Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Strassen ASTRA

RICHTLINIE

OT SECURITY

Ausgabe 2024 V2.00
ASTRA 13030

Impressum

Autoren / Arbeitsgruppe

Jolanda Geringer	ASTRA DS-DTI, Vorsitz
Martin Wyss	ASTRA I-B
Markus Berger	ASTRA I-FU
Daniel Gähwiler	CSI Consulting AG, Zürich
Patrick Gerber	CSI Consulting AG, Zürich

Begleitgruppe

Bruno Frey	ASTRA DS-GOV
Wolfgang Hoffmann	ASTRA DS-GOV
Bernard Crausaz	ASTRA DS-UARS
Markus Eisenlohr	ASTRA I-FU
Patrick Fuhrer	ASTRA F3
Peter Baur	ASTRA F4
Ivo Perseghini	ASTRA F5
Daniel Sägesser	GE I
Pascal Roth	GE VIII
Fabio Caspani	GE VIII
Ludovic Roulet	UT IX
Ivo Achermann	GE X
Patrik Imhof	GE XI
Luca Hunziker	IM Maggia Engineering SA, Locarno
Alain Gatti	ingegna SA, Muralto
Markus Schlup	Amstein + Walthert Progress AG, Zürich

Originalsprache
Deutsch

Herausgeber
Bundesamt für Strassen ASTRA
Abteilung Strassennetze N
Standards und Sicherheit der Infrastruktur SSI
3003 Bern

Bezugsquelle
Das Dokument kann kostenlos von www.astra.admin.ch heruntergeladen werden.

Vorwort

Der rasche Fortschritt der Technik und die stetig steigenden Anforderungen an die Strasseninfrastruktur erfordern einheitliche Vorgaben in Bezug auf die Betriebssicherheit. Die Verkehrssicherheit auf dem aktuellen Strassennetz wird heute in hohem Mass durch die Betriebs- und Sicherheitsausrüstungen (BSA) gewährleistet.

Die vorliegende Richtlinie definiert die Grundzüge einer einheitlichen Sicherheitsarchitektur für die Betriebs- und Sicherheitsausrüstungen des ASTRA. Sie wurde abgeleitet aus den Weisungen zur OT-Security Governance des ASTRA, den Vorgaben des Bundes, den Sicherheitsbedürfnissen (Schutzbedarf) mit den Anforderungen an den Informations- und Datenschutz sowie der Risikoanalyse mit dem Anspruch, soviel Sicherheit wie nötig zu gewährleisten, und nicht so viel Sicherheit wie möglich.

Durch die vorliegende Richtlinie soll die Grundlage für ein einheitliches OT-Sicherheitsniveau für die Betriebs- und Sicherheitsausrüstungen des ASTRA gelegt werden.

Die vorliegende Version 2.00 wurde überarbeitet und an den Stand der Technik und an die neue Cyberstrategie des Bundes angepasst. Besondere Berücksichtigung fanden dabei vor allem auch die vielen Besonderheiten der BSA/OT-Umgebung.

Bundesamt für Strassen

Jürg Röthlisberger
Direktor

Inhaltsverzeichnis

1 Einleitung

1.1 Zweck der Richtlinie

Sicherheit bezeichnet einen Zustand, in dem die verbleibenden Risiken als akzeptabel eingestuft wird. Die vorliegende Richtlinie legt Anforderungen und Massnahmen zum Schutz von Elementen der Betriebs- und Sicherheitsausrüstungen (BSA) unter Zuhilfenahme von OT-Mitteln fest, um die Sicherheit in genügendem Masse zu gewährleisten.

1.2 Geltungsbereich

Da IT- und OT-Security einerseits Gemeinsamkeiten aber andererseits auch grosse Unterschiede aufweisen, werden die beiden Security-Themen getrennt behandelt und über separate Richtlinien gesteuert. Die vorliegende Richtlinie behandelt nur den OT-Security-Bereich.

Die Richtlinie gilt verbindlich für die Planung, die Projektierung, die Realisierung und den Betrieb der Kommunikations-, Leit- und Steuersysteme (OT-Systeme) sämtlicher Betriebs- und Sicherheitsausrüstungen (BSA) der Nationalstrasse.

1.3 Adressaten

Die Richtlinie wendet sich an:

- Fachspezialisten und Erhaltungsplaner BSA des ASTRA;
- Fachspezialisten BSA der Gebietseinheiten;
- Projektleiter SA-CH des ASTRA;
- Projektleiter des ASTRA (bei Projekten mit Steuer- und Leittechnik);
- Planer und Unternehmungen, die im Auftrag des ASTRA Tätigkeiten an den BSA ausführen.

1.4 Inkrafttreten und Änderungen

Die Richtlinie tritt am 01.03.2016 in Kraft. Die „Auflistung der Änderungen“ ist auf Seite 27 dokumentiert.

2 Begriffe

In der vorliegenden Richtlinie werden folgende spezifischen Begriffe verwendet:

- **Security Management System (SMS):** Ein Security Management System (SMS) definiert die Regeln und Methoden, um die Security innerhalb einer Organisation oder eines Bereichs zu gewährleisten;
- **Sicherheitsniveau**: Unter dem Begriff Sicherheitsniveau versteht man das Ausmass an geforderter oder vorhandener Sicherheit;
- Die **Betriebs- und Sicherheitsausrüstung (BSA)** umfasst elektromechanische sowie steuer- und leitechnischen Anlagen, welche für den Betrieb und die Sicherheit der Nationalstrassen dienen;
- **OT und OT-System (System):** OT steht für Operational Technology und ist die Verwendung von Hardware und Software zur Überwachung und Steuerung von physischen Prozessen, Geräten und Infrastrukturen. Die OT umfasst damit die Steuer- und Leittechnik der BSA, die dazu benötigte Infrastruktur (bspw. IP-Netz BSA), die OT-Systeme als auch die Applikationen und Services. OT-Systeme und Aggregate sind Teil der BSA;
- **Netzwerkzone (Zone):** Eine Zone ist ein logischer Verbund von OT-Systemen, die sich durch gemeinschaftliche Aufgaben auszeichnen und der gleichen Zonenpolicy unterliegen. Die netzwerkmässige Erschliessung einer Zone erfolgt über Netzwerkkomponenten, während die Durchsetzung der Regeln der Zonenpolicy über Sicherheitselemente erfolgt;
- **Sicherheitselemente** / Policy Enforcement Point (PEP): Sicherheitselemente dienen der Durchsetzung von Regeln (von Policies) an einem Policy Enforcement Point (Übergangspunkt zweier Zonen). Sicherheitselemente haben verschiedene Ausprägungen und Funktionen wie bspw. Firewalls, dynamische Paketfilter, Applikationsprotokoll-Gateways, Proxy Server oder Reverse Proxy Server.

3 OT-Security Management System (OT-SMS)

Das OT- Security Management System (OT-SMS) definiert die Regeln und Methoden, um die Security innerhalb des ASTRA zu gewährleisten. Das OT-SMS ist in den ASTRA Weisungen zur OT-Security Governance verankert und wird in der vorliegenden Richtlinie detaillierter beschrieben.

Mit dem OT-SMS stellt das ASTRA sicher, dass

- ein einheitliches OT-Sicherheitsniveau erreicht wird;
- eine einheitliche Sicherheitsarchitektur befolgt wird;
- unter Berücksichtigung der Bedrohungslage und den daraus abgeleiteten Risikoszenarien so viel Sicherheit wie nötig und nicht so viel Sicherheit wie möglich gewährleistet wird.

