IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn

(IT-Grundschutz-Profil Bundesautobahn)

von

Die Autobahn GmbH des Bundes

Stand: 22.06.2022

Version 1.0

Allgemeine Informationen zum vorliegenden Dokument

Bezeichnung	Inhalt	Bearbeitungshinweis
Name des Dokuments	IT-Grundschutz-Profil Bundesautobahn	[Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.]
Herausgeber	Die Autobahn GmbH des Bundes Frank Felde	
Autoren	Autobahn GmbH: Bresser, Ingo; Ehlers, Boris; Estel, Anja; Mahnke, Jens; Meier, Steffen; Mikesic, Tania; Müller-Drenkberg, Jörg; Preisner, Karsten; Rupieper, Nico; Schüttler, Josef; Walter, Stefan	
Version	1.0	
Status	freigegeben, öffentlich	
Revisionszyklus	alle zwei Jahre	[Revisionszyklus alle 1, 2, 3 Jahre]

Änderungshistorie

Version	Datum	Änderung	Bearbeitet von
0.1 – 0.92	31.03.2021	Initiale Erstellung	Die Autobahn GmbH
0.99	28.03.2022	Finaler Entwurf	Stefan Walter / Die Autobahn GmbH
1.0	22.06.2022	Freigabe	Frank Felde / Die Autobahn GmbH

Die Autobahn

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Überblick

1.1 Einleitung

Die Digitalisierung schreitet immer schneller voran ebenso wie die Durchdringung aller Geschäftsprozesse mit Informationstechnik erfolgt. Auch in der Verkehrssteuerung und -beeinflussung sind viele Komponenten bereits auf Feldebene vernetzt. Dies führt einerseits zu gesteigerter Leistungsfähigkeit und Qualität der Infrastrukturen, andererseits birgt die Digitalisierung aber auch vermehrt Risiken wie Cyberangriffe. Die potenzielle Angriffsfläche nimmt daher mit zunehmender Vernetzung stetig zu.

Um dieser Herausforderung zu begegnen, ist es erforderlich, sichere und resiliente Systeme zu entwickeln und zu betreiben. Grundlage für den sicheren Betrieb muss ein etabliertes Managementsystem für Informationssicherheit darstellen. Dieses ermöglicht die Umsetzung von angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität der informationstechnischen Systeme, Komponenten oder Prozesse. Die Umsetzung der Maßnahmen soll dabei nach dem Stand der Technik erfolgen, um ein angemessenes Sicherheitsniveau zum Schutz und zur Aufrechterhaltung der Kritischen Infrastruktur zu erreichen.

Das vorliegende BSI IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn soll anhand einzelner Prozesse eine beispielhafte Konkretisierung des Stands der Technik für diesen Bereich aufzeigen und somit die Einführung eines Informationssicherheitsmanagementsystems für die bestehende Infrastruktur erleichtern.

1.2 Management Summary

Das IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn richtet sich an die für Informationstechnik verantwortlichen Entscheidungsträger aus dem Bereich des Betriebs der Bundesautobahnen.

Im Folgenden werden die im Kontext der Kritischen Infrastrukturen wesentlichen Geschäftsprozesse zur Erbringung der Dienstleistung Personen- und Güterverkehr behandelt.

Die Geschäftsprozesse

- Durchführung des Straßenbetriebsdienstes,
- Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur

  und

- Operatives Verkehrsmanagement

stellen sogleich die Grundgesamtheit der Prozesse für den Betrieb aller Betreiber in dieser Anlagenkategorie dar.

Das IT-Grundschutz-Profil soll Anwendern dabei helfen, ein Informationssicherheitskonzept am Beispiel dieser Geschäftsprozesse der Bundesautobahnen zu etablieren. Diese Schablone des BSI IT-Grundschutzes verfolgt den Anspruch, das Sicherheitsniveau der Standard-Absicherung zu erfüllen.

Abseits der Bundesautobahnen kann dieses Profil weiteren Betreibern des Straßenverkehrs, die ähnliche Prozesse zur Erbringung Ihrer Dienstleistung ausüben, eine Hilfestellung bieten. Ebenso soll es Herstellern und Dienstleistern in diesem Bereich als Handlungsleitfaden für die Informationssicherheitskonzeption in ihrem Anwendungsbereich dienen.

1.3 Abgrenzung des Informationsverbunds

Die folgende Abbildung zeigt eine abstrahierte Sicht auf die Informationsverbünde im Sinne eines bereinigten Netzplans nach dem BSI-Standard 200-2 (siehe 8.3, Buchstabe c) und weist dabei die Grenzen und Schnittstellen des in diesem Sicherheitskonzept betrachteten Informationsverbunds auf. Nicht im Geltungsbereich des Informationsverbunds befindliche Objekte werden gesondert abgesichert.

