nextRailplus Tour d’Horizon

Cybersécurité dans les systèmes de contrôle et les installations de sécurité

SIEMENS

nextRailplus Tour d’Horizon

Cybersicherheit in Leitsystemen und Sicherungsanlagen

SIEMENS

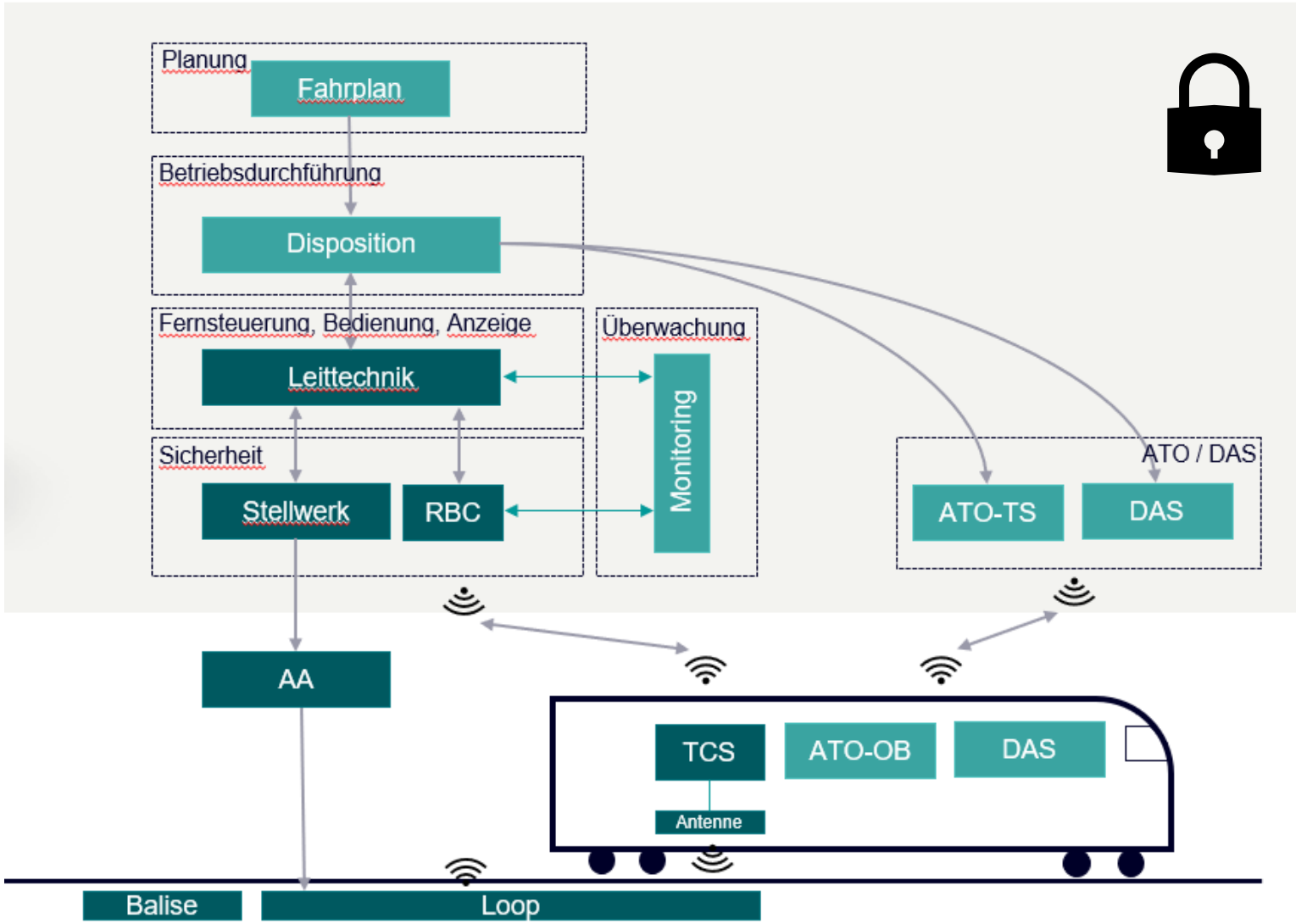
Les défis du marché ...

- Expansion de l'offre
- Pression sur les coûts
- Flexibilité opérationnelle
- Sécurité des investissements
- Migration sur une base existante
- Modulaire et standardisé
- Indépendance des fournisseurs
- Phases de réalisation courtes
- Cybersécurité

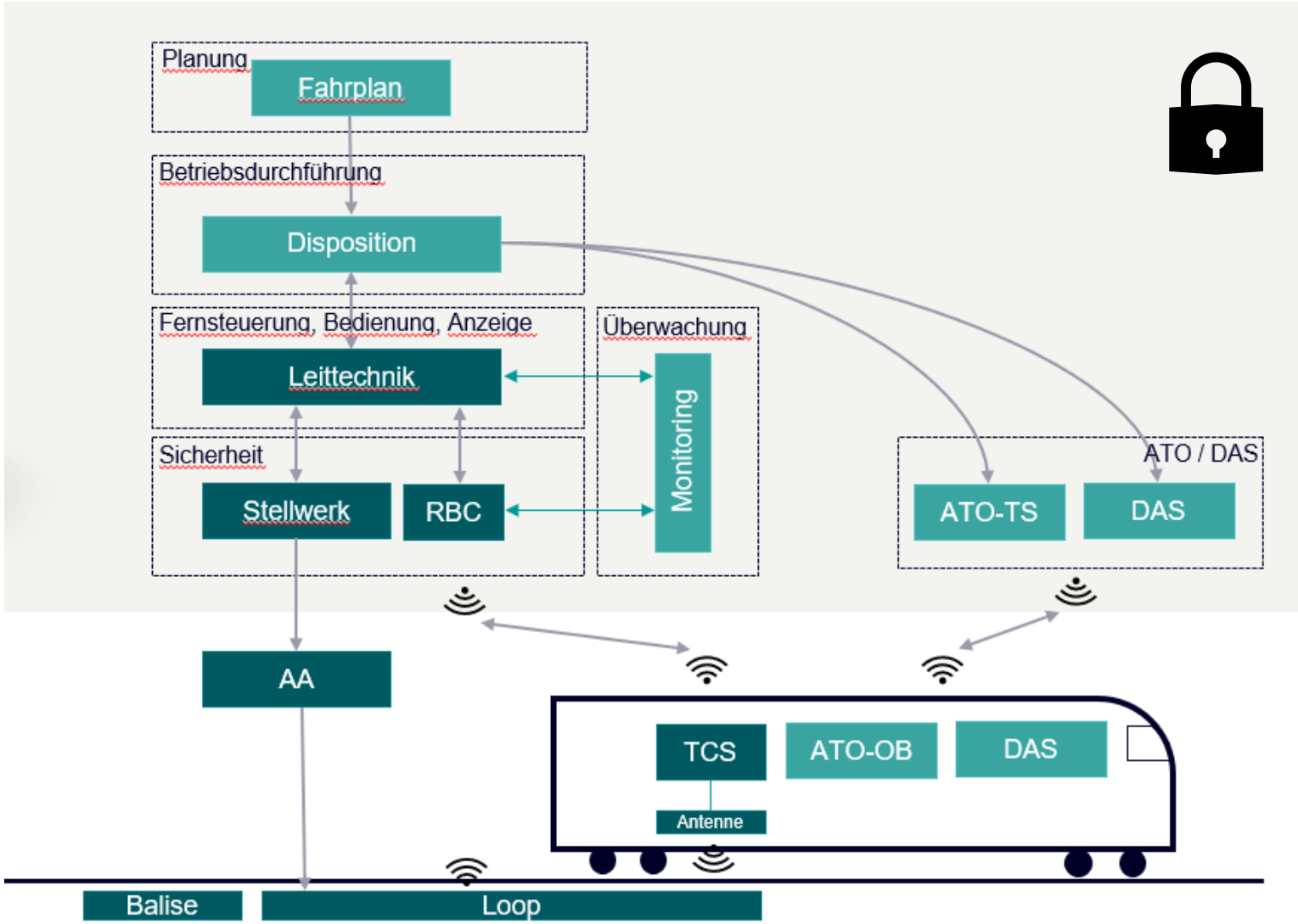
Herausforderungen auf dem Markt …

- Angebotsausbau
- Kostendruck
- Betriebliche Flexibilität
- Investitionssicherheit
- Migration auf bestehender Basis
- Modular und Standardisiert
- Lieferantenunabhängigkeit
- Kurze Realisierungsphasen
- Cyber Security