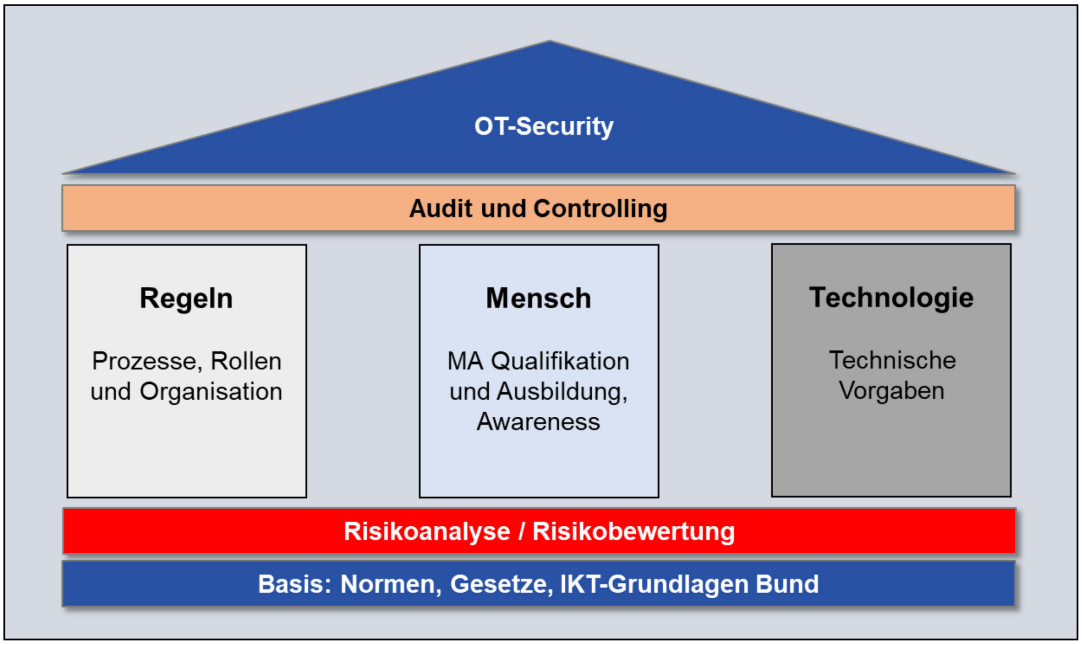

Abb. 3.1 OT-Security Management System (OT-SMS) der Nationalstrassen

In den folgenden Kapiteln werden einerseits die Risikoszenarien aufgezeigt und andererseits die Regeln und die Methoden der drei Grundbausteine Regeln, Mensch und Technologie des OT-SMS erläutert:

- Kap. 4 zeigt Bedrohungen, Schutzbedarf und -ziele auf;
- Kap. 5 beschreibt Prozesse mit Schwerpunkt OT-Sicherheitsorganisation, Rollen und Organisation;
- Kap. 6 beschreibt die Vorgaben und Bestimmungen bezüglich Qualifikation und Ausbildung der Mitarbeiter und Awareness im Bereich OT-Security auf;
- Kap. 7 beschreibt die Vorgaben und Bestimmungen bezüglich technischer Systeme und Umgang mit den OT-Systemen.

4 Bedrohungen, Schutzbedarf und -ziele

Vorbemerkung: Auf Stufe Bund existieren Stand diese Ausgabe noch keine Vorgaben zum Thema OT-Security. Das Thema ist beim Bund in Bearbeitung und wird ASTRA-seitig eingearbeitet, sobald die Vorgaben verfügbar sind.

4.1 Risiko- und Bedrohungsanalyse

Die Risikoanalyse ist im Risikomanagement die Analyse der durch Risikoidentifikation ermittelten Risiken von unterschiedlichen Sachverhalten und Gefahrensituationen. Bei der Risikoanalyse kommen unterschiedliche Analysetechniken zur Anwendung, wie bspw. die qualitative Analyse und die quantitative Analyse. Das quantitative Risiko ergibt sich aus der Multiplikation der Schadenshöhe mit der Eintrittswahrscheinlichkeit bzw. der Gefährdungsrate. Bei der Risikoanalyse steht das Ausmass des Schadenpotentials und deren Kosten für das ASTRA im Mittelpunkt.

Die Bedrohungsanalyse ist ein Teilbereich des Risikomanagements. Mithilfe der Bedrohungsanalyse im Kontext eines OT-Systems lassen sich die verschiedenen Bedrohungen für OT-Systeme und OT-Prozesse systematisch erfassen, strukturieren und bewerten. Aus den identifizierten Bedrohungen und der Einschätzung der Gefährdungslage lassen sich als Ergebnis die einzelnen Risiken für das Risikomanagement ableiten.

4.2 Bedrohungen und Risikoszenarien

In der nachfolgenden Tabelle sind die möglichen Gefahren / Bedrohungen für die OT-Infrastruktur BSA aufgelistet und konkretisiert.

Tab. 4.1 Gefahren/Bedrohungen

G-Nr.	Beschreibung
G1	Social Engineering (Phishing, Dumpster Diving) / Ausspähen von Informationen (Spionage)
G2	Einschleusen von Schadsoftware über Internet, Intranet, Wechseldatenträger oder externer Hardware
G3	Infektion mit Schadsoftware über Internet, Intranet, Wechseldatenträger oder externer Hardware
G4	Unbefugtes Eindringen in OT-Systeme (bspw. Eindringen über Wartungszugänge)
G5	Missbrauch von Berechtigungen (unberechtigte Nutzung/Administration von Geräten und Systemen)
G6	Mit dem Internet verbundene Steuerungskomponenten
G7	Sicherheitslücke in der Software
G8	Ausfall oder Störung von Kommunikationsnetzen
G9	Offenlegung schützenswerter Informationen
G10	Ausfall / Fehlfunktion von Geräten oder Systemen
G11	Lokaler Stromausfall
G12	Personalausfall / Personalmangel

Tab. 4.2 Gefahren/Bedrohungen, die nicht im Fokus stehen

G-Nr.	Beschreibung
G13	Staatlicher Terrorismus
G14	Höhere Gewalt (grossflächiger Stromausfall, Naturkatastrophen, Pandemien), Ausfall von Lieferanten, technische Katastrophen (Explosionen und Brände, Einsturz von Bauwerken, Verkehrsunfälle [Massenautounfälle, Flugzeugabstürze, Zugentgleisungen, Schiffsunglücke, etc.], Radioaktive Unfälle)
G15	Vorsätzliche Handlungen wie Missbrauch, Diebstahl

Daraus ergeben sich verschiedene mögliche Risikoszenarien im BSA-Umfeld:

Tab. 4.3 Risikoszenarien

R-Nr.	Titel	Risikoszenario	Mögliche Auswirkungen
R1	Fehl-manipulation	• Ausgelöst durch einen Menschen	• Erschwerter Verkehr auf den Nationalstrassen • Ausfall von BSA-Komponenten • Gefahr für Personen
R2	Falschalarm	• Störung der Alarmsysteme löst Fehlalarme aus	• Vertrauensverlust bei Alarmorganisation Imageschaden • Zeitverlust der Mitarbeiter • Unbeobachtetes Zeitfenster für Angreifer (weil die Mitarbeiter mit den Fehlalarmen beschäftigt sind)
R3	Schadsoftware (Malware)	• Malware oder Ransomware im IP-Netz BSA • Malware wird über die OT-Systeme in das Client Netz des ASTRA verbreitet • OT-Systeme werden verschlüsselt • Konfigurationen der OT-Systeme werden gelöscht (automatisches ausführen von einem Reset)	• Längerfristiger Totalausfall der BSA-Funktionalität • Im schlimmsten Fall sind weite Teile des ASTRA betroffen. • Manipulation von Anlagen, Verlust und/oder Änderung der Konfiguration der Aggregate auf der Feldebene • Verkehrseinschränkungen auf den schweizerischen Nationalstrassen • Gefahr für Personen • Datenverlust
R4	Netzausfall	• Ausfall der Netzwerkverbindung • Ausfall des Stromnetzes	• Verlust der zentralen Übersicht. • Ausfall der Alarmierung BSA • Verkehrseinschränkungen auf den Nationalstrassen • Ausfall von BSA-Komponenten
R5	Offenlegung von Informationen (Information Disclosure)	• Unbefugte erhalten Einsicht in Daten der Nationalstrassen • Verlust von sensitiven Daten (bspw. Daten aus dem Bereich SZP-BSA)	• Daten werden veröffentlicht • ASTRA wird erpresst • Daten werden an den Höchstbietenden verkauft
R6	Funktions-ausfall	• Ausfall der Zentralsysteme, Leittechnik, Alarmierung • Ausfall dezentraler Systeme	• Verlust der zentralen Übersicht. • Ausfall der Alarmierung BSA • Verkehrseinschränkungen auf den schweizerischen Nationalstrassen • Ausfall von BSA-Komponenten • Gefahr für Personen
R7	Fehlfunktion	• Technisch bedingte Fehlfunktion	• Verkehrseinschränkungen auf den schweizerischen Nationalstrassen

Tab. 4.3 Risikoszenarien

R-Nr.	Titel	Risikoszenario	Mögliche Auswirkungen
			• Ausfall von BSA-Komponenten • Gefahr für Personen
R8	Vandalismus	• Nicht geschützte Komponenten der BSA werden manipuliert	• Verkehrseinschränkungen auf den Nationalstrassen • Ausfall von BSA-Komponenten • Zerstörung von OT-Geräten
R9	Datenverlust	• Die Daten zur BSA-Steuerung gehen verloren • Verlust von sensitiven Daten • Verlust von Backups	• Wenn Parameterdaten einer Anlagesteuerung verloren gehen, kann dies u.U. signifikanten Einfluss auf die Verfügbarkeit haben • Historische Daten stehen nicht mehr zur Verfügung. Optimierungen verzögern sich • Verlust von Dokumentationen
R10	Wiederanlauf	• Systemen kann nicht mehr gestartet werden	• Ausfall der Alarmierung BSA • Erschwertes Fahren auf den Nationalstrassen • Ausfall von BSA-Komponenten
R11	Personalausfall	• Systeme können nicht mehr bedient werden • Störungen können nicht mehr behoben werden	• Störungen/Alarme werden nicht bearbeitet; Erschwertes Fahren auf den Nationalstrassen • Ausfall von BSA-Komponenten

5 Regeln: Prozesse, Rollen und Organisation

5.1 Übersicht

Folgende Rollen und Gremien sind im Kontext OT-Security relevant:

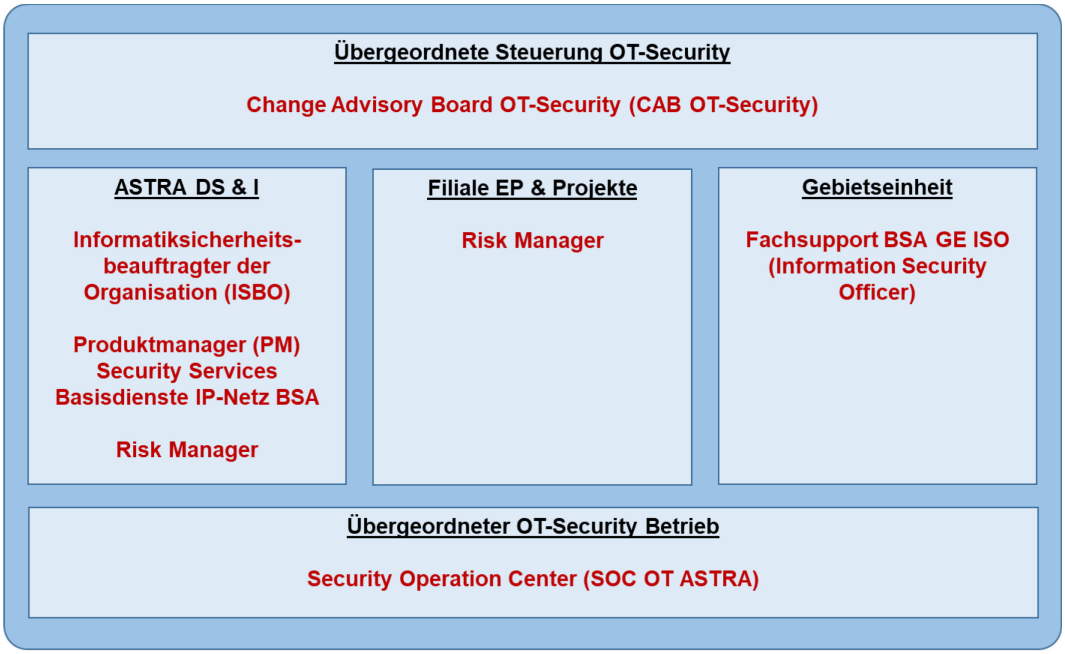

Abb. 5.1 Übersicht der Rollen und Gremien im Kontext OT-Security

Zukünftige und weitere Rollen werden bei der Revision der ASTRA Weisungen 73001 / 73002 beschrieben.

5.2 Security Rollen

Tab. 5.4 Security Rollen

Rolle	Beschreibung	Stelle / Organisationseinheit
Informatiksicherheitsbeauftragter der Organisation (ISBO) (gem. ISO 27000 ist das der Informationssicherheitsbeauftragte)	Der ISBO koordiniert die IKT-Sicherheitsaspekte innerhalb des ASTRA sowie mit den übergeordneten Bundesstellen. Er erarbeitet die notwendigen Grundlagen für die Umsetzung der IKT-Sicherheitsvorgaben auf Stufe ASTRA. Der ISBO organisiert die Schutzbedarfsanalysen (SCHUBAN) und ist im ASTRA die Anlaufstelle für generelle Sicherheitsprobleme.	ASTRA DS
Risk Manager	Der Risk Manager befasst sich mit der Analyse, Beurteilung und Steuerung von Risiken. Er identifiziert Schwachstellen, die das ASTRA unter finanziellen, operativen oder sicherheitstechnischen Aspekten schädigen könnten, beugt ihnen vor und koordiniert Lösungsvorschläge bei der Umsetzung. Er ist verantwortlich für die Entwicklung von Strategien, Prozessen und Systemen für Risk-Management und -überwachung zum Schutz der Geschäftskontinuität.	Die Rolle des Risk Managers wird auf Stufe ASTRA zentral und Filiale wahrgenommen.