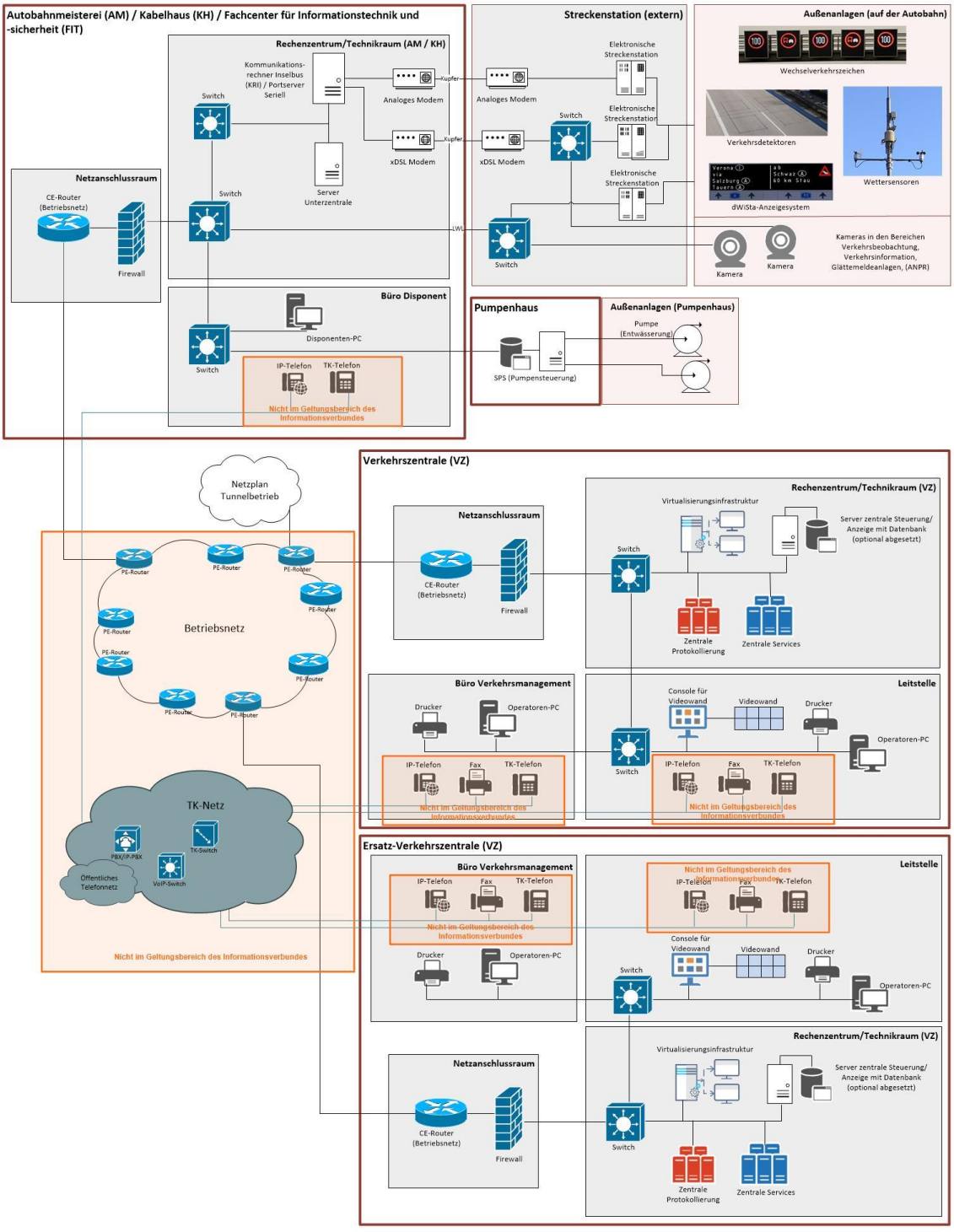

Abbildung 1: vereinfachter Netzplan für die Verkehrssteuerung

Die nachfolgende Abbildung benennt alle Komponenten und Schnittstellen, welche im Geltungsbereich für den Betrieb von Straßentunneln benötigt werden. Als Definition eines Straßentunnels im Sinne des Grundschutz-Profils gilt, dass dieser für den Kraftfahrzeugverkehr bestimmt ist, mindestens eine geschlossene Länge von 80 m aufweist und mit einer Planungsgeschwindigkeit von 80 km/h oder 100 km/h konzipiert wurde.

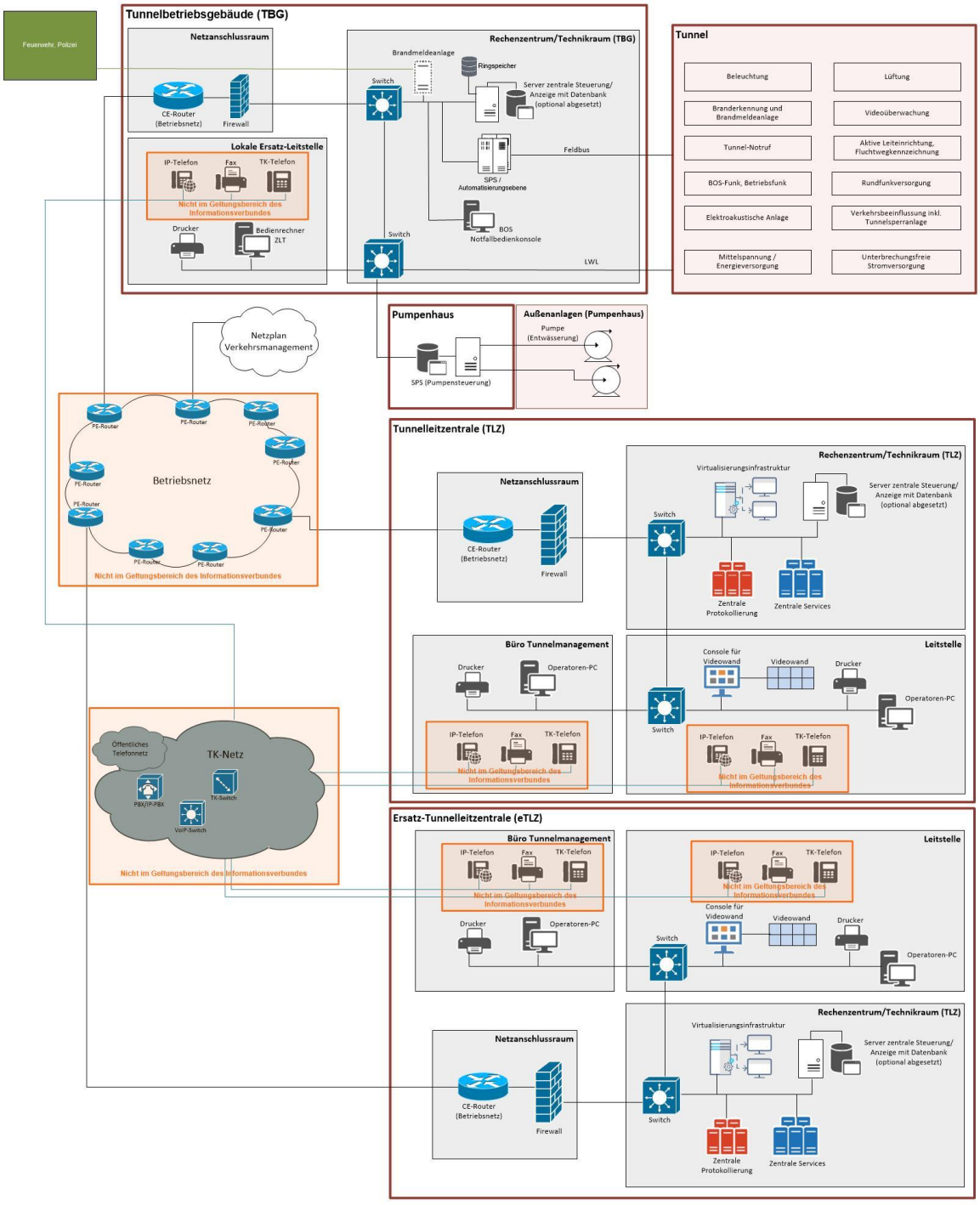

Abbildung 2: vereinfachter Netzplan für die Tunnelsteuerung

Die nachfolgende Abbildung stilisiert die möglichen Arten der Anbindung eines Customer-Edge-Routers (CE-Router) an das Betriebsnetz via dem Provider-Edge-Router (PE-Router).