… exigent des solutions provenant de la mise en communication des systèmes existants



…verlangen Lösungen durch Vernetzung vorhandener Systeme



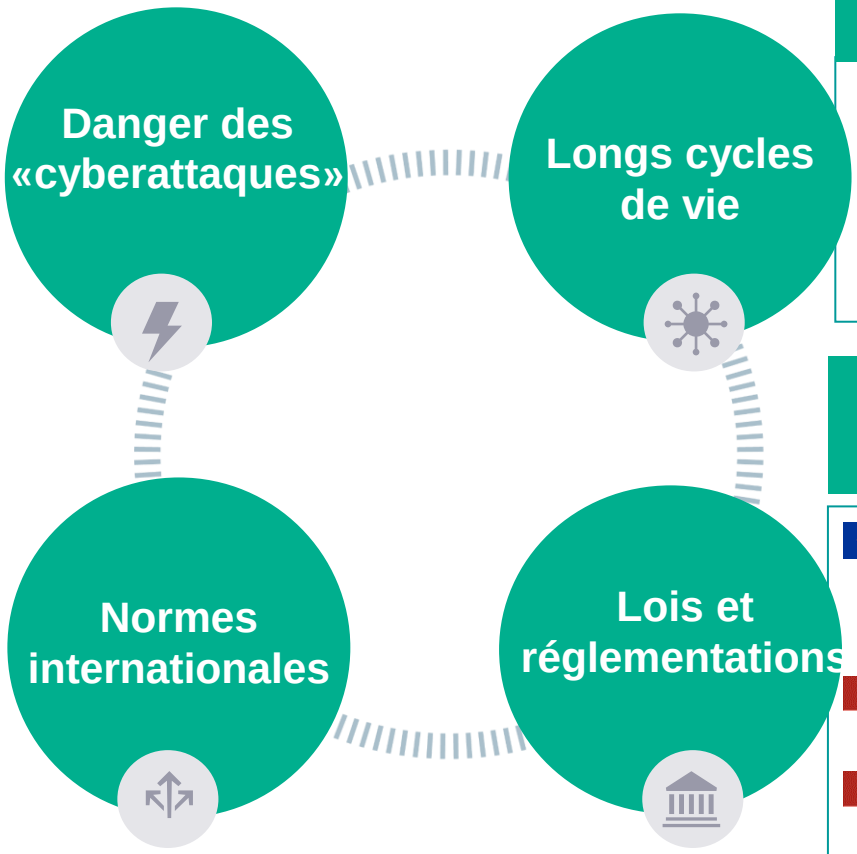
Cybersécurité - Pourquoi

Augmentation des «cyberattaques»

Les «cyberattaques» sont en augmentation – Les systèmes ferroviaires peuvent également être ciblés par des hackers

Normes de cybersécurité

- IEC 62443: réseaux de communication industriels – Sécurité IT pour réseaux et systèmes
- **CLC/TS 50701 (cybersécurité pour applications ferroviaires)**
- ISO 27001: systèmes de gestion de la sécurité de l'information



Longs cycles de vie

Les menaces cybernétiques frappent des systèmes de plus en plus complexes et ayant des cycles de vie longs

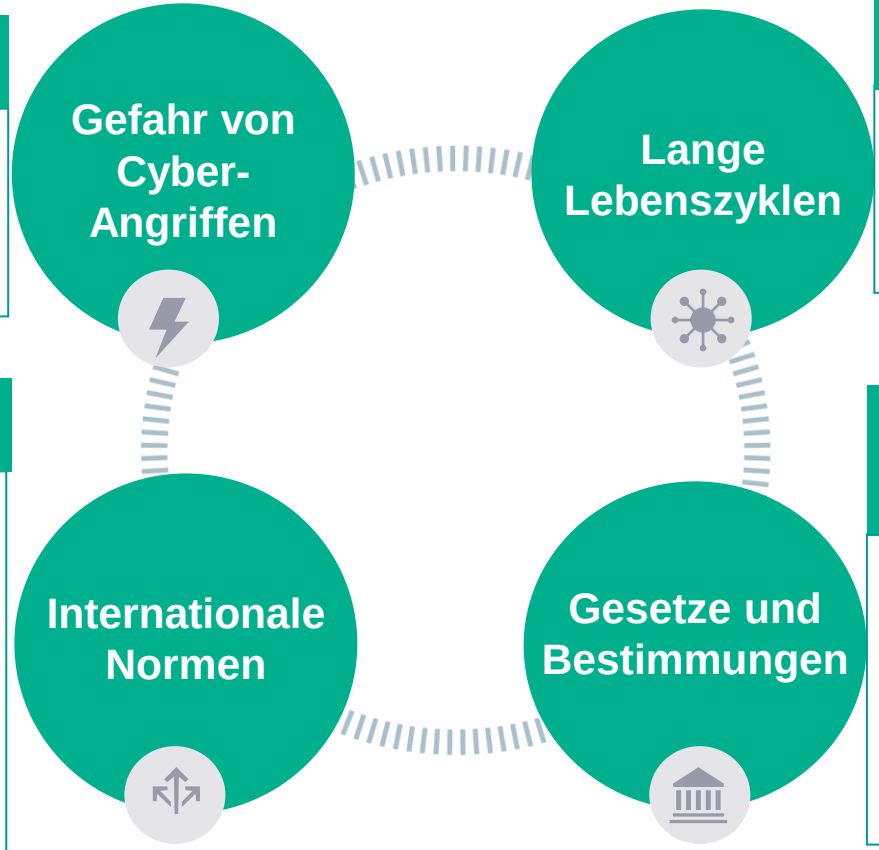
Lois et initiatives nationales et internationales en matière de cybersécurité

- Directive sur la sécurité des réseaux et des systèmes d'information (directive NIS)
- Stratégie nationale de cybersécurité (NCS)
- Directive BAV Cybersécurité (RL CySec-Rail)

Cybersicherheit - Warum

Zunehmende Cyber Angriffe

Cyber-Angriffe auf dem Vormarsch – Bahnsysteme können auch ins Visier von Hackern rücken



Lange Lebenszyklen

Cyber-Bedrohungen treffen auf Systeme mit zunehmender Komplexität und langen Lebenszyklen