Tab. 5.4 Security Rollen

Rolle	Beschreibung	Stelle / Organisationseinheit
Information Security Officer (ISO)	Der ISO ist eine von der GE-Leitung benannte Person, die im Auftrag der Leitungsebene dafür sorgt, dass die Sicherheitsanforderungen im Bereich der OT-Infrastruktur (u.a. Firewall) mit ihren industriellen Steuerungen abgedeckt sind und die Sicherheitsorganisation aus dem Bereich ISO in das OT-SMS (OT-Security Management System) eingebunden ist.	Fachsupport BSA Gebietseinheit (FaS BSA GE)
Produktmanager (PM) Security Services Basisdienste IP-Netz BSA	Der Produktmanager Security Services BD IP-Netz BSA ist eine Rolle, die sich um den Aufbau und die Weiterentwicklung der zentralen Dienste und Tools wie IAM BSA, Multifactor Authentication/MFA, Single-Sign-On, Security Dashboard IP-Netz BSA in enger Abstimmung mit den Stakeholdern ASTRA, der Filialen, Gebietseinheiten und Lieferanten kümmert.	Produktmanager (PM) Security Services Basisdienste IP-Netz BSA

5.3 Übergeordnete Steuerung OT-Security

Das Change Advisory Board (CAB OT-Security) koordiniert die OT-Sicherheit für den Betrieb der BSA und übernimmt das Changemanagement für die übergeordneten Funktionen. Es werden auch Empfehlungen oder Entscheidungen bezüglich den GE Aufgaben getroffen, welche die Sicherheit betreffen.

Das CAB OT-Security ist ein zentrales Gremium auf Stufe ASTRA. Im Gremium müssen mindestens folgende Rollen vertreten sein:

- Informatik Controlling-Beauftragter der Organisation (ICBO);
- Informatiksicherheitsbeauftragter der Organisation (ISBO);
- Vertreter I-B;
- Vertreter I-FU / Fachunterstützung BSA SA-CH;
- Programmleitung SA-CH;
- Mindestens zwei Vertreter der GE (GE ISO).

5.4 Security Operation Center OT (SOC OT ASTRA)

Das Security Operation Center OT (SOC OT ASTRA) ist die zentrale Anlaufstelle für Sicherheitsthemen der OT-Systeme der BSA. Das SOC OT ASTRA setzt Menschen, Prozesse und Technologie ein, um die Sicherheitslage der BSA kontinuierlich zu überwachen und zu verbessern und gleichzeitig Cybersecurity-Vorfälle zu verhindern, zu erkennen, zu analysieren und darauf zeitnah zu reagieren.

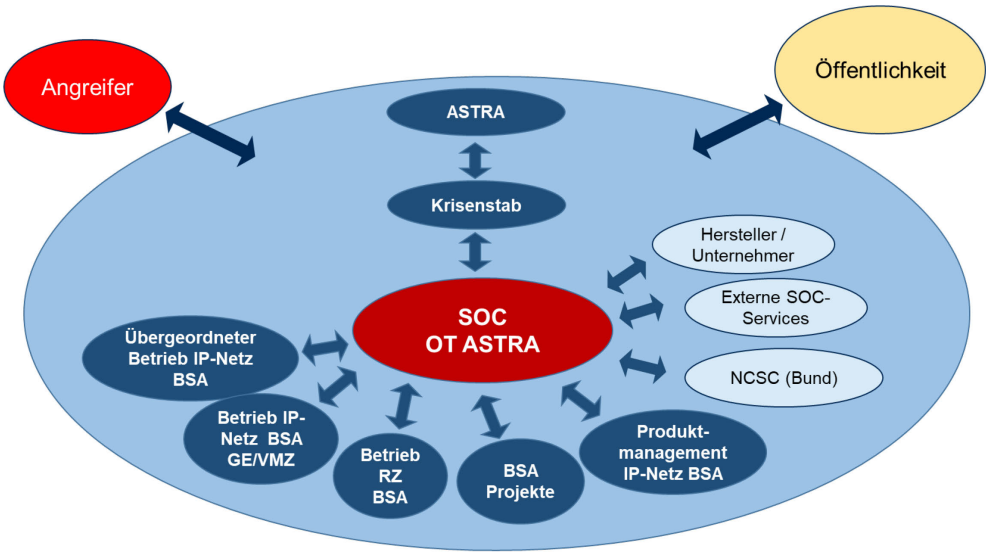

Abb. 5.2 Das SOC OT im Kontext der Stakeholder

Das SOC OT ASTRA wird über spezialisierte Fachkräfte verfügen und in den nächsten Jahren kontinuierlich aufgebaut werden.

6 Mensch: Qualifikation, Ausbildung und Awareness

6.1 Know-how, Ausbildung und Awareness

Tab. 6.5 Know-how, Ausbildung und Awareness

ID	Beschreibung	
GS-1	Sensibilisierung und Schulung	
	GS-1.1	Alle Benutzerinnen und Benutzer von OT-Systemen müssen im Bereich der OT-Sicherheit stufen- bzw. funktionsgerecht sensibilisiert und geschult sein.
	GS-1.2	Sie müssen die für OT-Systeme relevanten Einsatzrichtlinien kennen und sind zu deren Einhaltung verpflichtet.
	GS-1.3	Sie müssen jährlich ein Training zum bewussten Umgang mit OT-Systemen absolvieren (Awareness-Training).
GS-2	Meldepflicht	
	GS-2.1	Alle Benutzerinnen und Benutzer von OT-Systemen müssen Ereignisse, wie z.B. anormales und verdächtiges Systemverhalten oder physischer Verlust, möglichst zeitnah der dafür zuständigen Stelle melden.
GS-3	Personensicherheitsprüfung (PSP)	
	GS-3.1	Personensicherheitsprüfungen sind grundsätzlich nicht notwendig.
	GS-3.2	Die Personensicherheitsprüfung erfolgt nur bei Personen in sicherheitsempfindlichen Funktionen mit Zugang zu klassifizierten Informationen, Materialien oder Anlagen.
GS-4	Security Rollen	
	GS-4.1	Die Security Rollen gem. Kap. 5.2 sind zu besetzen.

7 Technologie: Technische Vorgaben

7.1 Grundsätze und Prinzipien

Bei der OT-Sicherheit werden die gleichen Prinzipien angewendet wie beim Bau der BSA-Infrastruktur. D.h. die Sicherheit wird auch wie alle BSA-Anlagen im Zwiebel-Schalenprinzip aufgebaut. Der Datenaustausch erfolgt nur über definierte Schnittstellen/Zugänge und die Gebietseinheitsnetze sind in sich geschlossen.

Wenn ein Mechanismus fehlschlägt, schaltet sich sofort ein anderer ein, um einen Angriff zu vereiteln. Dieser mehrschichtige Ansatz mit gezielten Redundanzen erhöht die Sicherheit eines Systems als Ganzes und richtet sich gegen viele verschiedene Angriffsvektoren.