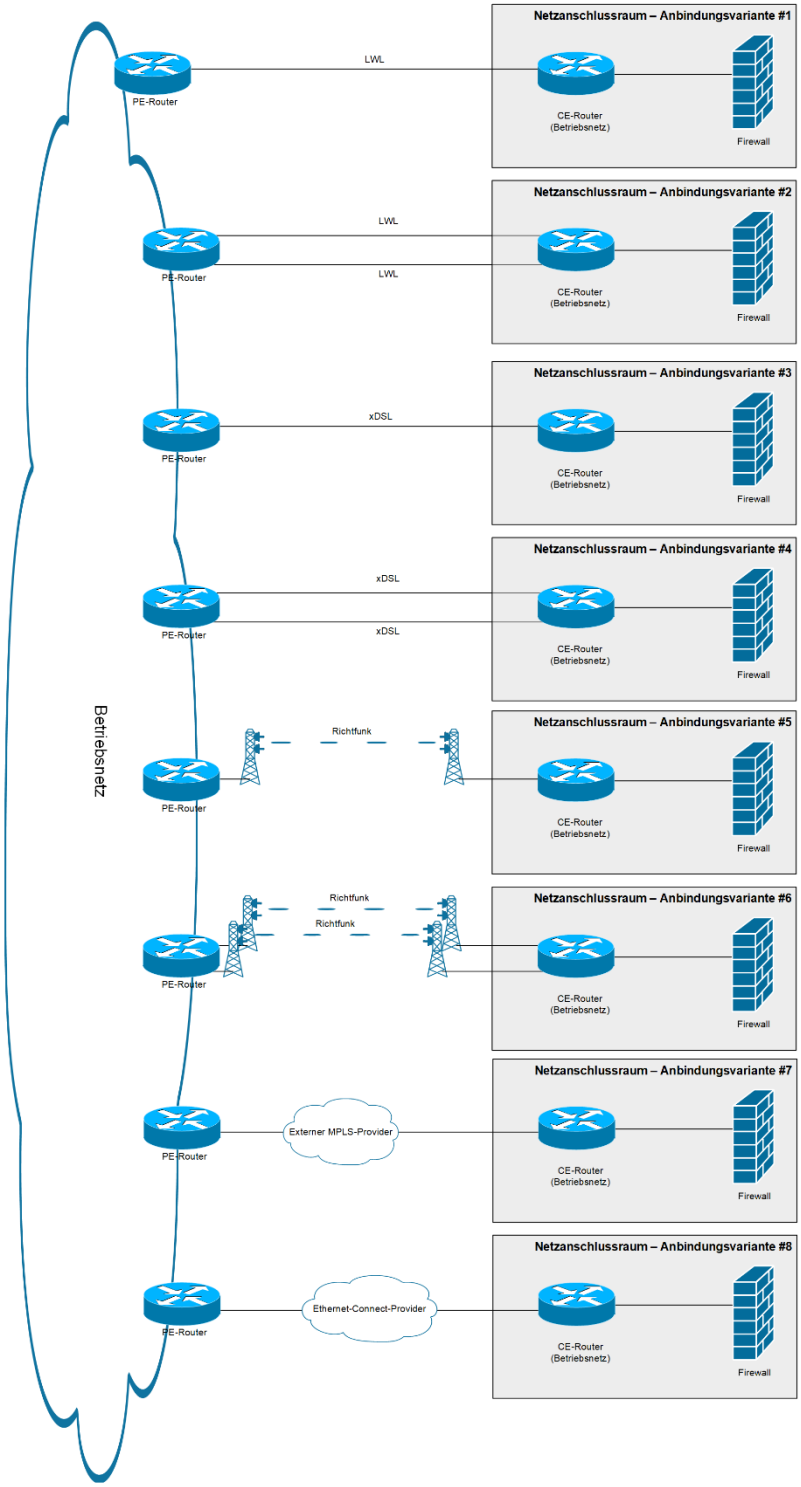

Abbildung 3: Anbindungsvarianten der CE-Router an den PE-Router des Betriebsnetzes

Außerhalb des Informationsverbunds liegen die Zielobjekte der nicht verwendeten einzelnen System-Bausteine der Schichten APP, SYS, IND, NET und INF, die im Kapitel Modellierung nach IT-Grundschutz beschrieben sind.

Die nicht verwendeten Bausteine der Schichten ISMS, ORP, CON, OPS und DER müssen in übergreifenden Informationsverbünden sowie im Teilverbund zur Administration behandelt werden.

1.4 Verfahrensdaten

Im Rahmen dieses IT-Grundschutz-Profils werden die folgenden Verfahrensdaten betrachtet und bewertet.

System	Erhobene Daten	Personenbezug ja/nein
Verkehrsdatenerfassung	Fahrzeugarten in maximal 8 Klassen Anzahl der Fahrzeuge pro Intervall Geschwindigkeit von Einzelfahrzeugen Fahrtrichtung	Nein
Umfelddatenerfassung	Lufttemperatur Luftfeuchte Windrichtung Windgeschwindigkeit Sichtweite Niederschlagsart Niederschlagsintensität Fahrbahntemperatur Tiefentemperatur Zustand der Fahrbahnoberfläche (trocken, feucht, nass, glatt) Wasserfilmdicke	Nein
Linienbrandmelder (Tunnel)	Anstieg und Verlauf der Temperatur (über die Zeit und absolut)	Nein
Strömungsmessung (Tunnel)	Luftgeschwindigkeit und Luftrichtung	Nein
Sichttrübemessung (Tunnel)	Eintrübung der Luft durch Partikel (z.B. durch Rauch, Nebel, Staub) Extinktionskoeffizient Transmission	Nein
CO-Messung (Tunnel)	CO-Konzentration in ppm	Nein
Lichtmessung (Tunnel)	Leuchtdichte	Nein
Videobeobachtung (temporäre Seitenstreifenfreigabe, Tunnel, Strecke, Wetter)	Videobilder des Verkehrsablaufs und des Ablaufes von Ereignissen (z.B. Pannen,	Ob ein Personenbezug herstellbar ist, hängt von den Einstellungen der Kameras ab. In der Regel sind diese

	Brände, Unfälle, insbesondere in Tunneln)	Parameter so gewählt, dass KFZ-Kennzeichen und Gesichter nicht erkennbar sind. Personenbezogene Daten werden dann lediglich intern in den Kameras verarbeitet.

2. IT-Strukturanalyse

2.1 Geschäftsprozesse

ID	Geschäftsprozess	Typ des Prozesses	Erläuterung
P-0001	Durchführung des Straßenbetriebsdienstes	Hauptprozess	Die folgenden Aufgaben sind Bestandteil des Prozesses: • Durchführung der Streckenwartung/-kontrolle • Durchführung des Winterdienstes (inkl. SWIS) • Durchführung von Sofortmaßnahmen am Straßenkörper oder zur Verkehrssicherung aufgrund unvorhergesehener Ereignisse
P-0002	Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur	Hauptprozess	Die folgenden Aufgaben sind Bestandteil des Prozesses: • Systemüberwachung für verkehrs-, betriebs-, nachrichten- und elektrotechnische Infrastruktur • Wartung und Betrieb von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • Instandsetzung nach Störung und Schäden von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur
P-0003	Operatives Verkehrsmanagement	Hauptprozess	Die folgenden Aufgaben sind Bestandteil des Prozesses: • Bedienen von Verkehrsbeeinflussungsanlagen • Bedienen tunnelbetrieblicher Einrichtungen • Strategiemanagement • Störfall- und Ereignismanagement durchführen • Bereitstellung von Verkehrsinformationen

Tabelle 1: Strukturanalyse - Geschäftsprozesse

2.2 Anwendungen

ID	Anwendung	Typ der Anwendung	Erläuterung
APP-0001	Datenbank – Server zentrale Steuerung/Anzeige	relationale Datenbank	Die Datenbank ist Bestandteil der Server zentrale Steuerung/Anzeige. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0001 - Durchführung des Straßenbetriebsdienstes • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement
APP-0002	Domain Name Service (DNS) - KRITIS	DNS	Für die IT-Systeme im Geltungsbereich wird eine auf Basis des Schutzbedarfes orientierte Infrastruktur (SYS-0011 - Zentrale Services) betrieben. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0001 - Durchführung des Straßenbetriebsdienstes • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement

