

# OT-Security Sicherungsanlagen

Idee für eine  
Arbeitsgruppe zur  
VöV FG ET

# Entwurf Arbeitsgruppe für OT Security Themen Sicherungsanlagen

1. Ausgangslage und Hintergrund
2. Bedarf, warum eine neue Arbeitsgruppe
3. Abgrenzung zu „VöV Arbeitsgruppe CyberSecurity“
4. Scope und Zielgruppe
5. Vernetzung der Gruppen

# 1. Ausgangslage und Hintergrund

## Ausgangslage

Die erfolgreiche ERFA-Tagung des VöV 27. Juni 2024 und Auswertung der Gruppenarbeiten haben gezeigt, dass das Thema Cybersecurity bei Sicherungsanlagen von grossem Interesse ist.

Das Thema ist für Projektleitende und Entscheidungsträger sowie Security Verantwortliche bei den Sicherungsanlagen wichtig, es fehlt aber oft noch an Management Attention, Grundlagen und Knowhow.

Nicht zuletzt ist es schwierig, Personen im Bereich IT Security mit fundierten Bahn- und Sicherungsanlagenkenntnissen zu finden.

## Hintergrund

Die Cybersecurity für Sicherungsanlagen ist neues Themenfeld bei der Bahn.

Im Auftrag des BAV erarbeitet die SBB im Rahmen eines Projektes die Methoden und Grundlagen für Security Monitoring und Management für Security im Bereich der Sicherungsanlagen.

Im Austausch mit Partnerbahnen zeigt sich der Bedarf an Austausch von Knowhow und Diskussion zu den Herausforderungen unter Experten und Projektleitern.



## 2. Bedarf, warum eine neue Arbeitsgruppe



### Auswertung Gruppenarbeit

Es wurden zwei Gruppenarbeiten durchgeführt.

Eine erste kurze zur Einschätzung der Top Risiken für die Eisenbahnsysteme aus Sicht der Teilnehmer.

Die zweite Gruppenarbeit hatte zum Ziel anhand der Themenübersicht aus der RL CySec-Rail eine Übersicht über die grössten Herausforderungen, Erfahrungen und Lösungen / Konzepte zu erstellen.



### Key Messages

Die Top drei Risiken zusammengefasst aus den Gruppenarbeiten betreffen:

- Möglichkeiten über menschliches Fehlverhalten und Sabotage (intern und extern)
- Einbruch über Fernwartungszugänge an Sicherungsanlagen
- Soft- und Hardware Schwachstellen in der Lieferkette



### Pain Points – was fehlt

Generell fehlt noch Knowhow, Awareness, fundierte Kenntnisse über Lieferantenmanagement, gute Fachkenntnisse und genügend Ressourcen.

Im Bereich Security bei Sicherungsanlagen sind Profile mit spezifischen SA- und fundierten Security-Kenntnissen gefragt. Da diese bisher primär on the Job ausgebildet werden, sollen hier Möglichkeiten entwickelt und ausgetauscht werden. Eine spätere Überführung ins Programm BTE ist zu prüfen.

### 3. Scope und Zielgruppe



Fokus auf Security (OT) für Sicherungsanlagen

Orientierung an konkreten Inhalten, Methoden und Fallbeispielen.

Spezifische Themen aufnehmen wie z.B. Umsetzung RL CySec Rail, HCBöV, Anwendung NIST Framework.

Hilfsmittel, Anleitungen, Handbücher, Methoden austauschen (geschieht punktuell schon heute)

Erfahrungsaustausche und Gruppenarbeiten durchführen



Die „Macher“

- Fachpersonen in Security für Sicherungsanlagen
- Projektleiter
- Security Manager
- Security Engineers
- Security Architekten
- Entscheidungsträger in Projekten

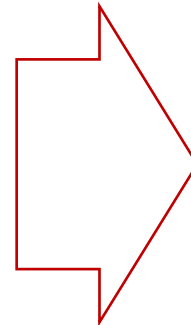
Anbindung an die Fachgruppe Elektrotechnik (FG ET) beim VöV, offen für die Mitglieder des VöV.

Rahmenbedingungen und Vertrauen für einen offenen Austausch mittels Charta schaffen.

## 4. Abgrenzung zu „VöV Arbeitsgruppe CyberSecurity“

### Kernelemente „VöV Arbeitsgruppe CyberSecurity“

1. Koordination von Anfragen von Bundesstellen / Austausch mit dem BAV
2. Austausch zur Bedrohungslage: - Informationen zur aktuellen Lage - Aufbau eines RAIL ISAC
3. Cyber Security im Bereich OT / Bahnanwendungen - Sicherheitsanforderungen für Fahrzeuge und Anlagen - Empfehlungen für praktische Umsetzungsmöglichkeiten
4. Supplier Management: - Abstimmung von Eckwerten von Ausschreibungsunterlagen (mehr gleichgerichteter Druck durch gleiche Anforderungen auf die Hersteller) - Informationsaustausch zu Herstellerprüfungen / Auditergebnisse
5. Abstimmung branchenspezifischer Awarenesssthemen - Tipps und Trick



### „Arbeitsgruppe OT Security Sicherungsanlagen“

1. Sammlung und Behandlung von aktuellen Themen die von den Teilnehmern eingegeben werden.
2. Bei der Erarbeitung und Behandlung von Inhalten Einbezug von hoheitlichen und/oder unternehmensstrategischen Vorgaben.
3. Fokus auf das Umfeld der Sicherungsanlagen und neuer Technologien, Zentralisierung und Virtualisierung von Anlagen.
4. Austausch zu Supply Chain, Vulnerability, Incident und Patchmanagement auf Stufe Fach (Engineer, Architect, ...)
5. Interaktion und Koordination mit „VöV Arbeitsgruppe CyberSecurity“, wo gewünscht.



# 5. Vernetzung der Gruppen „VöV CyberSecurity“ und „OT Security Sicherungsanlagen“

## Gegenseitig Informieren

- Informationsfluss von Fach zu Leitung sicherstellen

## Themen zuspielen

- der neuen Arbeitsgruppe können Aufträge zu Themen gegeben werden

## Resultate teilen

- Protokolle und Ergebnisse aus der Fachgruppe sowie Organisation eines ERFA-Tages (inhaltlich) einmal pro Jahr.

## Gäste einladen

- Bei spezifischen Themen ist es möglich, gegenseitig Gäste einzuladen

## Vertraulichkeit

- Für die AGr wird eine Charta erstellt und damit die Vertraulichkeit und den Rahmen für offene Diskussionen sicher gestellt.

