SBB CFF FFS

IT-Sicherheit für Eisenbahn Verkehrs-unternehmen

Schutz kritischer Infrastrukturen

Jan Hohenauer

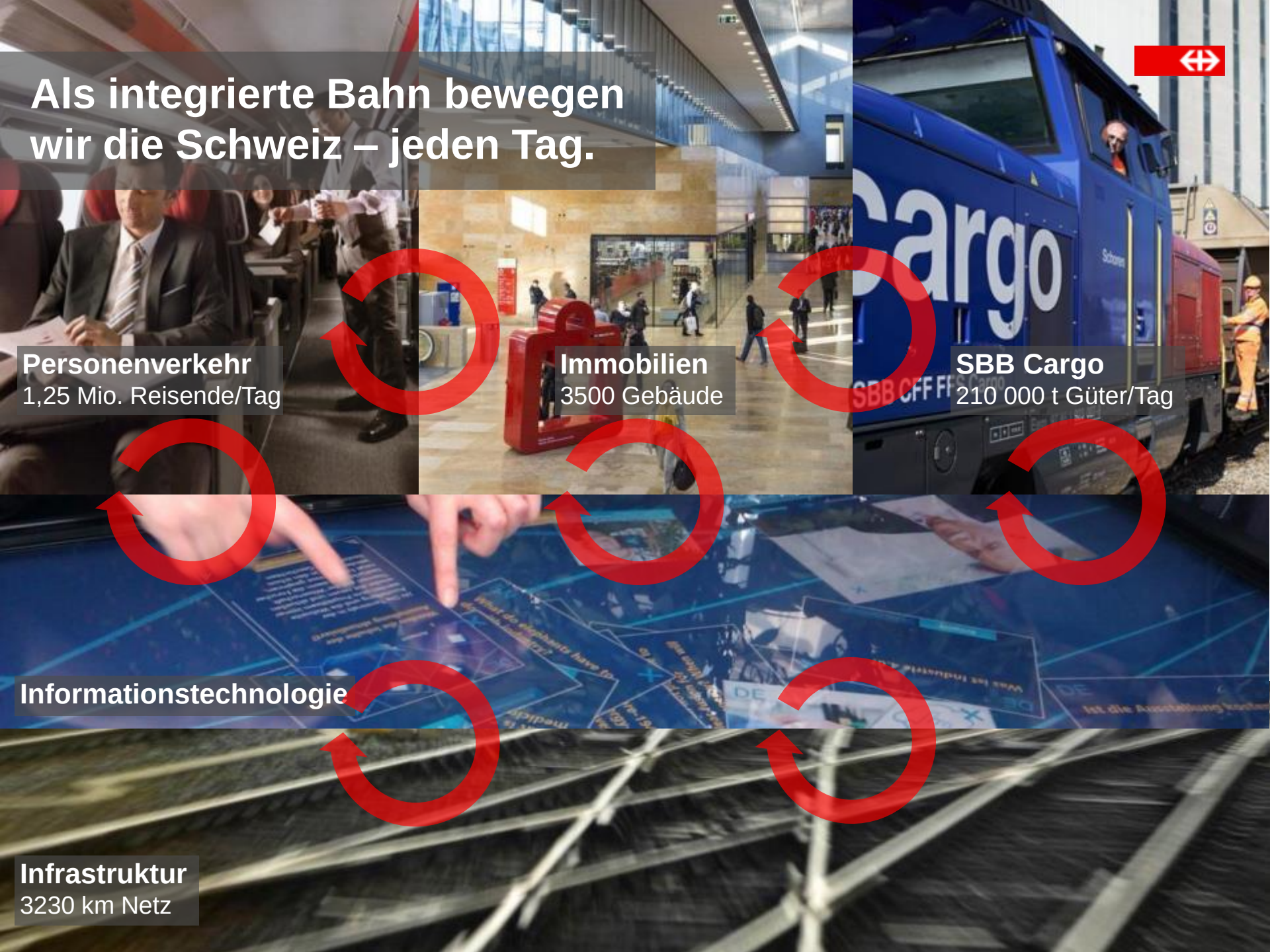
7. IHRUS-Fachtagung

9. November 2017, VHS Luzern

Inhalt.