ID	Anwendung	Typ der Anwendung	Erläuterung
APP-0003	Network Time Protocol (NTP) - KRITIS	NTP	Für die IT-Systeme im Geltungsbereich wird eine auf Basis des Schutzbedarfes orientierte Infrastruktur (SYS-0011 - Zentrale Services) betrieben. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0001 - Durchführung des Straßenbetriebsdienstes • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement
APP-0004	Dynamic Host Configuration Protocol (DHCP) - KRITIS	DHCP	Für die IT-Systeme im Geltungsbereich wird eine auf Basis des Schutzbedarfes orientierte Infrastruktur (SYS-0011 - Zentrale Services) betrieben. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung des Prozesses: • P-0001 - Durchführung des Straßenbetriebsdienstes • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement

ID	Anwendung	Typ der Anwendung	Erläuterung
APP-0005	Verzeichnisdienst	LDAP/Active-Directory	Für die IT-Systeme im Geltungsbereich wird eine auf Basis des Schutzbedarfes orientierte Infrastruktur (SYS-0011 - Zentrale Services) betrieben. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0001 - Durchführung des Straßenbetriebsdienstes • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement
APP-0006	Visualisierung Prozessleitsystem (Server)	Individuelle Software	Über das Prozessleitsystem werden alle technischen Anlagen eines Tunnels visualisiert und bedient. Der Server des Prozessleitsystems stellt für die Clients die Bedienoberfläche bereit. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement

ID	Anwendung	Typ der Anwendung	Erläuterung
APP-0007	Datenbank vom Prozessleitsystem	Datenbank	In der Datenbank des Prozessleitsystems werden Messwerte, Störungen, Alarme und Schalthandlungen gespeichert. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement
APP-0008	Visualisierung Prozessleitsystem (Client)	Individuelle Software	Auf den Clients wird das Prozessleitsystem des Tunnels über die vom Server bereitgestellte Bedienoberfläche durch entsprechend geschulten Personals überwacht und bedient. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement
APP-0009	Videomanagement (Client-Anwendung)	Allgemeine Software	Über den Client des Videomanagements können die auf dem Server gespeicherten Videos aufgerufen, abgespielt, gesichert oder exportiert werden. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0001 - Durchführung des Straßenbetriebsdienstes • P-0003 - Operatives Verkehrsmanagement

ID	Anwendung	Typ der Anwendung	Erläuterung
APP-0010	Videomanagement (Server-Anwendung)	Allgemeine Software	Auf dem Videoserver werden die Videos der angeschlossenen Kameras gespeichert. Dies erfolgt i.d.R. in einem Ringspeicher, bei dem die jeweils ältesten Dateien unter Beachtung der Aufbewahrungsfristen automatisch überschrieben werden. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0001 - Durchführung des Straßenbetriebsdienstes • P-0003 - Operatives Verkehrsmanagement
APP-0011	Steuerungssoftware-Server (gemäß MARZ)	Individuelle Software	Auf der Unterzentrale werden die von den Außenanlagen erfassten Verkehrs- und Umfelddaten weiterverarbeitet und die automatischen Anzeigeprogramme für die Wechselverkehrszeichen auf Basis der hinterlegten Parametersätze ermittelt. Die Unterzentrale versendet die entsprechenden TLS-Stellbefehle (siehe 8.2, Buchstabe a) an die Außenanlagen gemäß MARZ (siehe 8.2, Buchstabe b). Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement

ID	Anwendung	Typ der Anwendung	Erläuterung
APP-0012	Datenbank von Steuerungssoftware	Datenbank	In der Datenbank der Unterzentrale werden alle Rohdaten und aggregierten Daten, die Störungen, Parametersätze, Schaltgründe und Rückmeldungen gespeichert. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement
APP-0013	Steuerungssoftware-Client (gemäß MARZ)	Individuelle Software	Auf den Clients wird die Steuerungssoftware durch entsprechend geschulten Personals überwacht und bedient. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement

ID	Anwendung	Typ der Anwendung	Erläuterung
APP-0014	Kommunikationsrechner Inselbus (gemäß TLS)	Individuelle Software	Der Kommunikationsrechner Inselbus steuert und überwacht die TLS-Kommunikation der Unterzentrale mit den Außenanlagen. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement
APP-0015	Streckenstationssoftware (gemäß TLS)	Individuelle Software	An der Streckenstation sind die örtlich vorhandenen Sensoren und Aktoren über Eingabe- Ausgabe-Konzentratoren (EAK) angeschlossen. In der Streckenstation werden die erfassten Daten geglättet und aggregiert (Summen- und Mittelwertbildung) und an die Unterzentrale versandt. Stellbefehle der UZ werden an die Aktoren weitergeleitet. Weiterhin wird der Zustand der angeschlossenen Sensoren und Aktoren überwacht. Diese referenzierte Anwendung unterstützt bei der Aufrechterhaltung der Prozesse: • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement

ID	Anwendung	Typ der Anwendung	Erläuterung
APP-0016	Office-Anwendung	Allgemeine Software	Auf den Clients wird die Office-Anwendung verwendet. Sie unterstützt bei der Aufrechterhaltung der folgenden Prozesse: • P-0001 - Durchführung des Straßenbetriebsdienstes • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement
APP-0017	Web-Browser	Allgemeine Software	Auf den Clients wird der Web-Browser verwendet. Dieser unterstützt bei der Aufrechterhaltung der folgenden Prozesse: • P-0001 - Durchführung des Straßenbetriebsdienstes • P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur • P-0003 - Operatives Verkehrsmanagement

Tabelle 2: Strukturanalyse - Anwendungen

2.3 IT-System

ID	IT-System	Plattform	Erläuterung
SYS-0001	Kommunikationsrechner Inselbus (KRI) / Portserver Seriell	Eingebettete Systeme	Der Kommunikationsrechner Inselbus ist gemäß TLS ein Verbindungsglied zwischen Unterzentrale und den dazugehörigen Streckenstationen. Er koordiniert den Datenfluss und organisiert umfangreiche Pufferfunktionen. Funktionell übernimmt er entsprechend dem OSI-Referenzmodell die beiden unteren OSI-Ebenen, während er auf den oberen Protokollschichten transparent arbeitet. Als unabhängige Hardwareeinheit stellt der KRI eine (theoretisch) beliebige Anzahl von Inselbussen der übergeordneten Hierarchieebene zur Verfügung. Begrenzt wird die Anzahl lediglich durch die verwendete Bit-/Baudrate auf den unterschiedlichen Schnittstellen bzw. durch die physikalische Adressiermöglichkeit. Das IT-System dient als Plattform zur Bereitstellung der nachfolgend aufgeführten Anwendung: • APP-0014 - Kommunikationsrechner Inselbus (gemäß TLS)