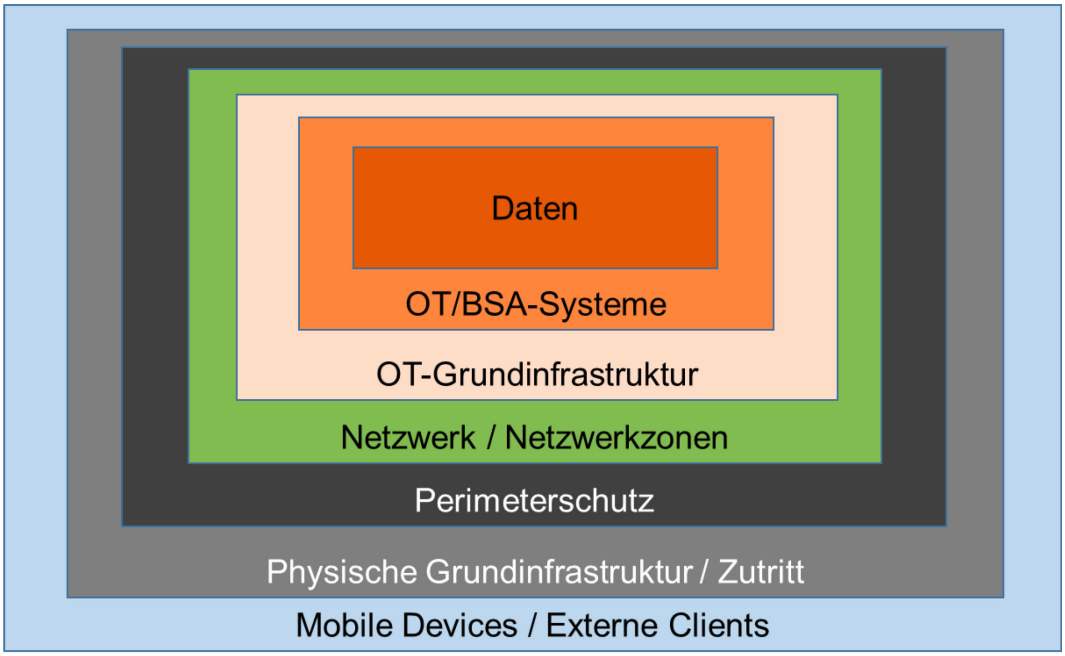

Abb. 7.1 Prinzip der mehrschichtigen Security-Anforderungen / Massnahmen – «Defense-in-Depth»-Prinzip

Zusätzlich gelten folgende Prinzipien:

Stand der Technik: Alle eingesetzten (präventiv, detektiv und/oder reaktiv wirkenden) Sicherheitsmassnahmen müssen dem Stand der Technik entsprechen, idealerweise standardisiert und im operativen Betrieb erprobt sein. Massnahmen, die veraltet sind oder für die relevante Verwundbarkeiten oder Schwachstellen bekannt sind, müssen zeitnah und unabhängig vom Lifecycle nachgebessert oder ersetzt werden. Als Stand der Technik gilt der aktuelle Entwicklungsstand bei Verfahren, Einrichtungen und Betriebsweisen, der bei vergleichbaren Anlagen im In- und Ausland erfolgreich erprobt ist oder bei Versuchen erfolgreich eingesetzt wurde und nach den Regeln der Technik auf andere Anlagen übertragen werden kann; und wirtschaftlich tragbar ist.

«Least Privilege»- bzw. «Need-to-Know»-Prinzip: Die Vergabe von Zugriffsrechten und Privilegien muss minimal erfolgen.

«Security by Design»-Prinzip: Bei der Entwicklung von Hard- und Softwarekomponenten bzw. deren Einsatz in OT-Systemen und Anwendungen muss die Sicherheit von Anfang an mitberücksichtigt und aktuell gehalten werden, so dass diese möglichst frei von Schwachstellen und Verwundbarkeiten sind und entsprechende Angriffsmöglichkeiten klein gehalten werden.

«Security by Default»-Prinzip: BSA-Anlagen müssen so entwickelt, konfiguriert und betrieben werden, dass alle in einem spezifischen Umfeld sinnvollen Sicherheitsmassnahmen standardmässig aktiviert sind und ihre Wirkung entfalten können, ohne dass sich die Benutzerinnen und Benutzer darum kümmern müssen.

Nachvollziehbarkeit, Audit Trail: Die Systeme müssen so aufgebaut sein, dass im Schadensfall die Nachvollziehbarkeit von User- und Systemaktivitäten vorgelegt werden kann.

7.2 Grundschutz

Der Grundschutz legt die minimale Sicherheit fest, die von allen involvierten Systemen erreicht werden muss. Wo zusätzliche Sicherheitsvorschriften bestehen, müssen diese befolgt werden. Falls ein Widerspruch zwischen den Bestimmungen vorliegt, gehen jene Vorschriften vor, die ein höheres Sicherheitsniveau zur Folge haben.

Wo begründete Abweichungen vom Grundschutz notwendig werden, sind diese zu dokumentieren und durch das CAB OT-Security freizugeben.

7.2.1 Informationen (Daten)

Tab. 7.6 Grundschutz Informationen (Daten)

ID	Beschreibung	
GS-5	Zulässigkeit von OT-Systemen	
	GS-5.1	Geschäftsrelevante Informationen dürfen nur auf OT-Systemen gespeichert und verarbeitet werden, deren Inhaber entweder eine Verwaltungseinheit der Bundesverwaltung oder für die die Einhaltung der sicherheitstechnischen Anforderungen aus dieser Vorgabe vertraglich geregelt ist (z.B. im Rahmen einer RZ-Lösung).
GS-6	Vertraulichkeit und Integrität	
	GS-6.1	Die eingesetzten OT-Systeme müssen geeignet sein, den Schutz der Vertraulichkeit und Integrität der Informationen zu gewähren.
	GS-6.2	Der Einsatz von kryptografischen Verfahren ist nur dort vorzusehen, wo dies aufgrund des Schutzbedarfs absolut notwendig ist.
	GS-6.3	Werden Informationen verschlüsselt, dann müssen die dazu verwendeten Schlüssel so verwaltet werden, dass eine Wiederherstellung und damit eine Entschlüsselung der Informationen jederzeit möglich ist. In der Regel bedingt das eine aufwändige Schlüsselverwaltung (mit einem «Key Recovery»-Mechanismus) sowie ein periodisches Austesten der Wiederherstellbarkeit der Informationen.
GS-7	Verfügbarkeit, Backup und Restore	
	GS-7.1	Die Verfügbarkeit von geschäftsrelevanten Informationen muss jederzeit dem Schutzbedarf entsprechend sichergestellt sein.
	GS-7.2	Der für Informationen verantwortliche Betreiber muss über eine Backup-Strategie verfügen und diese auch umsetzen. Diese Strategie muss ein Mehrgenerationen-Prinzip und eine offline Speicherung wichtiger Datenbestände vorsehen, so dass Daten auch im Falle von datenverschlüsselnder Malware («Ransomware») wiederhergestellt werden können.
	GS-7.3	Die Wiederherstellung von Daten (Restore) muss mindestens einmal jährlich getestet werden. Zusätzlich ist die Wiederherstellung immer dann zu testen, wenn sich die OT-Systeme grundlegend ändern.
GS-8	Datenträger	
	GS-8.1	Die Datenträger, auf denen geschäftsrelevante Informationen gespeichert sind, müssen jederzeit dem Schutzbedarf der Informationen entsprechend geschützt sein. Namentlich für die Reparatur und Entsorgung von Datenträgern müssen geeignete Prozesse definiert und umgesetzt sein.
	GS-8.2	Die Verwendung von mobilen Datenträgern wie USB-Sticks, etc. ist nicht gestattet.