1. SBB - Intro
2. Herausforderungen Mobilitätsdienstleister
3. Cyber-Security in kritischen Infrastrukturen
4. Pragmatische Lösungsansätze

Als integrierte Bahn bewegen wir die Schweiz – jeden Tag.



Personenverkehr
1,25 Mio. Reisende/Tag

Immobilien
3500 Gebäude

SBB Cargo
210 000 t Güter/Tag

Informationstechnologie

Infrastruktur
3230 km Netz

Wir gestalten die Mobilität der Zukunft – einfach, persönlich, vernetzt.

Herausforderungen eines integrierten Bahnsystems.
Die kritischen Infrastrukturen der Bahn.

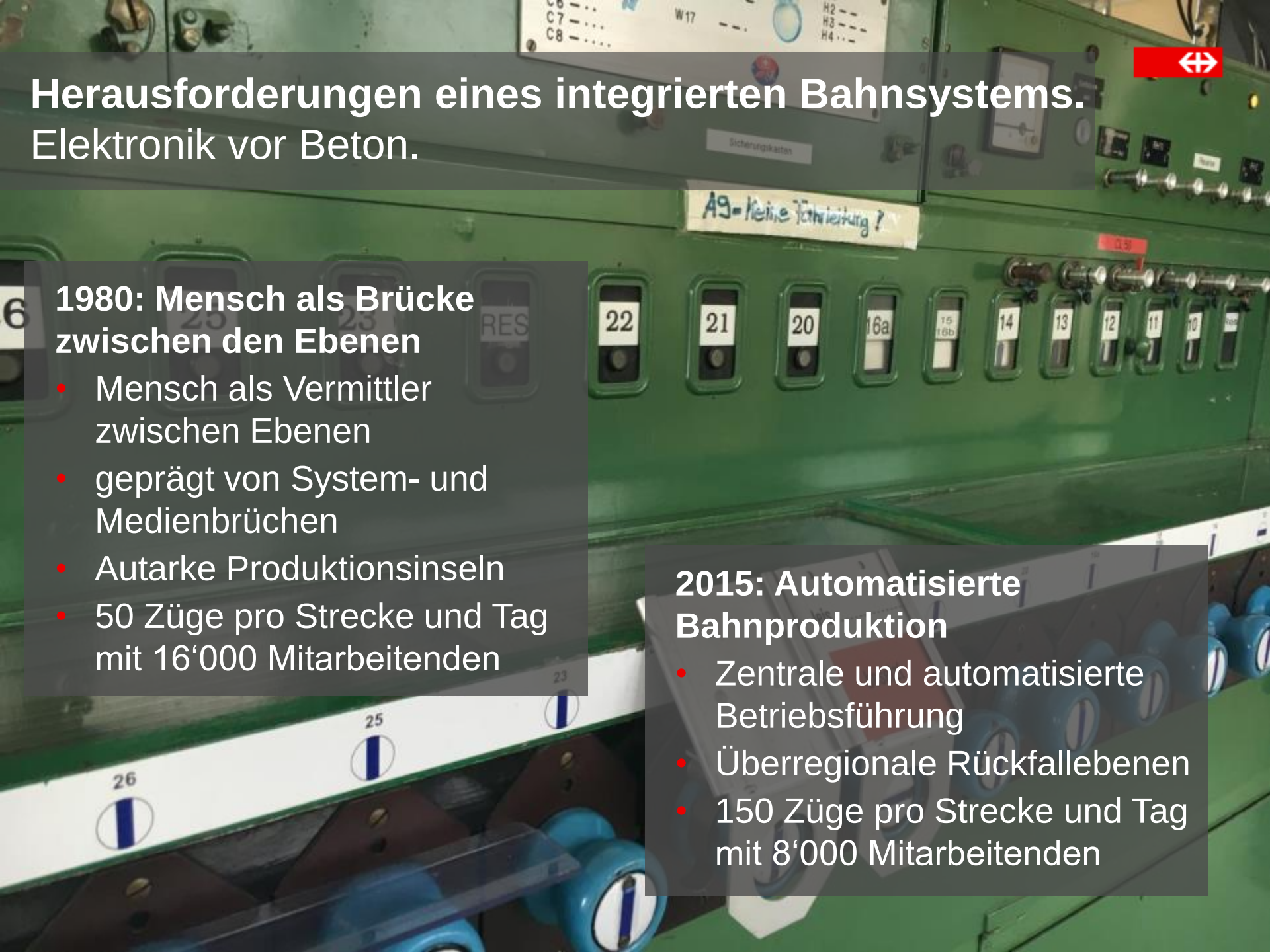
Telecomnetz

Energienetz

Schienennetz

Ziel für die Kunden:
Bereitstellung hoher Trassenkapazität

*Anzahl Züge, welche sich in kurzer Zeit auf den Gleisen ***sicher*** und ***pünktlich*** bewegen.



Herausforderungen eines integrierten Bahnsystems.

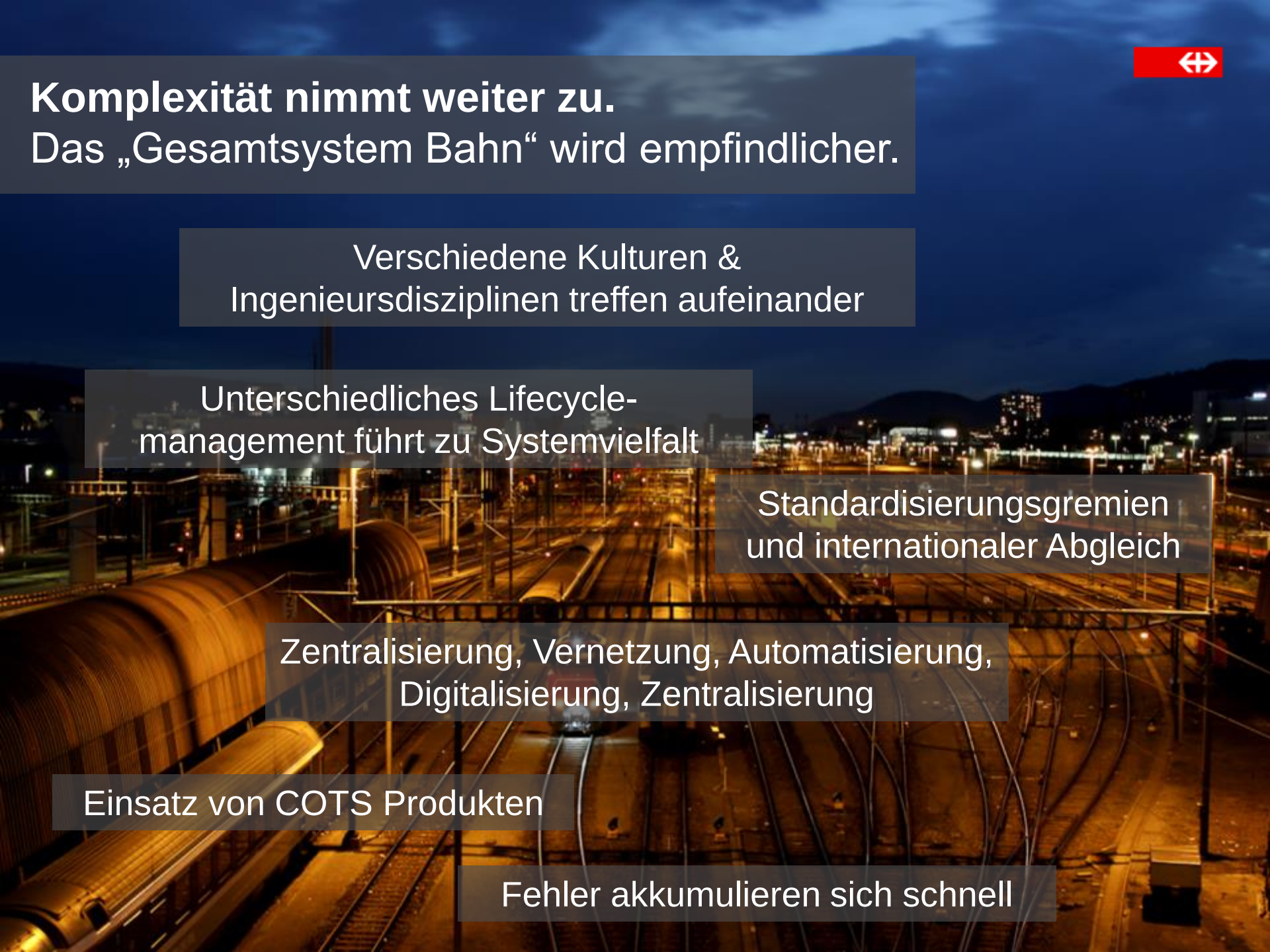
Elektronik vor Beton.