ID	IT-System	Plattform	Erläuterung
SYS-0002	Server Unterzentrale	Eingebettete Systeme	Der Server Unterzentrale fungiert als Primary-Station für die Kommunikation. Dies bedeutet, sofern die Unterzentrale das Polling des KRI einstellt muss auch der KRI nach einem festgelegten Timeoutintervall das Polling auf dem Inselbus einstellen. Denn nur so kann die Streckenstation in den autarken Modus wechseln. Das IT-System „Server Unterzentrale ” dient als Plattform zur Bereitstellung der nachfolgend aufgeführten Anwendung: • APP-0015 - Streckenstationssoftware (gemäß TLS)
SYS-0003	Drucker	Drucker	Durch die Bereitstellung der Drucker wird es den Anwendern in der Leitstelle benötigte Informationen zur Weitergabe bzw. Aufbewahrung in Papierform anzufertigen.
SYS-0004	Operatoren-PC	Windows Betriebssystem oder Linux Betriebssystem	Mittels dem Operatoren-PC wird der Operator in der Leitstelle dazu befähigt die Verkehrssteuerung in Abhängigkeit der vorliegenden Informationen zu beeinflussen und zu überwachen. Das IT-System „Operatoren-PC ” dient als Plattform zur Bereitstellung der nachfolgend aufgeführten Anwendungen: • APP-0008 - Visualisierung Prozessleitsystem (Client) • APP-0009 - Videomanagement (Client-Anwendung) • APP-0013 - Steuerungssoftware-Client (gemäß MARZ) • APP-0016 - Office-Anwendung • APP-0017 - Web-Browser

ID	IT-System	Plattform	Erläuterung
SYS-0005	Videowand	Großbildschirm/Videowand	Die Videowand ist eventgesteuert. Das bedeutet, dass jeder Inhalt des Operatoren-PCs und jede Kamera ohne Einwirkung des Operators automatisch aufgeschaltet werden kann, um sofort in Realtime bedient zu werden.
SYS-0006	Console Videowand	Windows Betriebssystem oder Linux Betriebssystem	Die Console Videowand nimmt alle Signale des darzustellenden Inhaltes des Operatoren-PCs (Tastatur, Maus, Monitor, Audio), analoge oder digitale Kameras, TV (Bild und Audio) gleichzeitig auf und verteilt diese in Realtime auf Teile der Videowand bzw. als Großbild auf die komplette Videowand.
SYS-0007	Elektronische Streckenstation	Eingebettete Systeme	Eine Streckenstation enthält ein Steuermodul (SM), das die verschiedenen E/A-Konzentratoren (EAK) bedient. Diese ist nach der TLS aufgebaut.
SYS-0008	Wechselverkehrszeichen	Eingebettete Systeme	Zur Darstellung von Inhalten zur kollektiven Verkehrsbeeinflussung werden verschiedene Anzeigetechniken verwendet. Dabei wird sowohl nach dem Typ des dargestellten Inhalts unterschieden als auch nach Darstellungsprinzip (aktiv leuchtend, mechanisch).
SYS-0009	dWista-Anzeigesystem	Eingebettete Systeme	Als Dynamischer Wegweiser mit integrierten Stauinformationen, kurz dWiSta, wird ein Anzeigesystem bezeichnet, welcher Verkehrsinformationen an die Verkehrsteilnehmer vermittelt. Die dWiSta-Anzeigesysteme befinden sich an Schilderbrücken und werden vor Autobahnanschlussstellen oder Autobahnknotenpunkten aufgestellt.

ID	IT-System	Plattform	Erläuterung
SYS-0010	Kamera	Eingebettete Systeme	Diese Gruppe beinhalten Kameras zum Zwecke der Verkehrsbeobachtung, Erhebung von Verkehrsinformationen, der automatischen Erkennung von Nummernschildern. Ebenfalls können diese als Bestandteil von Glättemeldeanlagen integriert sein.
SYS-0011	Zentrale Services	Windows Betriebssystem oder Linux Betriebssystem	Die physischen bzw. virtuellen IT-Systeme “Zentrale Services” dienen als Plattform zur Bereitstellung der nachfolgend aufgeführten Anwendungen: • APP-0002 - Domain Name Service (DNS) - KRITIS • APP-0003 - Network Time Protocol (NTP) - KRITIS • APP-0004 - Dynamic Host Configuration Protocol (DHCP) - KRITIS • APP-0005 – Verzeichnisdienst
SYS-0012	Zentrale Protokollierung	Windows Betriebssystem oder Linux Betriebssystem	Mittels den IT-Systemen “Zentrale Protokollierung” werden die Services für eine zentrale Auswertung von Syslogs bzw. Windows-Events etabliert.
SYS-0013	Virtualisierungsinfrastruktur	Infrastruktur as a Service (IaaS)	Die Infrastruktur as a Service Plattform stellt virtuelle Hardware für den verdichteten Betrieb der zentralen Services, der zentralen Protokollierung oder den Systemen für die zentrale Steuerungssoftware und deren Datenbänke bereit.

ID	IT-System	Plattform	Erläuterung
SYS-0014	Server zentrale Steuerung/Anzeige	Windows Betriebssystem oder Linux Betriebssystem	Das IT-Systeme „Server zentrale Steuerung/Anzeige" dient als Plattform zur Bereitstellung der nachfolgend aufgeführten Anwendungen: • APP-0001 - Datenbank – Server zentrale Steuerung/Anzeige • APP-0010 - Videomanagement (Server-Anwendung) • APP-0011 - Steuerungssoftware-Server (gemäß MARZ) • APP-0012 - Datenbank von Steuerungssoftware
SYS-0015	Bedienrechner Zentrale Leittechnik (ZLT)	Windows Betriebssystem oder Linux Betriebssystem	Das IT-System „Bedienrechner ZLT " dient als Plattform zur Bereitstellung der nachfolgend aufgeführten Anwendungen in der lokalen Ersatz-Leistelle im Tunnelbetriebsgebäude (TBG): • APP-0008 - Visualisierung Prozessleitsystem (Client) • APP-0009 - Videomanagement (Client-Anwendung)
SYS-0016	Brandmeldeanlage (TBG)	Eingebettete Systeme	Die Brandmeldeanlage im Rechenzentrum bzw. Technikraum des Tunnelbetriebsgebäudes (TBG) stellt zusätzlich noch einen Link zur Feuerwehr und/oder Polizei zur Verfügung. Die aufgeschalteten Systeme in den Örtlichkeiten der Feuerwehr und Polizei gehören nicht zum Informationsverbund im Geltungsbereich der KritisV (siehe 8.4, Buchstabe b) für Bundesautobahnen.

ID	IT-System	Plattform	Erläuterung
SYS-0017	BOS Notfallbedienkonsole	Eingebettete Systeme	Für die am Tunnel eintreffende Feuerwehr und Polizei steht mittels der computergesteuerten BOS Notfallbedienkonsole die Möglichkeit der Erlangung der Schalthoheit über die komplette Beleuchtung, die Belüftung sowie der Sperrung und Entsperrung des Tunnels zur Verfügung.
SYS-0018	Branderkennung und Brandmeldeanlage (Tunnel)	Eingebettete Systeme	Gemäß der EABT 80-100 (siehe 8.1, Buchstabe a) erfolgt die Meldung an die ständig besetzte Stelle durch Auslösung eines manuellen oder automatischen Brandalarms. Manuelle Brandmeldeeinrichtungen sind in Tunnels mit Längen ≥ 400 m als Handfeuermelder nach DIN EN 54-11 außen an jeder Notrufkabine anzuordnen. Automatische Brandmeldeeinrichtungen sind ab einer Tunnellänge von 400 m bzw. Bei Tunneln mit mechanischer Lüftung vorzusehen.
SYS-0019	Videoüberwachung	Eingebettete Systeme	Gemäß der EABT 80-100 muss in Tunneln von einer Länge ≥ 400 m eine Überwachung des Tunnelraumes per Videoüberwachung etabliert werden. Hierzu wird im Tunnelfahrraum im Abstand von max. 75 m feststehende und an den Portalen schwenkbare Kameras zur Beobachtung installiert. Ebenfalls werden hierüber punktuell die Rettungswege beobachtet. Die angefallenen Daten werden für mindestens 72 Stunden vorgehalten.
SYS-0020	Rundfunkversorgung	Eingebettete Systeme	Gemäß der EABT 80-100 ist der Empfang mindestens eines UKW-Rundfunksenders (Verfügbarkeit) mit Verkehrsfunkkennung im Tunnel zu gewährleisten.