Cybersicherheitsnormen

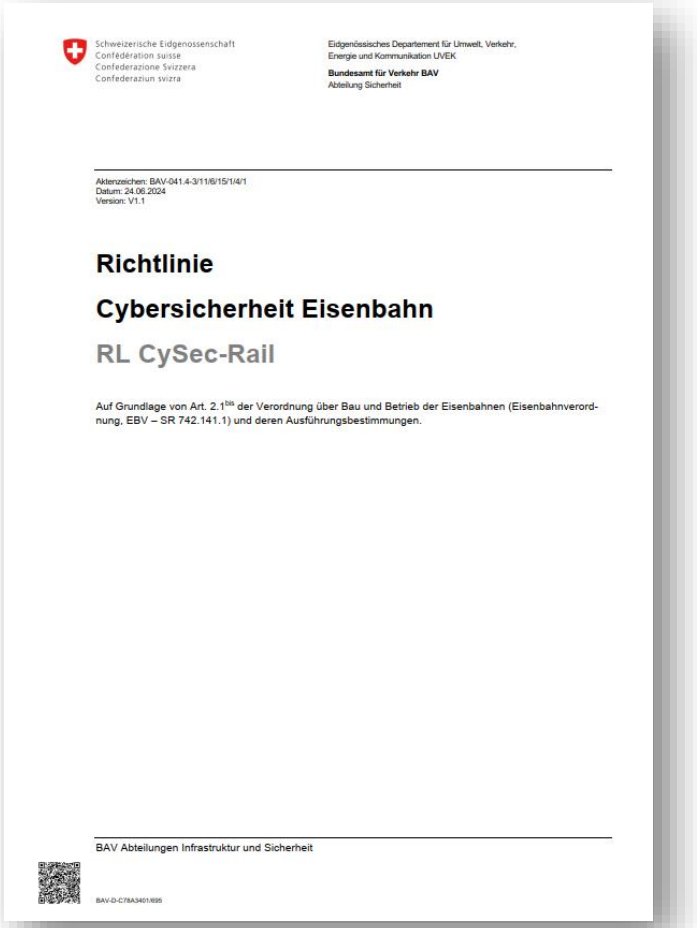
- IEC 62443: Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme
- **CLC/TS 50701 (Cybersecurity für Eisenbahn-Anwendungen**
- ISO 27001: Informationssicherheits-Managementsysteme

Nationale und internationale Gesetze und Initiativen zur Cybersicherheit

- Richtlinie über Netzwerk- und Informationssystemsicherheit (NIS-Richtlinie)
- Nationale Cyberstrategie (NCS)
- BAV Richtlinie Cybersicherheit (RL CySec-Rail)

SIEMENS

Exigences en matière de cybersécurité



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Verkehr BAV
Abteilung Sicherheit

Aktenzeichen: BAV-041.4-3/11/6/15/1/4/1
Datum: 24.06.2024
Version: V1.1

Richtlinie

Cybersicherheit Eisenbahn

RL CySec-Rail

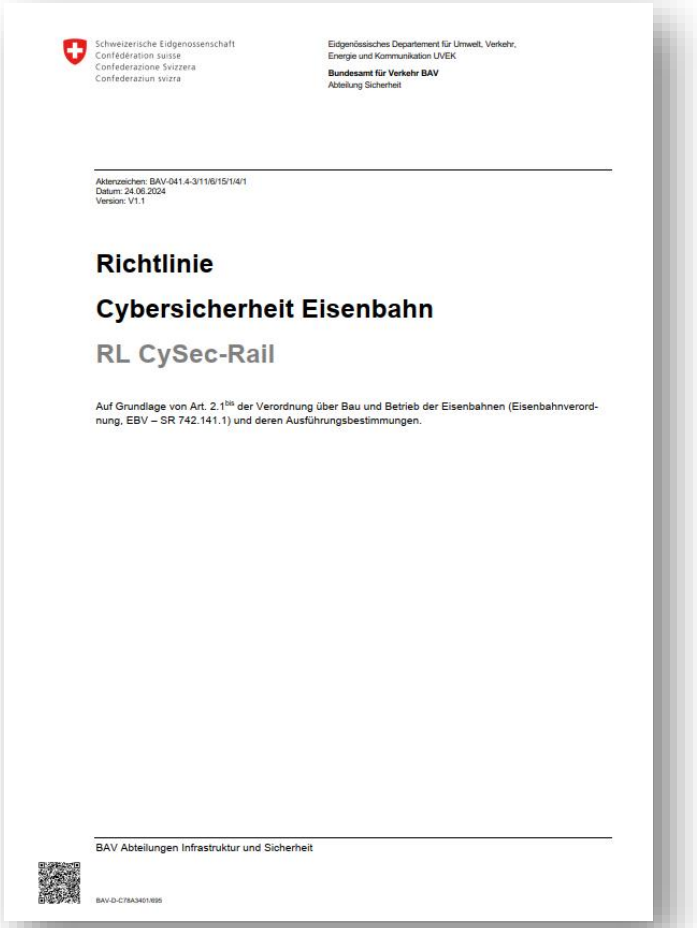
Auf Grundlage von Art. 2.1^{bis} der Verordnung über Bau und Betrieb der Eisenbahnen (Eisenbahnverordnung, EBV – SR 742.141.1) und deren Ausführungsbestimmungen.

BAV Abteilungen Infrastruktur und Sicherheit

BAV-D-C78A3401/695

- Entrera en vigueur avec l'AB-EBV.
- « Spécifie l'AB-EBV en ce qui concerne la conception minimale du système de gestion de la sécurité de l'information (SMSI) »
- « Les informations, les données et les systèmes devraient être protégés en fonction de leurs besoins de protection et en tenant compte de la situation de risque spécifique. Cette approche fondée sur les risques constitue la base pour les utilisateurs de cette directive »
- La directive fixe des exigences minimales en matière de cybersécurité

Anforderungen bezüglich Cybersicherheit



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Verkehr BAV
Abteilung Sicherheit

Aktenzeichen: BAV-041.4-3/11/6/15/1/4/1
Datum: 24.06.2024
Version: V1.1

Richtlinie

Cybersicherheit Eisenbahn

RL CySec-Rail

Auf Grundlage von Art. 2.1^{bis} der Verordnung über Bau und Betrieb der Eisenbahnen (Eisenbahnverordnung, EBV – SR 742.141.1) und deren Ausführungsbestimmungen.

BAV Abteilungen Infrastruktur und Sicherheit

BAV-D-C78A3401/695

- Wird mit der AB-EBV in Kraft gesetzt.
- «Konkretisiert die AB-EBV hinsichtlich der minimalen Ausgestaltung des Informationssicherheitsmanagementsystems (ISMS).»
- «Informationen, Daten und Systeme sollen entsprechend ihrem Schutzbedarf und unter Berücksichtigung der spezifischen Risikosituation geschützt werden. Dieser risikobasierte Ansatz ist die Grundlage für die Anwender dieser Richtlinie.»
- Die Richtlinie stellt Minimalanforderungen in Bezug zur Cybersicherheit

