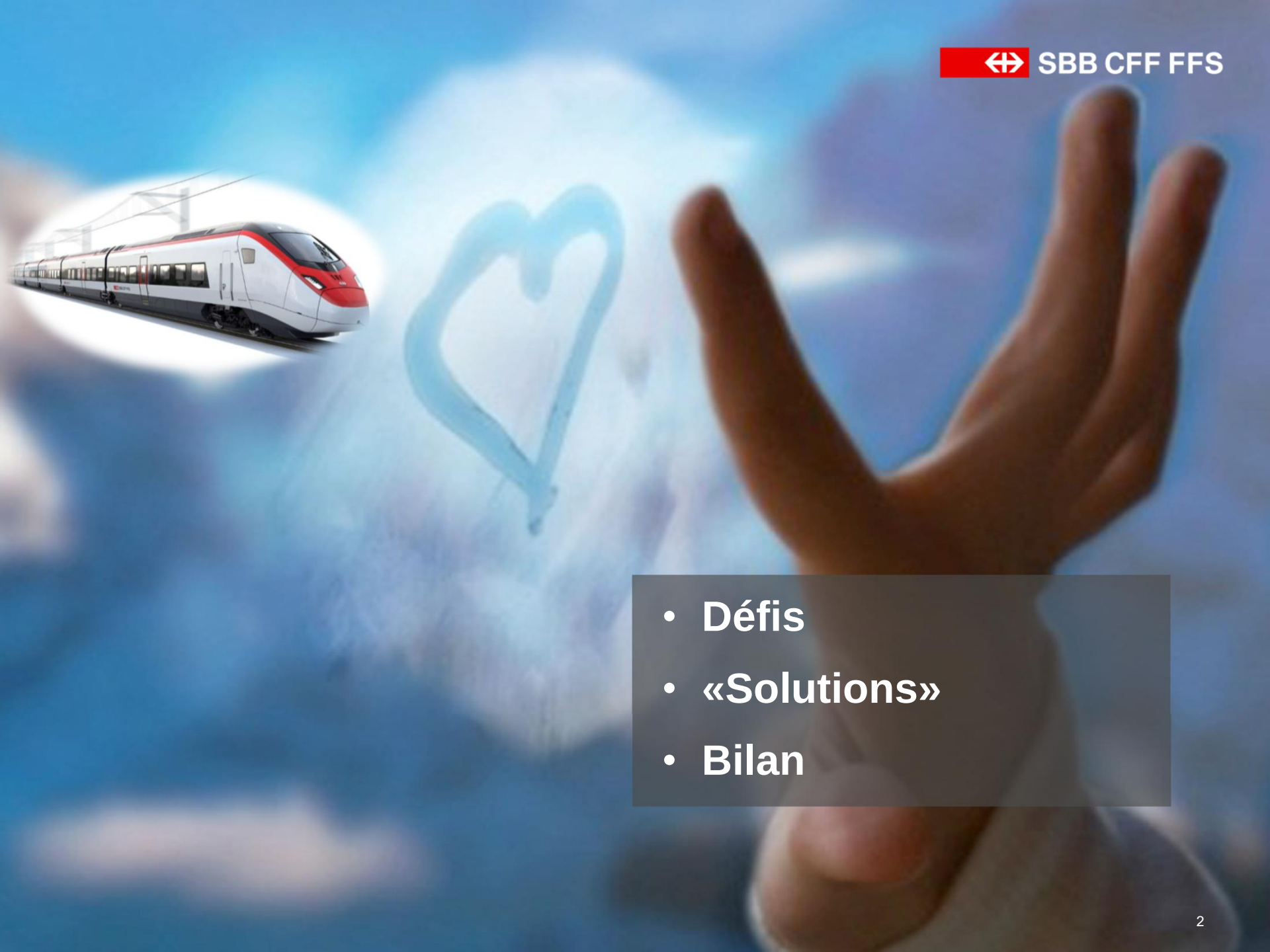
IT Security In Bewegung

«Protection des infrastructures et des systèmes sensibles»