ID	IT-System	Plattform	Erläuterung
SYS-0021	Elektroakustische Anlage	Eingebettete Systeme	Gemäß der EABT 80-100 sind Tunnel, welche videoüberwacht sind, mit Lautsprechern im Tunnel und an den Tunnelportalen auszurüsten. Über diese werden im Ereignisfall Verhaltensweisen an die Tunnelnutzer übermittelt.
SYS-0022	Verkehrsbeeinflussung inkl. Tunnelsperranlage	Eingebettete Systeme	Gemäß der EABT 80-100 sind als Kommunikationsstandard für die an die Steuersysteme angebundenen Sensoren und Aktoren der verkehrstechnischen Einrichtungen die Anforderungen aus dem aktuell gültigen Standard der TLS entsprechend der Funktionsgruppen (Verkehrserfassung, Umfeld Datenerfassung für verkehrstechnische Zwecke, Wechselzeichengebersteuerung, Betriebsmeldungen und Systemsteuerung) anzuwenden. Bezüglich des Zusammenwirkens von Tunnelsperranlagen, Wechsellichtzeichen (WLZ) und vorgelagerter Wechselverkehrszeichen (WVZ) ist zu beachten, dass diese eine funktionale Einheit bilden.
SYS-0023	Ringspeicher	Speicherlösung	Gemäß der EABT 80-100 muss in Tunneln von einer Länge ≥ 400 m eine Überwachung des Tunnelraumes per Videoüberwachung etabliert werden. Die angefallenen Daten werden für mindestens 72 Stunden auf einem lokalen Ringspeicher vorgehalten. Der Ringspeicher selbst stellt seine Funktion nur im Zusammenspiel mit SYS-0020 – Videoüberwachung bereit.

Tabelle 3: Strukturanalyse – IT-System

2.4 Industrielle IT

ID	Industrielle IT	Plattform	Erläuterung
IND-0001	SPS / Automatisierungsebene	SPS	Das IT-Systeme „SPS/Automatisierungsebene" dienen als Plattform zur Bereitstellung der nachfolgend aufgeführten Anwendungen: • APP-0006 - Visualisierung Prozessleitsystem (Server) • APP-0007 - Datenbank vom Prozessleitsystem
IND-0002	Beleuchtung	Eingebettetes System	Gemäß der EABT 80-100 werden umfangreiche Kriterien an die Beleuchtung eines Tunnels gestellt.
IND-0003	Lüftung	Sensoren und Aktoren	Gemäß der EABT 80-100 stellen die Systeme der Lüftung des Tunnelfahrraums (Tunnellüftung) sowie die Systeme der Lüftung der Rettungswege von Straßentunneln (Rettungsweglüftung) im Regelbetrieb sicher, dass die Versorgung der Personen im Tunnel mit ausreichend frischer Luft und die Abführung der Abluft gewährleistet ist. Ebenfalls wird sichergestellt, dass die Sichtverhältnisse in der von Abgasen und Staub belasteten Luft ausreichend sind. Insofern ein Brand im Tunnel sein sollte, verringern die Systeme die Rauch- und Wärmewirkung auf den Fluchtwegen im Tunnelfahrraum und auf den Rettungswegen.

ID	Industrielle IT	Plattform	Erläuterung
IND-0004	Aktive Leiteinrichtung, Fluchtwegkennzeichnung	Eingebettetes System	Die aktiven Leiteinrichtungen und Fluchtwegkennzeichnungen sind in jeder Tunnelröhre auf der Seite der Notausgänge etabliert. Fluchtwegkennzeichen bestehen aus dem Fluchtsymbol (zum nächstgelegenen Notausgang hin orientiert) und den Pfeilsymbolen je Fluchtrichtung mit darüber angeordneten Entfernungsangaben zu den nächstgelegenen Notausgängen bzw. Portal. Die Kennzeichen sind ständig hinterleuchtet. Fluchtwegkennzeichnungen und Orientierungsbeleuchtungen werden in einem Abstand von ca. 25 m ausgeführt. Die Orientierungsbeleuchtung wird nur im Brandfall automatisch durch die Branddetektoren in der Tunnelröhre oder manuell durch ständig Vor-Ort befindliches Personal aktiviert.
IND-0005	Verkehrsdetektoren	Sensoren und Aktoren	Verkehrsdetektoren dienen zur Erfassung jedes einzelnen Fahrzeugs beim Durchfahren ihres Wahrnehmungsbereiches. Die Detektoren ermöglichen die zahlenmäßige Erfassung und Klassifizierung nach Fahrzeugarten sowie die Ermittlung der Fahrzeuggeschwindigkeiten. Jedem Fahrstreifen ist ein E/A-Kanal als kleinste adressierbare Einheit eindeutig zuzuordnen. Damit ist es möglich, die Daten fahrstreifenbezogen zu erfassen und Berechnungsparameter individuell für jeden Fahrstreifen einzugeben und zu ändern.

ID	Industrielle IT	Plattform	Erläuterung
IND-0006	Wettersensoren	Sensoren und Aktoren	Umfelddaten werden auch vom Betriebsdienst für die Einsatzplanung des Winterdienstes (Straßenzustands- und Wetterinformationssystem - SWIS) benötigt und für statistische Auswertungen genutzt. Wetterinformationen können nach manueller Bestätigung als Gefahreninformation angelegt werden.
IND-0007	SPS (Pumpensteuerung)	SPS	Tunnelbauwerken und Straßenkörper unterliegen verschiedenen Richtlinien und Normen. In erster Linie steht die Sicherheit im Falle einer Havarie im Fokus. Das IT-System „SPS (Pumpensteuerung)" dient als Plattform zur Steuerung des Zielobjektes IND-0008 – Pumpe (Entwässerung).
IND-0008	Pumpe (Entwässerung)	Pumpe (Maschine)	Die Pumpe dient der zur ausreichenden und schnellen Entwässerung von Tunnelbauwerken und Straßenkörpern und wird von der IND-0007 – SPS (Pumpensteuerung) gesteuert. Dies dient in erster Linie der Aufrechterhaltung der Funktionsfähigkeit der Autobahnen in Falle von Extremwetterereignissen.

Tabelle 4: Strukturanalyse – Industrielle IT

2.5 Netze und Kommunikation

ID	Netzkomponente	Plattform	Erläuterung
NET-0001	CE-Router (Betriebsnetz)	Router/L3-Switch	Ein Customer Edge Router (CE) ist ein Router, der sich im Netzanschlussraum (INF-0004 – Netzanschlussraum) befindet und die Schnittstelle zwischen dem LAN und dem Betriebsnetz der Institution bildet.