Vue d’ensemble des exigences minimales RL CySec - Rail

Exigences minimales SMSI

A-07	**Risikobeurteilung und –behandlung** Das Unternehmen muss einen Prozess zur Beurteilung von Informationssicherheitsrisiken festlegen und anwenden. Es müssen Kriterien für die Risikoakzeptanz und die Durchführung von Risikobeurteilungen definiert werden. Der Prozess muss folgende Punkte beinhalten: **a) Risiken identifizieren** Risiken, die sich aus dem Ausfall oder Beeinträchtigung von Informationssystemen ergeben, sind im Hinblick auf Integrität, Verfügbarkeit und Vertraulichkeit zu ermitteln. Es sind Personen zu bestimmen, die als Risikoeigner fungieren. **b) Risiken analysieren** Die möglichen Folgen bei Eintritt der identifizierten Risiken und deren Eintrittswahrscheinlichkeit sind abzuschätzen. **c) Risiken bewerten** Die Ergebnisse der Risikoanalyse (Risk Assessment) müssen mit den definierten Risikokriterien verglichen und eine Priorisierung für die Risikobehandlung durchgeführt werden. **d) Risiken behandeln** Basierend auf den Ergebnissen der Risikobeurteilung muss das Unternehmen angemessene Massnahmen zur Risikobehandlung auswählen und deren Umsetzung planen und durchführen. Die Risikoeignerin bzw. der Risikoeigner muss diesen Plan genehmigen, die Restrisiken dokumentieren, ggf. akzeptieren und die Mitarbeitenden sowie externe Beteiligte informieren. Es ist sicherzustellen, dass diese Schritte bei relevanten Änderungen sowie bei einer Verschlechterung der Bedrohungslage wiederholt werden. Mindestens einmal jährlich sind die Schritte a) bis d) zu wiederholen, um neue Risiken zu identifizieren, bestehende Risiken ggf. neu zu bewerten und die Wirksamkeit der umgesetzten Massnahmen auf die Risiken zu beurteilen.	AB-EBV Artikel 2.1[bis] Absatz 1.2 ISO/IEC 27001 Kapitel 6.1.2 Kapitel 6.1.3 NIST CSF 2.0 GV.RM-01 GV.RM-02 GV.SC-01 Handbuch VöV Kapitel 3.3 VO 2018/762 Kapitel 3.1 (Eingang in SMS von relevanten Bedrohungen aus der Risikoanalyse der Cybersicherheit) Hilfsmittel zum Risikomanagement siehe Anhang 3	B-04 B-13 B-15 B-16 B-19 B-20 B-26 B-27

Exigences IT, OT, réseaux de données, véhicules ferroviaires

B-11	**Betreiben von Systemen und Datennetzwerken** Systeme und Datennetzwerke sind so zu konfigurieren bzw. zu schützen, dass ungeplante Beeinträchtigungen oder Ausfälle vermieden werden. a) Für eine Übersicht des vorhandenen Netzes müssen aktuelle Netzwerkpläne vorliegen. b) Netzwerke müssen in sinnvollem Mass und unter Berücksichtigung der Grösse segregiert werden. Hierfür ist ein Netzwerkkonzept zu erstellen, das spezifische Massnahmen zum Informationsschutz beschreibt. c) Falls eine Vernetzung von OT- und IT-Diensten z.B. mit Public-Cloud Anwendungen so zunimmt, dass Netzübergänge nicht mehr sicher nach dem klassischen Zonenkonzept «Zones and Conduits» betrieben und verwaltet werden können, ist eine geeignete Sicherheitsarchitektur z.B. nach dem Zero-Trust-Prinzip zu etablieren. d) Informationssicherheitsrelevante Aktivitäten und Änderungen an den Systemen müssen gemäss dem Änderungsmanagementprozess protokolliert werden.	ISO/IEC 27002:2022 Kapitel 5.2 Kapitel 7.11 Kapitel 8.9 Kapitel 8.14 Kapitel 8.20 Kapitel 8.22 NIST CSF 2.0 ID.RA-07 PR.IR-01 PR.PS-01 PR.AA-06 Handbuch VöV Kapitel 3.5 Betrifft ISB , Datennetze für OT: D RTE 28100 Kapitel 5	Kapitel 3.1.2

Contrôles spécifiques OT

B-22	**Installation von Software auf OT** Aufgrund der Kritikalität (Schutzbedarf) der OT-Systeme müssen Softwareinstallationen überwacht und kontrolliert werden. a) Die Installation von Updates auf OT-Systemen dürfen nur von qualifiziertem Personal durchgeführt werden. b) Es muss sichergestellt werden, dass Softwareupdates der Hersteller für die OT-Systeme in einem vorgängig mit dem Hersteller definierten Zeitraum zur Verfügung gestellt werden. c) Für die Installation von Updates muss ein Genehmigungsverfahren durchlaufen werden, an dem auch das Safety-Management involviert ist. d) Vor der Installation von Updates auf OT-Systemen ist die Software umfangreich zu testen. Für die Tests sind Testprotokolle zu führen, mit denen die getesteten Funktionen und eventuelle Auffälligkeiten dokumentiert werden. Bei Problemen darf keine Installation respektive Update durchgeführt werden. e) Es muss im Voraus eine Rollback-Strategie definiert und getestet werden. Dies bedeutet, dass die OT-Systeme bei Nichtfunktionalität auf den ursprünglichen, funktionierenden Zustand zurückgeführt werden können. f) Es ist zu protokollieren, von wem und aus welchem Grund Updates oder Software installiert werden. g) Ältere Softwareversionen müssen zusammen mit den notwendigen Informationen und Parametern archiviert werden.	TS50701:2023 Kapitel 9 Kapitel 10.2 Kapitel 10.3 NIST CSF 2.0 ID.AM-08 PR.DS-01 PR.PS-02

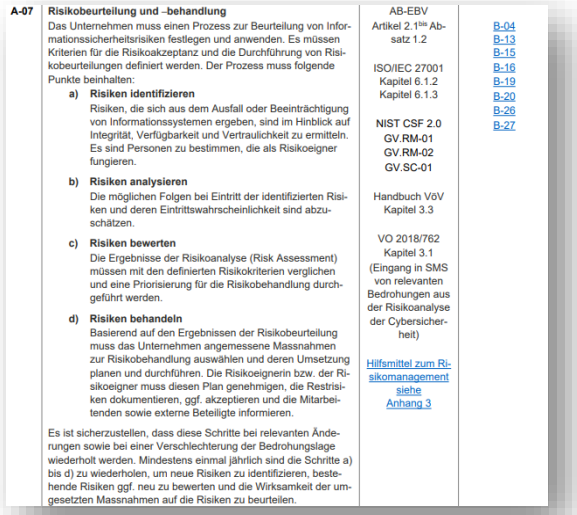
Contrôles spécifiques des véhicules ferroviaires

B-29	**Physischer Schutz** a) Es ist durch geeignete Massnahmen (z.B. abschliessbarer Schrank) sicherzustellen, dass schützenswerte Komponenten vor physischer Manipulation geschützt sind. b) Falls kein wirksamer physischer Schutz realisiert werden kann, sind andere Massnahmen wie z.B. ein Fahrzeugüberwachungssystem zu etablieren.. c) Für die Überwachung sind Alarmsysteme (z.B. durch Videoüberwachung, Überwachung von Abdeckungen bei schützenswerten Komponenten) zu konfigurieren und entsprechend zu schützen (siehe folgender Punkt). d) Überwachungssysteme sollten sich in einem Bereich befinden, der für die Person, die den Alarm auslöst, nicht zugänglich ist. e) Die Überwachungssysteme müssen über manipulationssichere Mechanismen verfügen und regelmässig getestet werden.	ISO/IEC 27002:2022 Kapitel 7.4 NIST CSF 2.0 PR.AA-06 Videoüberwachung: VüV-ÖV [16]

SIEMENS

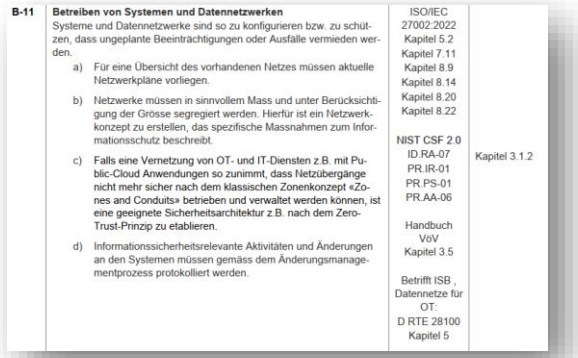
Übersicht Minimalanforderungen RL CySec - Rail