Marcus Griesser, CISO
CFF
Berne, Octobre 2018

RAILplus
Die Meterspurigen
La voie métrique
A scartamento metrico

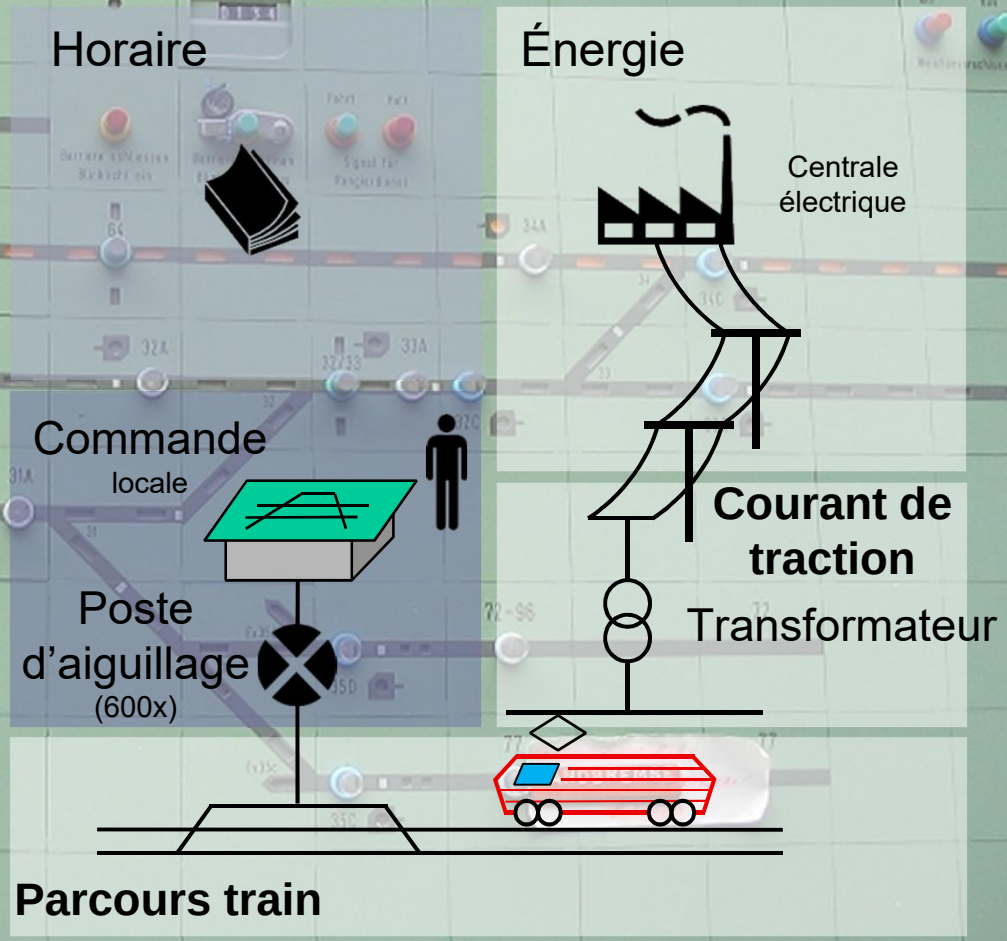
Sécurité et risques


SBB CFF FFS
• Défis
• «Solutions»
• Bilan


SBB CFF FFS
Les infrastructures critiques des chemins de fer.
3 réseaux pour un sillon.
Réseau de télécommunications
IT
Réseau d'énergie
Objectif pour les clients:
Mettre à disposition une grande capacité de sillons
[Nombre élevé de trains qui circulent de manière rapide, sûre et ponctuelle sur les voies.]
Réseau ferré

SBB CFF FFS

L'électronique avant le béton.
Augmentation de l'efficacité grâce à l'automatisation.