ID	Netzkomponente	Plattform	Erläuterung
NET-0002	Firewall	Firewall	Die Firewall ist ein Sicherheitsgateway, welches sich im Netzanschlussraum (INF-0004 – Netzanschlussraum) befindet und die Absicherung der Schnittstelle zwischen dem LAN und dem CE-Router bildet.
NET-0003	Switch	Switch	Der „Switch“ als aktive Netzkomponente verbindet als Kopplungselement verschiedene Netzwerksegmente und IT-Systeme in den Gebäuden und Räumen der Institution miteinander.
NET-0004	Analoges Modem	Modem	Ein analoges Modem ist eine Datenübertragungseinrichtung, um digitale Signale in analoge Signale umzuwandeln und über ein Kommunikationsnetz zu übertragen. Zusätzlich ist ein analoges Modem mit einer Logik ausgestattet, um zu einer Gegenstelle (z. B. ein anderes Modem) eine Verbindung aufzubauen, Verbindungen anzunehmen und Daten zu übertragen.
NET-0005	xDSL-Modem	Modem	Ein xDSL-Modem ist eine Netzkomponente zur Übertragung von Daten über eine Teilnehmeranschlussleitung (TAL) per Digital Subscriber Line (DSL). Es bildet den Netzabschluss (NT) für den DSL-Teil beim Teilnehmer und stellt das Gegenstück zum amtsseitigen Digital Subscriber Line Access Multiplexer (DSLAM) dar.
NET-0006	Tunnelnotruf	BAB-Notrufsystem	Im Tunnel sind in regelmäßigen Abständen Notrufkabinen angeordnet, die jeweils eine Notrufsprechstelle enthalten. Weitere Notrufsprechstellen werden im Portalbereich angeordnet. In der Regel sind die Notrufsprechstellen als BAB-Notrufsystem (TK-Anlagen-Infrastruktur) ausgeführt, das jedoch direkt auf die ständig besetzte Stelle aufgeschaltet ist.

ID	Netzkomponente	Plattform	Erläuterung
NET-0007	BOS-Funk, Betriebsfunk (Tunnel)	hybride TK-Anlage	Gemäß der EABT 80-100 ist die funktechnische Ausstattung eines Tunnels abhängig von den örtlichen Gegebenheiten. Grundsätzlich erfolgt die Ausstattung in Anlehnung an den gültigen Leitfaden zur Planung und Realisierung von Objektversorgungen (L-OV) für das digitale Sprech- und Datenfunksystem für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) in der Bundesrepublik Deutschland.

Tabelle 5: Strukturanalyse – Netzkomponente

Die Kommunikationsverbindungen sollten durch die Institution für die eingesetzten Protokolle sowie etwaige Authentisierungsverfahren benannt werden.

Dies kann beispielsweise durch die folgende Tabelle erfolgen:

ID	Verbindungsaufbau von --> zu	Protokoll	Port	Verschlüsselung	Zweck / Kommunikationsinhalte
V-0001					

Tabelle 6: Strukturanalyse – Kommunikationsverbindungen

2.6 Räume und Gebäude

ID	Räume und Gebäude	Erläuterung
INF-0001	Autobahnmeisterei (AM) / Kabelhaus (KH) / Fachcenter für Informationstechnik und -sicherheit (FIT)	Innerhalb einer Autobahnmeisterei, eines Kabelhauses und einer FIT werden in den hier aufgeführten Räumen IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • INF-0004 – Netzanschlussraum • INF-0005 – Rechenzentrum/Technikraum (AM / KH) • INF-0017 – Büro Disponent

ID	Räume und Gebäude	Erläuterung
INF-0002	Verkehrszentrale (VZ)	Innerhalb der Verkehrszentrale (VZ) werden in den hier aufgeführten Räumen IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • INF-0004 – Netzanschlussraum • INF-0006 – Büro Verkehrsmanagement • INF-0007 – Leitstelle • INF-0009 – Rechenzentrum/Technikraum (VZ)
INF-0003	Ersatz-Verkehrszentrale (VZ)	Innerhalb der Ersatz Verkehrszentrale (VZ) werden in den hier aufgeführten Räumen IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • INF-0004 – Netzanschlussraum • INF-0006 – Büro Verkehrsmanagement • INF-0007 – Leitstelle • INF-0009 – Rechenzentrum/Technikraum (VZ)
INF-0004	Netzanschlussraum	Innerhalb des Netzanschlussraumes werden die hier aufgeführten IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • NET-0001 – CE-Router (Betriebsnetz) • NET-0002 – Firewall
INF-0005	Rechenzentrum/Technikraum (AM/KH)	Innerhalb des Rechenzentrums bzw. des Technikraums einer Autobahnmeisterei (AM) bzw. Kabelhauses (KH) werden die hier aufgeführten IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • NET-0003 – Switch • NET-0004 – Analoges Modem • NET-0005 – xDSL-Modem • SYS-0001 – Kommunikationsrechner Inselbus (KRI) / Portserver Seriell • SYS-0002 – Server Unterzentrale

ID	Räume und Gebäude	Erläuterung
INF-0006	Büro Verkehrsmanagement	Innerhalb des Büros fürs Verkehrsmanagement werden die hier aufgeführten IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • SYS-0003 – Drucker • SYS-0004 – Operatoren-PC
INF-0007	Leitstelle	Innerhalb des Raumes „Leitstelle“ werden die hier aufgeführten IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • NET-0003 – Switch • SYS-0003 – Drucker • SYS-0004 – Operatoren-PC • SYS-0005 – Videowand • SYS-0006 – Console Videowand
INF-0008	Streckenstation (extern)	Innerhalb der externen Streckenstation werden die hier aufgeführten IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • NET-0003 – Switch • NET-0004 – Analoges Modem • NET-0005 – xDSL-Modem • SYS-0007 – Elektronische Streckenstation
INF-0009	Rechenzentrum/Technikraum (VZ)	Innerhalb des Rechenzentrums bzw. des Technikraums der Verkehrszentrale bzw. Ersatz-Verkehrszentrale werden die hier aufgeführten IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • NET-0003 – Switch • SYS-0011 – Zentrale Services • SYS-0012 – Zentrale Protokollierung • SYS-0013 – Virtualisierungsinfrastruktur • SYS-0014 – Server zentrale Steuerung/Anzeige

ID	Räume und Gebäude	Erläuterung
INF-0010	Tunnelbetriebsgebäude (TBG)	In einem Tunnelbetriebsgebäude (TBG) werden in den hier aufgeführten Räumen IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • INF-0004 – Netzanschlussraum • INF-0011 – Lokale Ersatz-Leitstelle • INF-0012 – Rechenzentrum/Technikraum (TBG)
INF-0011	Lokale Ersatz-Leitstelle	Innerhalb des Büros fürs Verkehrsmanagement werden die hier aufgeführten IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • SYS-0003 – Drucker • SYS-0015 –Bedienrechner ZLT
INF-0012	Rechenzentrum/Technikraum (TBG)	Innerhalb des Rechenzentrums bzw. des Technikraums des Tunnelbetriebsgebäudes (TBG) werden die hier aufgeführten IT-Systeme (IT/OT) und Netzkomponenten im Geltungsbereich der KritisV betrieben: • NET-0003 – Switch • SYS-0016 – Brandmeldeanlage (TBG) • SYS-0014 – Server zentrale Steuerung/Anzeige • SYS-0017 – BOS Notfallbedienkonsole • IND-0001 – SPS / Automatisierungsebene • SYS-0023 – Ringspeicher