7.2.2 OT-Systeme

Tab. 7.7 OT-Systeme

ID	Beschreibung
GS-9	Konfiguration und Einstellung
	GS-9.1 Ein OT-System muss vor der Inbetriebnahme in der Produktivumgebung so konfiguriert und eingestellt sein, dass es vor unberechtigtem Zugriff geschützt ist, es soweit technisch möglich gehärtet ist und in einer zur Aufgabenerfüllung erforderlichen und vom Benutzer nicht veränderbaren Minimalkonfiguration betrieben wird (d.h. nicht genutzte Schnittstellen, Module, Dienste und Funktionen müssen deaktiviert sein), und wichtige sicherheitsrelevante Aktivitäten und Ereignisse (mit Zeitangaben) aufgezeichnet und zeitnah ausgewertet werden.
	GS-9.2 Sicherheitskonfigurationen und -einstellungen dürfen nur autorisiert aktiviert, geändert, deaktiviert und deinstalliert werden.
GS-10	Produktive Umgebung
	GS-10.1 Die produktive Umgebung des OT-Systems muss von einer allenfalls vorhandenen nicht produktiven Umgebung (z.B. für Entwicklung und/oder Test) getrennt sein.
GS-11	Wartung und Pflege
	GS-11.1 Für ein OT-System und ihre Komponenten (z.B. Software-Bibliotheken, Treiber) müssen während der ganzen Lebensdauer eine professionelle Wartung und Pflege sichergestellt sein. Darunter fällt insbesondere auch die Einspielung von regelmässigen und betrieblich oder sicherheitstechnisch notwendigen Updates und Fehlerkorrekturen (Patches). Die dafür notwendigen Wartungs- und Supportverträge sind vorzusehen.
	GS-11.2 Hardware und Software ist grundsätzlich vor End of Support zu ersetzen.
GS-12	Integritäts- und Malwareschutz
	GS-12.1 Die Integrität der auf dem OT-System eingesetzten Softwarekomponenten muss sichergestellt sein (z.B. mit Hilfe von digitalen Signaturen). Insbesondere muss jedes Server-System mit erhöhtem Schutzbedarf regelmässig einer Integritätsprüfung unterzogen werden.
	GS-12.2 Wird ein Integritätsverlust festgestellt, muss das OT-System vom Netzwerk getrennt, gesichert und untersucht werden. Im Falle einer bestätigten Kompromittierung muss je nach OT-System und erhaltener Malware das weitere Vorgehen geprüft werden (Neuaufsetzen, Ersatz, etc.).
	GS-12.3 Das OT-System muss in ein Malwareschutzkonzept eingebunden sein, das insbesondere auch regelt, wie bei einem Malwarebefall vorzugehen ist und welche Stellen wie informiert werden müssen.
GS-13	GS-13.1 Für betriebskritische OT-Systeme sind für einen Ausfall oder Teilausfall dieser Systeme Notfallprozesse und Wiederanlaufszenarien vorzubereiten. Insbesondere für Safety-relevante OT-Systeme sind diese Notfallprozesse und Wiederanlaufszenarien regelmässig zu üben und zu verbessern.
GS-14	GS-14.1 Für jegliche Änderungen an einem OT-System ist ein definierter Change Management Prozess einzuhalten. Im ordentlichen Betrieb ist dafür die Gebietseinheit zuständig, im Projektmodus erfolgen die Änderungen gemäss den Vorgaben der Filiale. Für zentrale Systeme der Management Ebene sind die entsprechenden Leistungserbringer zuständig.

7.2.3 OT-Grundinfrastruktur

Tab. 7.8 OT-Grundinfrastruktur

ID	Beschreibung
GS-15	Betrieb
	GS-15.1 Das OT-System muss unter Berücksichtigung von branchenüblichen Sicherheitsvorgaben und -empfehlungen («Best Practices») betrieben werden.
GS-16	Identitäten, Rollen und Berechtigungen
	GS-16.1 Für jedes in der Domäne nationalstrassen.admin.ch betriebene OT-System muss ein Berechtigungskonzept vorliegen, das die Berechtigungsvergabe anhand des Prinzips «Need-to-Know» regelt. Die Berechtigungen sind so zu vergeben, dass ein Benutzer nur vorgesehene Aktivitäten durchführen kann.
	GS-16.2 Die Benutzeridentitäten und Benutzerrollen müssen über das IAM BSA verwaltet werden. Insbesondere müssen die Benutzeridentitäten mindestens jährlich in Bezug auf Notwendigkeit und Richtigkeit überprüft und nicht mehr benötigte Benutzer gelöscht werden.
	GS-16.3 Alle Zugriffsrechte auf ein OT-System müssen im Rahmen eines definierten und dokumentierten Prozesses verwaltet und stets aktuell gehalten werden. Insbesondere müssen die Rechte mindestens jährlich in Bezug auf Notwendigkeit und Richtigkeit durch den Betreiber überprüft und nicht mehr benötigte Rechte entfernt werden.
GS-17	Benutzeranmeldung und Authentifikation
	GS-17.1 Der Zugriff auf OT-Systeme basiert auf persönlichen Logins.
	GS-17.2 Die Authentifikation eines Benutzers gegenüber einem OT-System muss mittels einer 2-Faktoren-Authentifikation erfolgen. Erfolgt die Anmeldung eines Benutzers von einer festen Bedienstation, welche direkt am OT-Netz angeschlossen ist, innerhalb eines überwachten Raumes der GE/ASTRA aus, so genügt eine Authentifikation mittels Benutzer-ID und Passwort.
	GS-17.3 Gruppen-Accounts/-logins werden grundsätzlich nicht zugelassen.
GS-18	Passwörter Für die Benutzerauthentifizierung mittels Passworts gelten die folgenden Anforderungen.
	GS-18.1 Das Passwort • muss persönlich sein; • darf nicht weitergegeben werden; • darf nicht aufgeschrieben werden. Das Passwort kann aber beispielsweise in einem Password-Safe verwaltet werden; • muss mindestens 12 Zeichen lang sein, wobei die Zeichen aus mindestens drei der vier Kategorien Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen stammen müssen; • darf auch mit einem Kleinbuchstabe, Zahl oder Sonderzeichen beginnen; • darf auch ein Satz sein wie bspw. «heuteum12Uhrhatteich12$gewechselt»; • hat keine maximale Gültigkeitsdauer.
	GS-18.2 Ein administrativ gesetztes Initialpasswort muss bei seinem Erstgebrauch geändert werden.
	GS-18.3 Wenn das Passwort geändert wird, muss sichergestellt sein, dass das neue Passwort keinem der 10 zuletzt verwendeten Passwörtern entspricht.
	GS-18.4 Nach maximal 5 Fehleingaben muss das Passwort gesperrt und darf nur im Rahmen eines definierten Prozesses wieder freigegeben werden.
	GS-18.5 Bei Verdacht (oder Bestätigung) auf Kenntnisnahme durch Unberechtigte oder Missbrauch muss das Passwort umgehend geändert werden.
	GS-18.6 Server-seitig muss sichergestellt sein, dass das Passwort nie im Klartext ausgelesen oder im Rahmen eines anderen Angriffs leicht kompromittiert werden kann.
	GS-18.7 Passwörter müssen nur dann geändert werden, wenn ein Verdacht auf Missbrauch vorliegt
	GS-18.8 Auto-Logout oder Sperrbildschirm nach einer inaktiven Zeitspanne von min. (durch Betrieb festzulegen), (ausser spezielle Clients z.B. Zentrale)
GS-19	Administrative Zugriffe und Fernzugriffe

Tab. 7.8 OT-Grundinfrastruktur

ID	Beschreibung
	GS-19.1 Administrative Zugriffe auf OT-Systeme müssen auf eine dokumentierte und kontrollierte Art und Weise erfolgen. Insbesondere müssen solche Zugriffe mittels sicherer Protokolle erfolgen, nachvollziehbar aufgezeichnet und ausgewertet werden können.
	GS-19.2 Die Nutzung der entsprechenden (privilegierten) Konti muss einer Person zugeordnet werden können. Zudem dürfen die Konti nur über minimal erforderliche und möglichst kurzlebige Zugriffsrechte verfügen.
GS-20	Monitoring, Logging
	GS-20.1 Sämtliche OT-Systeme müssen, soweit dies technisch machbar ist, aktiv überwacht (Monitoring-Konzept) werden. Ebenso muss ein Logging aktiviert sein und Logs müssen systematisch und zeitnah auswertet werden, damit Anomalien wie zum Beispiel Angriffsversuche, Fehlverhalten, Hardware-Probleme etc. frühzeitig entdeckt werden können.
	GS-20.2 Log-Files bzw. Loggings müssen mindestens 12 Monate aufbewahrt werden. Dabei ist sicherzustellen, dass die Log-Daten geschützt bleiben und nicht manipuliert werden.