1980: Mensch als Brücke zwischen den Ebenen

- Mensch als Vermittler zwischen Ebenen
- geprägt von System- und Medienbrüchen
- Autarke Produktionsinseln
- 50 Züge pro Strecke und Tag mit 16‘000 Mitarbeitenden

2015: Automatisierte Bahnproduktion

- Zentrale und automatisierte Betriebsführung
- Überregionale Rückfallebenen
- 150 Züge pro Strecke und Tag mit 8‘000 Mitarbeitenden


Komplexität nimmt weiter zu.
Das „Gesamtsystem Bahn“ wird empfindlicher.
Verschiedene Kulturen &
Ingenieursdisziplinen treffen aufeinander
Unterschiedliches Lifecycle-
management führt zu Systemvielfalt
Standardisierungsgremien
und internationaler Abgleich
Zentralisierung, Vernetzung, Automatisierung,
Digitalisierung, Zentralisierung
Einsatz von COTS Produkten
Fehler akkumulieren sich schnell

Die Risikolage verändert sich.
Das „System Bahn“ wird angreifbarer.

- Mythen und Halbwissen erschweren Sicherungsmassnahmen
- Neue Angriffsvektoren
- Angriffe treffen das System als Ganzes
- Vielfalt der Endpunkte
- Wirtschaftliche Bedeutung nimmt zu
- Wissen um die Anlagen verbreitet (COTS)

Bild: James Harrison/Wikipedia

Die Anforderungen nehmen zu.
Die Unternehmen müssen reagieren.

- Vorgaben und Auflagen werden zukünftig eine wichtigere Rolle spielen
- Gezielte Angriffe und Kollateralschäden nehmen zu
- Geschäftsprozesse verändern die Industrieanwendungen

Lösungsansätze.
Faktor Systemarchitektur.

Einfache Aktionen sind besser als keine

- Netzwerk segmentieren – Risiken segmentieren
- Systeme härten – Angriffsfläche verkleinern
- Wartungszugänge zentralisieren
- Überwachung und Monitoring etablieren
- Betriebsmodelle prüfen Dokumentieren(!)

Lösungsansätze.
Cyber-Security Prozesse etablieren.

Prozess-Vernetzung mit der «Business-Seite» nimmt zu

- Verantwortlichkeiten klären
- Gesamtsystem beobachten (Standards, Regulationen und Technik)
- Nicht zuwarten (Frameworks / ISMS weiterentwickeln)
- Pragmatische Umsetzung
- Reporting / Lagebeurteilung (nach ICT-Standards)
- Forensikwissen aufbauen

Lösungsansätze.
Faktor Mensch berücksichtigen.

Auch das «Angriffsrisiko» von innen nimmt zu.

- Awareness schaffen – Mitarbeitende schulen
- Kulturelle Aspekte beachten – Kulturwandel initiieren
- Gemeinsame Sprache finden

Heute wie damals.
Zuverlässig und sicher.

1930

2017

Bundesarchiv Bild 102-09857, Induktive Zugsicherung (Indusi) an D-Zug-Lok

Jan Hohenauer
Stv. CISO

+41 51 285 10 80
jan.hohenauer@sbb.ch

SBB AG
ICT-Security & Risk Management
Lindenhofstrasse 1
3000 Bern 65
Schweiz

www.sbb.ch

Besten Dank für Ihr Interesse.