Minimale Anforderungen ISMS



A-07	**Risikobeurteilung und –behandlung** Das Unternehmen muss einen Prozess zur Beurteilung von Informationssicherheitsrisiken festlegen und anwenden. Es müssen Kriterien für die Risikoakzeptanz und die Durchführung von Risikobeurteilungen definiert werden. Der Prozess muss folgende Punkte beinhalten: **a) Risiken identifizieren** Risiken, die sich aus dem Ausfall oder Beeinträchtigung von Informationssystemen ergeben, sind im Hinblick auf Integrität, Verfügbarkeit und Vertraulichkeit zu ermitteln. Es sind Personen zu bestimmen, die als Risikoeigner fungieren. **b) Risiken analysieren** Die möglichen Folgen bei Eintritt der identifizierten Risiken und deren Eintrittswahrscheinlichkeit sind abzuschätzen. **c) Risiken bewerten** Die Ergebnisse der Risikoanalyse (Risk Assessment) müssen mit den definierten Risikokriterien verglichen und eine Priorisierung für die Risikobehandlung durchgeführt werden. **d) Risiken behandeln** Basierend auf den Ergebnissen der Risikobeurteilung muss das Unternehmen angemessene Massnahmen zur Risikobehandlung auswählen und deren Umsetzung planen und durchführen. Die Risikoeignerin bzw. der Risikoeigner muss diesen Plan genehmigen, die Restrisiken dokumentieren, ggf. akzeptieren und die Mitarbeitenden sowie externe Beteiligte informieren. Es ist sicherzustellen, dass diese Schritte bei relevanten Änderungen sowie bei einer Verschlechterung der Bedrohungslage wiederholt werden. Mindestens einmal jährlich sind die Schritte a) bis d) zu wiederholen, um neue Risiken zu identifizieren, bestehende Risiken ggf. neu zu bewerten und die Wirksamkeit der umgesetzten Massnahmen auf die Risiken zu beurteilen.	AB-EBV Artikel 2.1[bis] Absatz 1.2 ISO/IEC 27001 Kapitel 6.1.2 Kapitel 6.1.3 NIST CSF 2.0 GV.RM-01 GV.RM-02 GV.SC-01 Handbuch VöV Kapitel 3.3 VO 2018/762 Kapitel 3.1 (Eingang in SMS von relevanten Bedrohungen aus der Risikoanalyse der Cybersicherheit) Hilfsmittel zum Risikomanagement siehe Anhang 3	B-04 B-13 B-15 B-16 B-19 B-20 B-26 B-27

Anforderungen IT, OT, Datennetze, Eisenbahnfahrzeuge

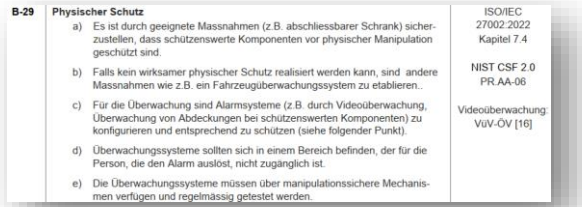


B-11	**Betreiben von Systemen und Datennetzwerken** Systeme und Datennetzwerke sind so zu konfigurieren bzw. zu schützen, dass ungeplante Beeinträchtigungen oder Ausfälle vermieden werden. a) Für eine Übersicht des vorhandenen Netzes müssen aktuelle Netzwerkpläne vorliegen. b) Netzwerke müssen in sinnvollem Mass und unter Berücksichtigung der Grösse segregiert werden. Hierfür ist ein Netzwerkkonzept zu erstellen, das spezifische Massnahmen zum Informationsschutz beschreibt. c) Falls eine Vernetzung von OT- und IT-Diensten z.B. mit Public-Cloud Anwendungen so zunimmt, dass Netzübergänge nicht mehr sicher nach dem klassischen Zonenkonzept «Zones and Conduits» betrieben und verwaltet werden können, ist eine geeignete Sicherheitsarchitektur z.B. nach dem Zero-Trust-Prinzip zu etablieren. d) Informationssicherheitsrelevante Aktivitäten und Änderungen an den Systemen müssen gemäss dem Änderungsmanagementprozess protokolliert werden.	ISO/IEC 27002:2022 Kapitel 5.2 Kapitel 7.11 Kapitel 8.9 Kapitel 8.14 Kapitel 8.20 Kapitel 8.22 NIST CSF 2.0 ID.RA-07 PR.IR-01 PR.PS-01 PR.AA-06 Handbuch VöV Kapitel 3.5 Betrifft ISB , Datennetze für OT: D RTE 28100 Kapitel 5	Kapitel 3.1.2

Spezifische Controls OT

B-22	**Installation von Software auf OT** Aufgrund der Kritikalität (Schutzbedarf) der OT-Systeme müssen Softwareinstallationen überwacht und kontrolliert werden. a) Die Installation von Updates auf OT-Systemen dürfen nur von qualifiziertem Personal durchgeführt werden. b) Es muss sichergestellt werden, dass Softwareupdates der Hersteller für die OT-Systeme in einem vorgängig mit dem Hersteller definierten Zeitraum zur Verfügung gestellt werden. c) Für die Installation von Updates muss ein Genehmigungsverfahren durchlaufen werden, an dem auch das Safety-Management involviert ist. d) Vor der Installation von Updates auf OT-Systemen ist die Software umfangreich zu testen. Für die Tests sind Testprotokolle zu führen, mit denen die getesteten Funktionen und eventuelle Auffälligkeiten dokumentiert werden. Bei Problemen darf keine Installation respektive Update durchgeführt werden. e) Es muss im Voraus eine Rollback-Strategie definiert und getestet werden. Dies bedeutet, dass die OT-Systeme bei Nichtfunktionalität auf den ursprünglichen, funktionierenden Zustand zurückgeführt werden können. f) Es ist zu protokollieren, von wem und aus welchem Grund Updates oder Software installiert werden. g) Ältere Softwareversionen müssen zusammen mit den notwendigen Informationen und Parametern archiviert werden.	TS50701:2023 Kapitel 9 Kapitel 10.2 Kapitel 10.3 NIST CSF 2.0 ID.AM-08 PR.DS-01 PR.PS-02