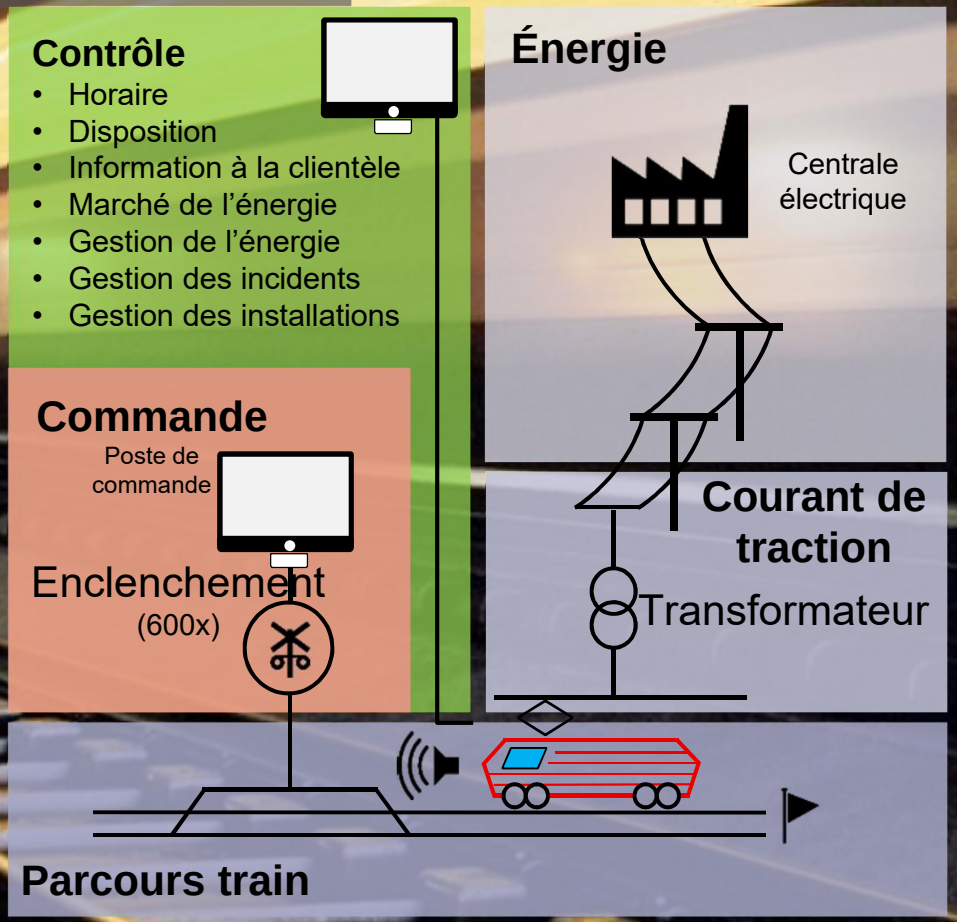


1980

- L'homme en tant que lien entre les niveaux
- Îlots de production autosuffisants

SBB CFF FFS

L’électronique avant le béton.
Augmentation de l’efficacité grâce à l’automatisation.



2018

- Exploitation centralisée
- Solutions de repli interrégionales

Les défis pour les entreprises

Cela fragilise également «l'ensemble du système ferroviaire»

Rencontre de différentes cultures (p. ex. les disciplines de l'ingénierie et de l'informatique)

Cycles de vie différents -> Diversité des systèmes -> Augmentation

Évolution des structures des réseaux – Accroissement de l'interconnexion et de la centralisation

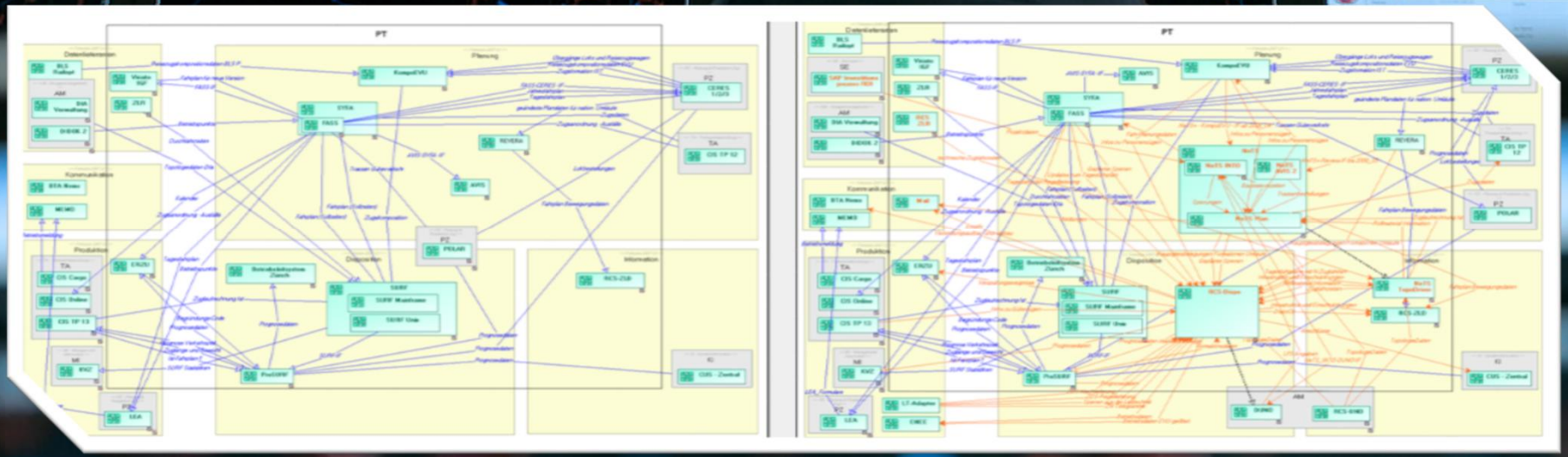
Utilisation accrue de matériel et de logiciels standardisés

Risque plus élevé d'accumulation d'erreurs

La maîtrise de la complexité

commence par la connaissance des interfaces de l'intégralité des systèmes et de leurs interdépendances. (Transparence)

Complexité générale avant	Complexité générale après
p. ex. avant l'introduction du «nouveau système d'horaire»*	p. ex. après l'introduction du «nouveau système d'horaire»*



Les développeurs et les opérateurs de systèmes ont besoin de plus en plus de savoir-faire pour maîtriser la complexité des systèmes techniques.