7.2.4 Netzwerk / Netzwerkzonen

Tab. 7.9 Netzwerk / Netzwerkzonen

ID	Beschreibung
GS-21	Geschlossenes Netz (gilt analog auch für die bestehenden Netze der GE)
	GS-21.1 Das IP-Netz BSA ist als geschlossenes Netz im Sinne eines OT-Netzes zu betreiben. Die Trennung von den Office-Netzen ist dabei strikt einzuhalten. Die Vorgaben erfolgen in der ASTRA Richtlinie 13040 IP-Netz BSA.
GS-22	Zonenmodell (gilt für die neuen Netze IP-Netz BSA GE, nicht anwendbar auf die bestehenden Netze der GE)
	GS-22.1 Das IP-Netz BSA setzt ein Zonenmodell konform zum Zonenmodell Bund um.
GS-23	NSP IP-Netz BSA (gilt für die neuen Netze IP-Netz BSA GE, nicht anwendbar auf die bestehenden Netze der GE)
	GS-23.1 Die ASTRA Dokumentation 83042 Network Security Policy IP-Netz BSA (NSP IP-Netz BSA) regelt den Aufbau und den Betrieb des Zonenmodells. Sie gilt als Policy für sämtliche im Perimeter IP-Netz BSA umgesetzten Zonen. Abweichungen davon müssen durch die jeweiligen Betreiber begründet und schriftlich festgehalten werden. Eine Freigabe erfolgt durch das CAB OT-Security.
GS-24	Zonenzugehörigkeit (gilt für die neuen Netze IP-Netz BSA GE, nicht anwendbar auf die bestehenden Netze der GE)
	GS-24.1 Jedes OT-System muss einer Netzwerkzone zugehören und die entsprechenden Policy-Anforderungen aus der Network Security Policy IP-Netz BSA (NSP IP-Netz BSA) erfüllen und gemäss der NSP IP-Netz BSA betrieben werden.
	GS-24.2 Die OT-Systeme müssen inventarisiert sein.
GS-25	WLAN (gilt analog auch für die bestehenden Netze der GE)
	GS-25.1 WLAN ist grundsätzlich zugelassen und erfolgt gemäss den Vorgaben der Network Security Policy IP-Netz BSA.

7.2.5 Perimeterschutz

Tab. 7.10 Perimeterschutz

ID	Beschreibung
GS-26	Fernzugriff
	GS-26.1 Der Fernzugriff (Remote Access) erfolgt zentral über die beiden Zugangspunkte in den Basisdiensten IP-Netz BSA BD A/B gemäss den Vorgaben aus der NSP IP-Netz BSA.
	GS-26.2 Der Fernzugriff erfolgt immer mittels 2-Faktor Authentisierung.
	GS-26.3 In der Migrationsphase IP-Netz BSA dürfen die Fernzugriffe noch über die lokalen externen Zugänge in den Netzen der Gebietseinheiten erfolgen. Grundsätzlich sind auch da die Vorgaben aus der NSP IP-Netz BSA zu befolgen.
	GS-26.4 Grundsätzlich dürfen die Fernzugriffe (Remote Access) nur zeitlich begrenzt geöffnet werden und müssen überwacht sein. Es ist sicherzustellen, dass sich ein Benutzer nach max. 24h erneut anmelden muss.
	GS-26.5 Während eines Fernzugriffes müssen sich die Benutzer beim Verlassen des Arbeitsplatzes abmelden.
	GS-26.6 Jumphosts müssen für Fernzugriffe verwendet werden, um auf OT-Systeme zuzugreifen. Administrative Tools für Wartungen, Diagnose und Konfiguration sind auf diesen Jumphosts zu installieren.
	GS-26.7 Fernzugriffe und Datentransfers sind separat freizuschalten. Daten dürfen nur mit Rücksprache des Betreibers transferiert werden.
GS-27	Internet
	GS-27.1 Direkte Zugänge von Internet auf OT-Systeme im IP-Netz BSA werden nicht zugelassen. Ebenso werden keine direkten Zugänge von OT-Systemen im IP-Netz BSA auf das Internet zugelassen.
	GS-27.2 Internetverbindungen sind auf ein Minimum zu beschränken und erfolgen über die DMZ-Infrastruktur der Basisdienste gemäss den Vorgaben der NSP IP-Netz BSA.

7.2.6 Physische Infrastruktur / Zutritt

Tab. 7.11 Physische Infrastruktur / Zutritt

ID	Beschreibung
GS-28	Grundsatz
	GS-28.1 Der physische Zugang zu BSA-Systemen steht nur berechtigten Personen zu.
GS-29	Abschliessbare Räume
	GS-29.1 Die OT-Systeme müssen in abschliessbaren Räumen oder Behältnissen untergebracht sein. Zwingend offen installierte Sensoren oder Aktoren müssen von der zugehörigen Steuerung auf unerlaubte Zugriffe und Manipulationen überwacht werden.
	GS-29.2 Operatoren Arbeitsplätze, Server- und Storage-Systeme müssen in geschützten und abschliessbaren Räumen betrieben werden.
GS-30	Definierte Standards
	GS-30.1 Technikräume und Tunnelzentralen sind nach definierten ASTRA-Standards zu bauen und zu betreiben.
GS-31	Zutritt Technikräume
	GS-31.1 Der Zutritt zu Technikräumen in Werkhöfen, Stützpunkten, Zentralen, etc. oder der Zugang zu Kabinen, Steuerkästen, etc. mit OT-Systemen ist einzuschränken und klar zu regeln.
	GS-31.2 Die Zutritte zu Technikräumen mit Serversystemen müssen nachvollziehbar sein (Logging),.
	GS-31.3 Schliess- und Zutrittskonzepte müssen vorhanden sein. Allenfalls Videoüberwacht, wenn nur physischer Schlüsselzugang möglich ist.

7.2.7 Mobile Devices und Fremdgeräte

Tab. 7.12 Mobile Devices / externe Clients

ID	Beschreibung
GS-32	Externe Clients
	GS-32.1 Externe Clients (nicht von der OT betriebene Geräte) erhalten keinen direkten Zugang zum IP-Netz BSA und werden immer als Fremdgeräte betrachtet (gilt auch für Geräte von Systemlieferanten). Der Zugang erfolgt über den Perimeterschutz.
	GS-32.2 Ein direkter Zugang auf OT-Systeme bspw. für Inbetriebnahmen oder Notfälle durch ein Fremdgerät ist nur dann gestattet, wenn dies explizit durch den Betreiber freigegeben wird.
GS-33	Mobile Devices
	GS-33.1 Mobile Devices erhalten keinen direkten Zugang zum IP-Netz BSA und werden immer als Fremdgeräte betrachtet (gilt auch für Geräte von Systemlieferanten und für Geräte des eigenen Betriebs). Der Zugang erfolgt immer über den Perimeterschutz.