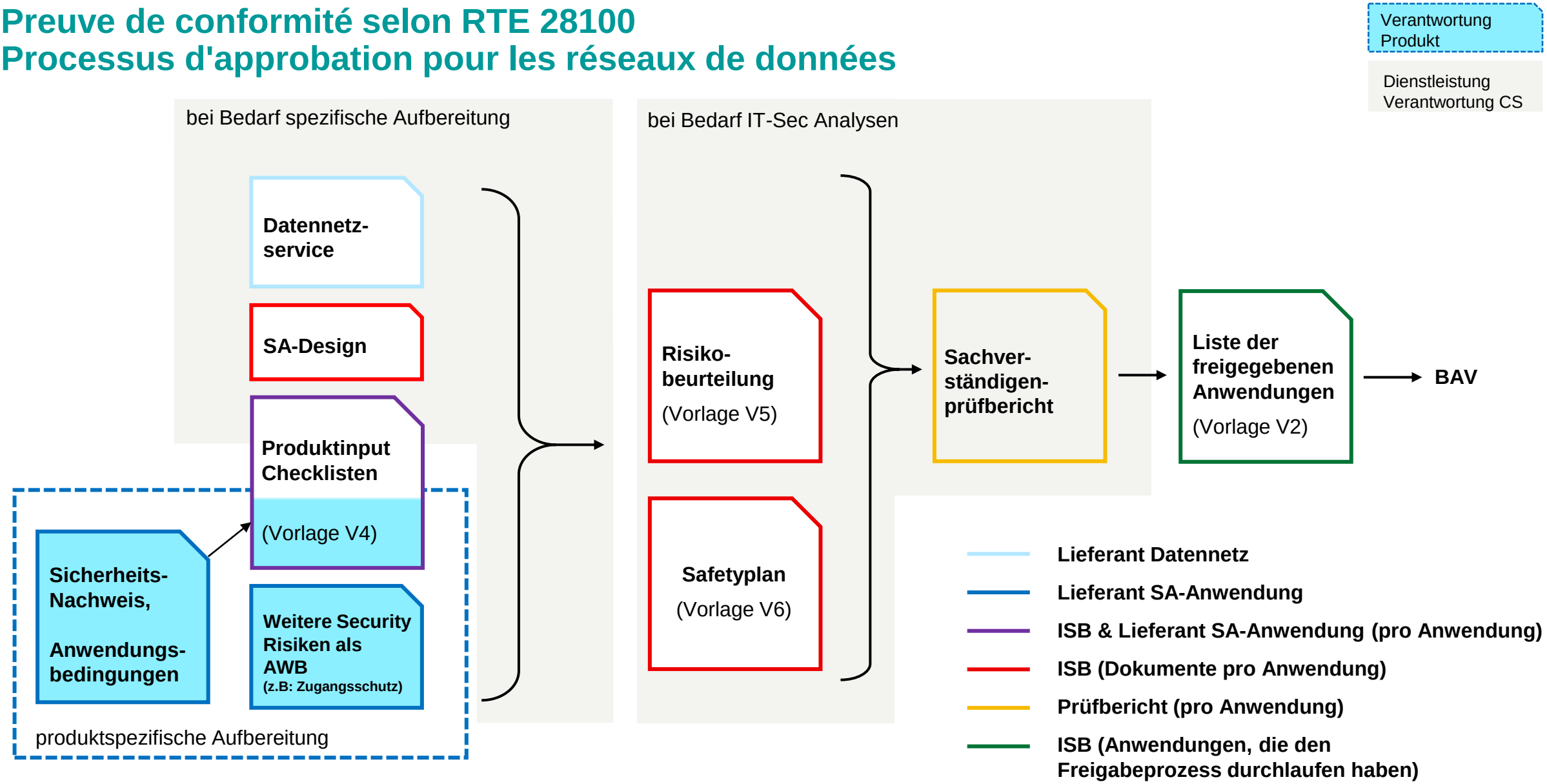
Spezifische Controls Eisenbahnfahrzeuge



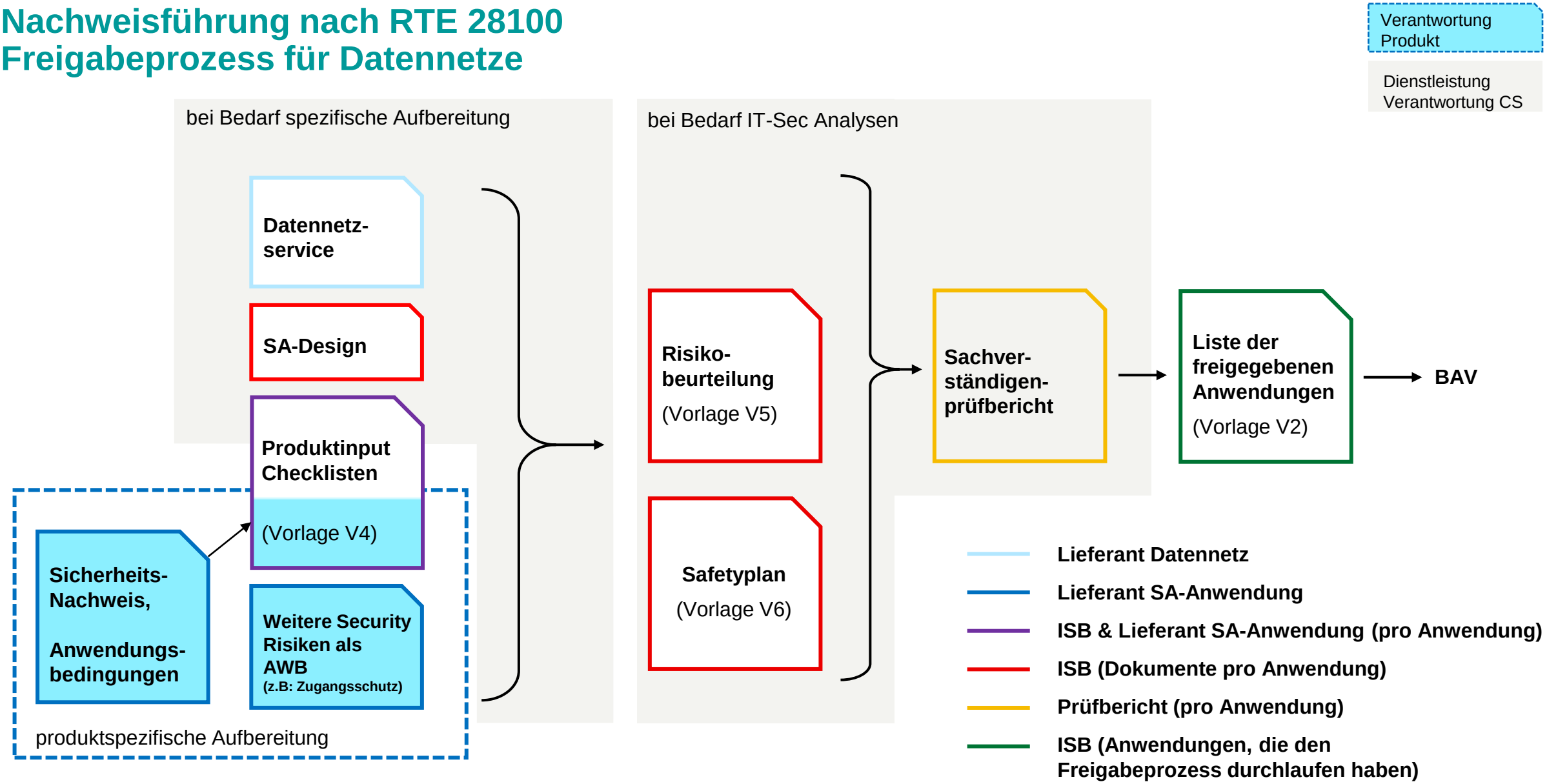
B-29	**Physischer Schutz** a) Es ist durch geeignete Massnahmen (z.B. abschliessbarer Schrank) sicherzustellen, dass schützenswerte Komponenten vor physischer Manipulation geschützt sind. b) Falls kein wirksamer physischer Schutz realisiert werden kann, sind andere Massnahmen wie z.B. ein Fahrzeugüberwachungssystem zu etablieren.. c) Für die Überwachung sind Alarmsysteme (z.B. durch Videoüberwachung, Überwachung von Abdeckungen bei schützenswerten Komponenten) zu konfigurieren und entsprechend zu schützen (siehe folgender Punkt). d) Überwachungssysteme sollten sich in einem Bereich befinden, der für die Person, die den Alarm auslöst, nicht zugänglich ist. e) Die Überwachungssysteme müssen über manipulationssichere Mechanismen verfügen und regelmässig getestet werden.	ISO/IEC 27002:2022 Kapitel 7.4 NIST CSF 2.0 PR.AA-06 Videoüberwachung: VüV-ÖV [16]