Les risques évoluent.
Le système ferroviaire devient plus vulnérable.

- **Nouveaux vecteurs d’attaque**
- **Diversité des points d’attaque**
- **Évolution de la situation**
- **Mesures de sécurité affaiblies par les idées reçues et le manque de connaissances**
- **Accroissement du poids économique**

SBB CFF FFS

La presse en parle.
La sensibilisation du public augmente.

Hackers Could Crash Trains by Hacking Rail Traffic System

Friday, April 24, 2015 Swati Khandelwal

TECHNOLOGY

TRAIN SYSTEMS ARE VULNERABLE TO HACKING

COMMUTE DELAYED? COULD BE A CYBERATTACKER ON THE TRACKS

By Kelsey D. Atherton Posted December 30, 2015

Handy-Problem legte Zugverkehr in Norwegen lahm

GSM-R-Ausfall sorgte für dreistündigen Bahn-Komplettausfall

Von dpa / Thorsten Neuhetzki

Kommentare (15) A A A Teilen

Ungläubiges Staunen und Zorn bei Zehntausenden Oster-Reisenden in Norwegen: Weil der Handy-Kontakt zwischen Zugführern und Leitzentralen nicht funktionierte, lag am Montagabend der komplette Bahnverkehr in dem skandinavischen Land ab 18.30 Uhr drei Stunden lang still. Erst als die defekte Stromversorgung für zwei zentrale Server in Trondheim nach drei Stunden ausgebessert war, durften die Züge wieder anfahren.

S. Korea accuses North of hacking railway systems and officials' phones

Published time: 8 Mar, 2016 07:31

Train-switching technology 'poses hacking threat'

8 March 2012 | Technology

Cyberkriminalität 01. Mai 2016 08:25; *Akt: 01.05.2016 08:37*

Hacker zeigen Lücke in Schweizer Zügen

Ein russischer Computerfachmann hat das Passwort eines Routers geknackt, der auch in Schweizer Zügen verwendet wird. Das Gerät überträgt Daten von Überwachungskameras oder Notrufe.

HOME » NEWS » UK NEWS » ROAD AND RAIL TRANSPORT

Hackers 'could hijack new signalling system and crash trains'

Rail expert warns a new digital system aimed to make lines safer, could be exposed to malicious software, or malware

SBB CFF FFS

Les exigences s’intensifient.
Les entreprises se doivent de réagir.

- **Les prescriptions et les exigences auront un impact majeur à l’avenir**
- **Les attaques ciblées et les dommages collatéraux ne cessent d’augmenter**
- **L’automatisation des processus opérationnels a aussi une influence sur les installations industrielles**

À quoi faire attention?
La sécurité des TIC est un processus continu.

Facteur humain:
… ne pas sous-estimer le «risque d'attaque» venant de «l'intérieur».
→ Formation / Prise de conscience

Facteur lié aux processus:
… les bons processus sont-ils vérifiés et la technologie doit-elle être adaptée à chaque processus?

Facteur technique:
… segmenter les réseaux et donc les risques
- Diversité des technologies et des systèmes
- manager les architectures des TIC
- manager les accès pour la maintenance

Facteur lié aux modèles d'exploitation des TIC:
… nouveaux modèles d'exploitation,
… autrement … p. ex. connectés partout et à tout moment, avoir une vue d'ensemble devient difficile, la «nébulosité» gagnant sans cesse du terrain.

Bilan – Ne rien faire n’est pas une alternative

- **Observer l’ensemble du système**
  (normes, réglementations et technologie)
- **Ne pas attendre**
  (continuer à développer ses propres *frameworks* / ISMS)
- **Favoriser une mise en œuvre pragmatique**
- **Amorcer un changement de culture**

Aujourd’hui comme autrefois. Fiable et sûr.

1930

2018

Photo: photo des archives fédérales 102-09857

Merci de votre intérêt.

CFF SA
Informatique

ICT-Security & Risk Management
Lindenhofstrasse 1
3000 Berne 65
Suisse
www.sbb.ch

Marcus Griesser
CISO
it.security@sbb.ch