Glossar

Begriff/Abkürzung	terme/abréviation	Bedeutung
(BSA) Abschnitt	section (EES)	logischer Abschnitt für BSA, nicht der Streckenabschnitt
(Netzwerk-)Segment	segment (de réseau)	Segmente gemäss ASTRA 83040 (meist VLAN)
(Netzwerk-)Zone	zone (de réseau)	im Sinne der NSP des Bundes Si003 (getrennt durch PEZ)
(Teil-)Anlage	(partie d')installation	nur im Sinn der AKS-Definitionen gebraucht
Access-Bereich	niveau accès	L2-Struktur, die den Zugang (Userport) den Endgeräten bereitstellt
AKS-CH		Struktur und Kennzeichnung der Betriebs- und Sicherheitsausrüstungen
AR		Abschnittsrechner
AS		Anlagensteuerung
Ausrüstung/Gerät	équipement	jede Art von aktiven Geräten im BSA-Umfeld (auch ohne Verbindung zum IP-Netz BSA)
Backbone/BB	backbone/BB	Vom Bund (L3 durch BIT, Übertragung durch FUB) bereitgestellte nationale Vernetzung aller Teilnetze
BD (Basisdienste)	BD (services de base)	Netzwerk-Basisdienste (IPAM-Tool, DNS, Zeitquellen, …) für das gesamte IP-Netz BSA
Betriebsleitebene		Diese Ebene bietet die Überwachung und Bedienung aller Anlagen einer Strecke mittels Betriebsleitrechnern, einerseits durch die Polizei hinsichtlich Ereignissen und speziellen betrieblichen Aspekten, andererseits durch den Unterhaltsdienst hinsichtlich Funktionsbereitschaft der Anlagen. Die Betriebsleitrechner sind über ein Kommunikationsnetzwerk mit den Abschnittsrechnern verbunden. Andere Bezeichnung: Übergeordnete Leitebene
BSA	EES	Betriebs- und Sicherheitsausrüstungen
BSA-Abschnitt	section EES	Von einem Abschnittsrechner gesteuerter Abschnitt der Nationalstrasse
BSA-Region	région EES	Anlagenspezifisch definierte Region, in der es eine regional übergeordnete Steuerung gibt
CAB	CAB	Change Advisory Board
Client/Host Server	client/hôte serveur	allgemeine ICT-Begriffe (keine BSA-spezifische Bedeutung), Verwendung bei der Beschreibung von Protokollen
Dienst	service	Dienst ist ein Obergriff sowohl für Fachdienste wie auch für Basisdienste. Dienste implementieren Zugriffs- und Verarbeitungslogik, verfügen aber nicht über eine Benutzeroberfläche.
DMZ	DMZ	Vorgelagerte Sicherheitszone, die von aussen den Zugriff unter weniger hohen Auflagen zulässt, als die nachgelagerten inneren Zonen mit höherem Schutzbedarf (aus dem Englischen für Demilitarized Zone)
DNS	DNS	Das Domain Name System (DNS) ist einer der wichtigsten Dienste in vielen IP-basierten Netzwerken. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung. Das DNS funktioniert ähnlich wie eine Telefonauskunft.
Domäne	domaine	Die Domäne ist ein Bereich um Dinge zu ordnen oder zusammen zu fassen. Beim ASTRA wird die Domäne verwendet für: Namensraum: Innerhalb eines Namensraums sind Identitäten eindeutig, d.h. es gibt nicht mehrere Identitäten für die gleiche Ressource. Funktionsdomäne: Zusammenfassung verschiedener Funktionen. Fachdomäne: Zusammenfassung verschiedener Fachdienste. Prozessdomäne: Zusammenfassung verschiedener Prozesse.
ELZ	ELZ	Einsatzleitzentrale (der Polizei).
Endgerät	équipement terminal	jede Art von Ausrüstung an einem Userport des IP-Netzes BSA

Begriff/Abkürzung	terme/abréviation	Bedeutung
F/Filiale	F/filiale	Filiale (fünf regionale Einheiten des ASTRA)
Firewall	firewall/pare-feu	Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.
GE	UT	Gebietseinheit (11 überkantonale organisatorischen Einheiten, die ihr eigenes IP-Netz BSA GE betreiben)
IAM BSA	IAM BSA	Identity Management System BSA
IKT	IKT	Informations- und Kommunikationstechnik
IP	IP	Internet Protokoll
IPAM	IPAM	IP Address Management
IP-Netz BSA GE GE Abschnitt BD VMZ Backbone	réseau IP EES UT UT section BD VMZ Backbone	Ein IP-Netz für die Betriebs- und Sicherheitsausrüstung der Nationalstrassen mit folgenden Elementen (Teilnetzen): - 11 IP-Netze BSA GE - dem IP-Netz BSA Backbone (Backbone der Bundesverwaltung) - Verbindungen zur VMZ-CH - Verbindungen zu den Rechenzentren BSA - Verbindungen zu den BD (Basisdiensten des IP-Netz BSA)
ISO	ISO	Information Security Officer
ISBO	ISBO	Informatiksicherheitsbeauftragter der Organisation
Leitebene	niveau gestion	Siehe Prozessleitebene
Leitsystem	système de gestion	Dient dem Bedienpersonal zur Überwachung und Leitung von Anlagen
Leittechnik	système de commande/gestion	Funktionen und Komponenten, die der Überwachung und Leitung von Anlagen dienen.
LS	LS	Lokalsteuerung
LWL	LWL	Lichtwellenleiter
Management-Ebene (auch Mgmt-Ebene oder ME)	niveau management (ou ME)	zentrale, übergeordnete Leitebene
Monitoring	monitoring	Überwachung und Visualisierung der technischen Funktionen der Anlagen und Leitsysteme.
NCSC	NCSC	Nationales Zentrum für Cybersicherheit (National Cyber Security Centre)
NMS	NMS	Network Management System
OT	OT	Operational Technology
PEP	PEP	Sicherheitselemente / Policy Enforcement Point
Prozessleitebene	niveau processus	Begriff aus der Leittechnik: In dieser Ebene erfolgen die Überwachung und Bedienung aller Anlagesteuerungen und die übergeordnete Steuerung (Tunnelreflexe) innerhalb eines Abschnitts mittels eines Abschnittsrechners.
RZ(-BSA)	RZ(-EES)	Rechenzentrum BSA
SA-CH	SA-CH	Systemarchitektur Schweiz
SAP	SAP	Service Access Point: Im IP-Netz BSA ist dies i.d.R. ein physisches Port eines Switches oder Routers.
Service	service	Siehe Dienst
SMS	SMS	Security Management System
SOC	SOC	Security Operation Center

Literaturverzeichnis

Weisungen und Richtlinien des ASTRA

[1] Bundesamt für Strassen ASTRA, „**OT-Security Governance**“, *Weisung ASTRA 73006*, www.astra.admin.ch.

[2] Bundesamt für Strassen ASTRA, „**Systemarchitektur Leit- und Steuersysteme der Betriebs- und Sicherheitsausrüstungen**“, *Richtlinie ASTRA 13031*, www.astra.admin.ch.

[3] Bundesamt für Strassen ASTRA, „**IP-Netz BSA**“, *Richtlinie ASTRA 13040*, www.astra.admin.ch.

Auflistung der Änderungen

Ausgabe	Version	Datum	Änderungen
2024	2.00	11.01.2024	Revidierte Version.
2016	1.21	15.12.2018	Publikation der französischen Version Formelle Änderungen
2016	1.20	11.12.2017	Anpassungen infolge Einführung des IP-Netzes BSA (Rili 13040)
2016	1.10	01.03.2016	Inkrafttreten Ausgabe 2016