SIEMENS

Preuve de conformité selon RTE 28100
Processus d'approbation pour les réseaux de données

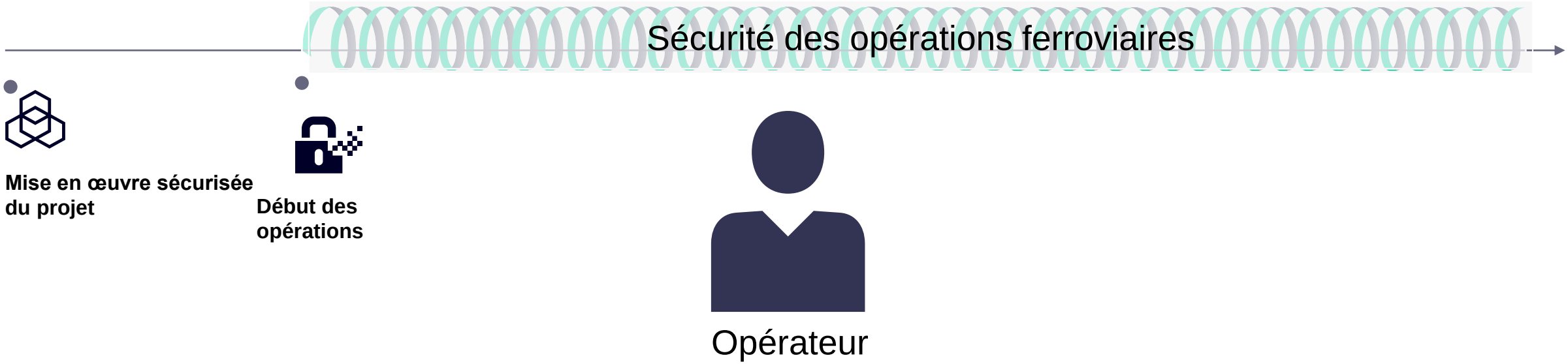


Nachweisführung nach RTE 28100
Freigabeprozess für Datennetze



SIEMENS

Exploitation ferroviaire sûre tout au long du cycle de vie



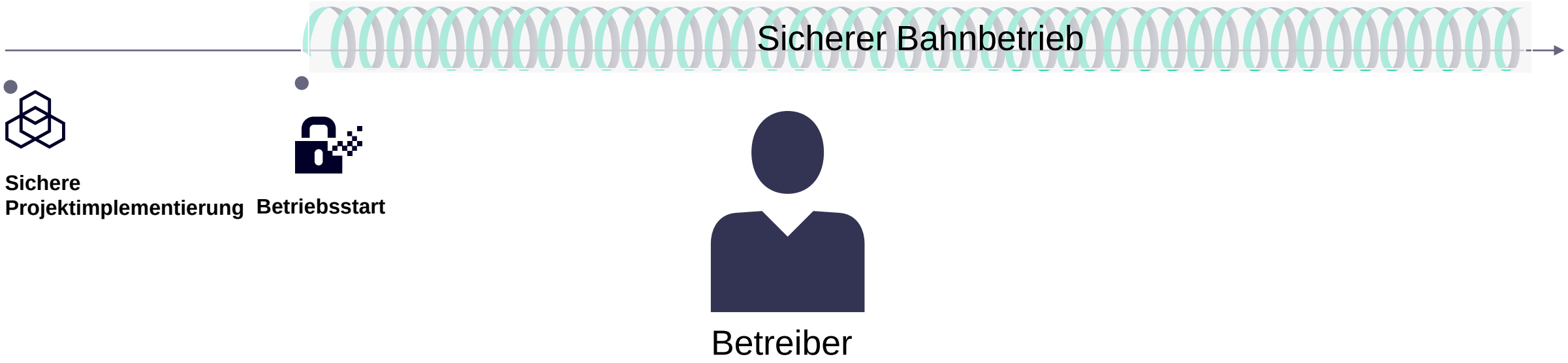
Défis:

- Systèmes plus complexes - Augmentation de la mise en réseau - Connexion IT/OT
- Longs cycles de vie
- Exigences et normes croissantes dans le domaine de la cybersécurité
- Cybercriminalité organisée
- Situation géopolitique tendue en Europe

Des défis de plus en plus importants nécessitent une plus grande coopération entre l'opérateur et le fournisseur

SIEMENS

Sicherer Bahnbetrieb über den gesamten Lebenszyklus

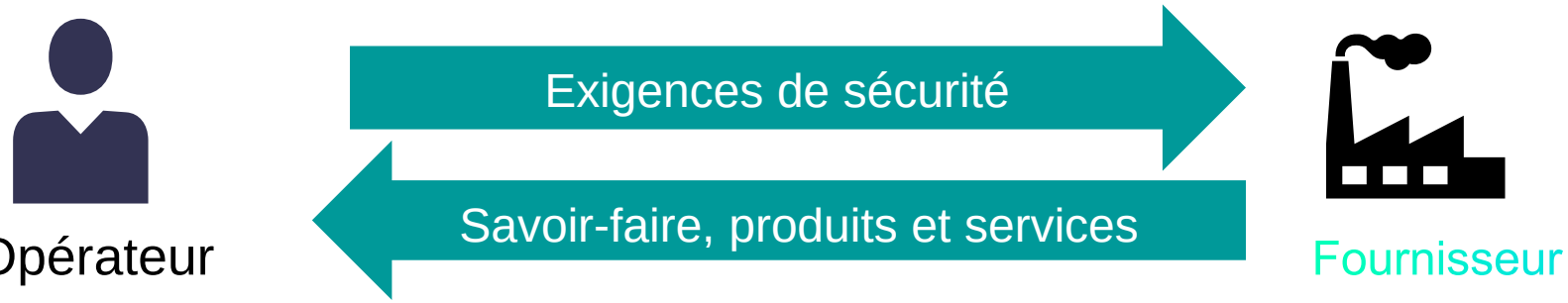


Herausforderungen:

- Komplexere Systeme - Zunehmende Vernetzung - IT/OT Verbindung
- Lange Lebenszyklen
- Zunehmende Anforderungen und Normen im Bereich Cyber Security
- Organisierte Cyberkriminalität
- Angespannte geopolitische Situation in Europa

Zunehmende Herausforderungen erfordert höhere Zusammenarbeit zwischen Betreiber und Lieferant

Responsabilités dans le contexte de la cybersécurité
Opérateur – Fournisseur



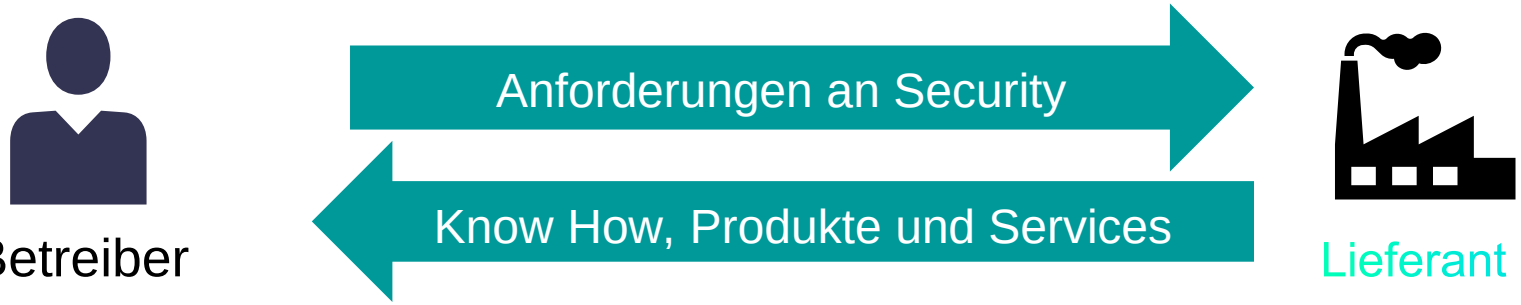
- Responsable de l'évaluation des risques de ses «Assets»
- Responsable de la sécurité de ses «Assets»
- Stratégie, employés, organisation, technologie et processus
- Responsable de la mise en œuvre des directives et des normes

- Services de cybersécurité proactifs pour une protection renforcée
- Mesures de protection réactives pour limiter les dommages
- Conseil et accompagnement

Une stratégie de sécurité globale et une évaluation des risques protègent contre les surprises

SIEMENS

Verantwortlichkeiten im Cyber Security Kontext
Betreiber – Lieferant



- Verantwortlich für Risikobeurteilung seiner Assets
- Verantwortlich für die Sicherheit seiner Assets
  - Strategie, Mitarbeitende, Organisation, Technik und Prozesse
- Verantwortlich für die Umsetzung von Richtlinien und Normen

- Proaktive Cyber Security Services für erhöhtem Schutz
- Reaktive Schutzmassnahmen für Schadensbegrenzung
- Beratung und Unterstützung

Ganzheitliche Sicherheitsstrategie und Risikobeurteilung schützt vor Überraschung

Services de cybersécurité

Proactif

Identifie
Risques/vulnérabilités de sécurité

- Analyse des menaces et des risques
- IEC 62443/TS 50701-Analyse
- Tests de pénétration
- Analyses de sécurité
- Recommandations de mise en œuvre (p. ex. RTE28001)

Découvre
Anomalies et vulnérabilités

- Gestion des vulnérabilités
- Détection d'intrusion

Protège
Vos systèmes

- Mises à jour et correctifs de sécurité
- Gestion des clés ETCS
- Formation de sensibilisation
- Formation CEI 62443

Réactif

Réagir
et se remettre d'incidents cybernétiques

- Réponse aux incidents *Coming soon*

Contactez-nous si vous souhaitez en savoir plus sur nos services

SIEMENS

Cyber Security Services
Nachhaltig sicherer Bahnbetrieb

Proaktiv

Identifiziert
Sicherheitsrisiken/-lücken

- Bedrohungs- und Risikoanalyse
- IEC 62443/TS 50701-Analyse
- Penetrationstests
- Sicherheitsscans
- Umsetzungs-empfehlungen (Bsp: RTE28001)

Entdeckt
Anomalien & Schwachstellen

- Schwachstellen-management
- Intrusion Detection

Schützt
Ihre Systeme

- Sicherheitsupdates und -patches
- ETCS-Key-Management
- Awareness Schulungen
- IEC 62443-Schulungen

Reaktiv

Reagieren
und Wiederherstellen von Cyber Vorfällen

- Incident Response *Coming soon*

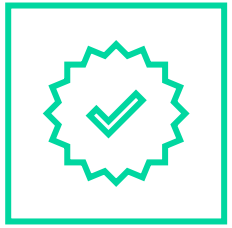
Kontaktieren Sie uns zu Deep Dives zu unseren Services

SIEMENS

Notre expertise, nos outils existants et nos services vous aident à augmenter la sécurité de vos installations

Partenaire de sécurité certifié

Nous sommes le fournisseur ferroviaire avec le plus de certifications de cybersécurité au monde

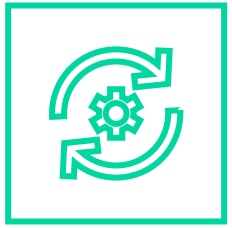


Combinaison du savoir-faire de nos installations et de la cybersécurité

> 1 300 experts en cybersécurité dans toutes nos branches d'activités

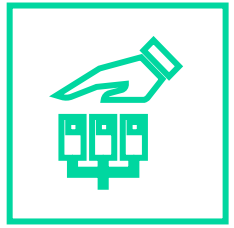
Approche intégrée de la solution de cybersécurité de bout en bout

Faible dépendance vis-à-vis des parties externes



De nombreuses années d'expérience dans la protection de nos produits

Transfert de savoir-faire, de technologie et de solutions



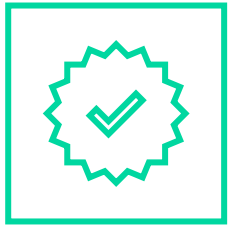
Partenariat pour la sécurité ferroviaire

SIEMENS

Unsere Expertise, bestehenden Tools und Services helfen Ihnen die Sicherheit Ihrer Anlagen zu erhöhen

Zertifizierter Sicherheitspartner

Wir sind der Bahnanbieter mit den meisten Cyber Security Zertifizierungen weltweit

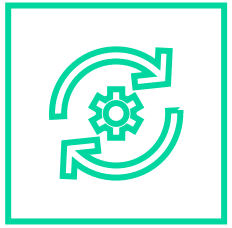


Verbindung von Anlagen Know How und Cyber Security

> 1.300 Cybersicherheits-experten in allen Geschäftsbereichen

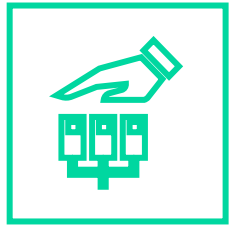
Integrierter Ansatz für eine durchgängige Cybersicherheits-lösug

Geringe Abhängigkeit von externen Parteien



Langjährige Erfahrung im Schutz unserer Produkte

Weitergabe von Know-how, Technologie und Lösungen



Partnerschaftlich für einen sicheren Bahnbetrieb

SIEMENS

Référence : centre de cyberdéfense

Coopération avec les CFF

Depuis 2020

Référence - CFF

SBB CFF FFS

- Siemens Mobility, en tant que partenaire stratégique important pour la création du premier centre de cyberdéfense dans l'industrie ferroviaire

Solution

- Conseil en sécurité et intégration de systèmes par nos experts en cybersécurité
- Tests d'intrusion précis avec un focus sur les systèmes IT/OT

Avantages

- Combinaison d'une connaissance approfondie des systèmes ferroviaires, d'un savoir-faire et de politiques en matière de cybersécurité
- Les CFF se protègent de manière proactive contre les cybermenaces afin d'assurer la disponibilité des systèmes ferroviaires

SIEMENS

Referenz: Cyber Defense Center
Zusammenarbeit mit SBB

Seit 2020

Referenz - SBB

SBB CFF FFS

- Siemens Mobility als strategisch wichtiger Partner für den Aufbau des ersten Cyber-Abwehrzentrums in der Bahnindustrie

Lösung

- Sicherheitsberatung und Systemintegration durch unsere Cyber-Experten
- Präzise Penetrationstests mit Fokus auf IT/OT-Systeme

Vorteile

- Kombination von fundiertem Wissen über Bahnsysteme, Cybersecurity-Know-how und Richtlinien
- Die SBB schützt sich proaktiv gegen Cyberbedrohungen, um die Verfügbarkeit der Bahnsysteme sicherstellen

SIEMENS

Contact

Published by Siemens Mobility

Sascha Lehmann

Digital Sales Manager

Siemens Mobility AG
Hammerweg 1

8304 Wallisellen

lehmann.sascha@siemens.com

+41 79 641 81 78

Sebastian Klabes

Product Management, Portfolio & Innovation Head

Siemens Mobility AG
Hammerweg 1

8304 Wallisellen

sebastian.klabes@siemens.com

+41 79 516 75 57

SIEMENS