ID	Räume und Gebäude	Erläuterung
INF-0013	Tunnel	In einem Tunnel werden die hier aufgeführten IT-Systeme (IT/OT) und Netzkomponenten im Geltungsbereich der KritisV betrieben: • IND-0002 – Beleuchtung • IND-0003 – Lüftung • IND-0004 – Aktive Leiteinrichtung, Fluchtwegkennzeichnung • SYS-0018 – Branderkennung und Brandmeldeanlage (Tunnel) • SYS-0019 – Videoüberwachung • NET-0006 – Tunnelnotruf • NET-0007 – BOS-Funk, Betriebsfunk (Tunnel) • SYS-0020 – Rundfunkversorgung • SYS-0021 – Elektroakustische Anlage • SYS-0022 – Verkehrsbeeinflussung inkl. Tunnelsperranlage Die benötigten Infrastrukturen zur Bereitstellung einer Mittelspannung / Energieversorgung sowie Unterbrechungsfreie Stromversorgung sind integraler Bestandteil des Gebäudes “Tunnel”
INF-0014	Tunnelleitzentrale (TLZ)	In einer Tunnelleitzentrale (TLZ) werden in den hier aufgeführten Räumen IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • INF-0004 – Netzanschlussraum • INF-0019 – Büro Tunnelmanagement • INF-0007 – Leitstelle • INF-0015 – Rechenzentrum/Technikraum (TLZ)

ID	Räume und Gebäude	Erläuterung
INF-0015	Rechenzentrum/Technikraum (TLZ)	Innerhalb des Rechenzentrums bzw. des Technikraum der Tunnelleitzentrale (TLZ) bzw. Ersatz-Tunnelleitzentrale (eTLZ) werden die hier aufgeführten IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • NET-0003 – Switch • SYS-0011 – Zentrale Services • SYS-0012 – Zentrale Protokollierung • SYS-0013 – Virtualisierungsinfrastruktur • SYS-0014 – Server zentrale Steuerung/Anzeige
INF-0016	Ersatz-Tunnelleitzentrale (eTLZ)	In einer Ersatz-Tunnelleitzentrale (eTLZ) werden in den hier aufgeführten Räumen IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • INF-0004 – Netzanschlussraum • INF-0019 – Büro Tunnelmanagement • INF-0007 – Leitstelle • INF-0015 – Rechenzentrum/Technikraum (TLZ)
INF-0017	Büro Disponent	In einem Raum Büro Disponent werden die hier aufgeführten IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • SYS-0004 – Operatoren-PC • NET-0003 – Switch
INF-0018	Pumpenhaus	Im Gebäude Pumpenhaus wird das hier aufgeführte IT-Systeme im Geltungsbereich der KritisV betrieben: • IND-0007 – SPS (Pumpensteuerung)
INF-0019	Büro Tunnelmanagement	Innerhalb des Büros für Tunnelmanagement werden die hier aufgeführten IT-Systeme und Netzkomponenten im Geltungsbereich der KritisV betrieben: • SYS-0003 – Drucker • SYS-0004 – Operatoren-PC

Tabelle 7: Strukturanalyse – Räume und Gebäude

3. Schutzbedarf

Alle Daten (und damit auch die sie verarbeitenden Systeme) müssen gemäß den Sicherheitszielen Vertraulichkeit, Verfügbarkeit und Integrität durch den Informationseigentümer klassifiziert und dementsprechend gekennzeichnet sein, um jederzeit eine angemessene Verarbeitung der Informationen zu gewährleisten.

Die Informationsklassifizierungen erfolgen nach der im BSI-Standard 200-2 dargestellten Vorgehensweise und bezieht sich dementsprechend auf die Sicherheitsziele **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und im Bereich der kritischen Infrastruktur (KRITIS) zusätzlich auf die **Authentizität**. Die Zuordnung des Schutzbedarfs erfolgt jeweils in den Stufen „**normal**“, „**hoch**“ und „**sehr hoch**“.

	Szenario	**Normal**	**Hoch**	**Sehr hoch**
Verfügbarkeit	Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Ein Ausfall der Plattform bzw. des Verfahrens zugehörig der Serviceklasse **Bronze** führt zu Beeinträchtigungen der verarbeitenden Prozesse. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen einer Stunde und in der Serviceklasse Bronze festgelegter Parameter.	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Ein Ausfall der Plattform bzw. des Verfahrens zugehörig der Serviceklasse **Silber** führt zu Beeinträchtigungen der verarbeitenden Prozesse. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen einer Stunde und in der Serviceklasse Silber festgelegter Parameter.	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Ein Ausfall der Plattform bzw. des Verfahrens zugehörig der Serviceklasse **Gold** führt zu Beeinträchtigungen der verarbeitenden Prozesse. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen 30 Minuten und in der Serviceklasse Gold festgelegter Parameter.
	Verstöße gegen Gesetze, Vorschriften und Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. Vertragsverletzungen mit hohen Konventionalstrafen.	Fundamentaler Verstoß gegen Vorschriften und Gesetze. Vertragsverletzungen, deren Haftungsschäden sehr hoch für die Institution sind.

	Szenario	Normal	Hoch	Sehr hoch
	Beeinträchtigung der informationellen Selbstbestimmung	Verstöße gegen Art. 15, 12 III DSGVO können zu einer Beeinträchtigung der informationellen Selbstbestimmung führen.	Verstöße gegen Art. 15, 12 III DSGVO führen zu einer Beeinträchtigung der informationellen Selbstbestimmung.	Verstöße gegen Art. 15, 12 III DSGVO führen zu einer erheblichen Beeinträchtigung der informationellen Selbstbestimmung.
	Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.	Eine Beeinträchtigung der persönlichen Unversehrtheit ist möglich. Es besteht erhöhte Gefahr für Leib und Leben.	Es besteht unmittelbare Gefahr für Leib und Leben. Durch fehlende Zugriffsmöglichkeit auf die Informationen/Daten besteht unmittelbar Gefahr einer gravierenden Beeinträchtigung für Betroffene.
	Negative Außenwirkung	Es ist eine nur geringe negative Außenwirkung bzw. ein interner Vertrauensverlust anzunehmen. Beeinträchtigungen werden von Kunden/Mitarbeitenden als bedeutungslos eingeschätzt bzw. gar nicht wahrgenommen. Das Vertrauen ist punktuell beeinträchtigt (einzelne Mitarbeitende, einzelner Bereich / Service) und nicht flächendeckend auf den gesamten Betreiber der Bundesautobahn bezogen.	Ein erheblicher öffentlicher sowohl temporärer als auch dauerhafter Vertrauensverlust für den Betreiber der Bundesautobahn ist anzunehmen. Der fehlende Zugriff auf Informationen/Daten bzw. der Ausfall des Verfahrens wird von Kunden/Mitarbeitenden bemerkt und wahrgenommen. Das Vertrauen in den Betreiber der Bundesautobahn ist bei einzelnen Kunden/Mitarbeitende beeinträchtigt.	Ein enormer öffentlicher Vertrauensverlust ist für den Betreiber der Bundesautobahn anzunehmen. Es drohen politische Konsequenzen. Ein Großteil der Kunden/Mitarbeitenden beenden oder weigern die Nutzung des Verfahrens. Es entsteht ein Vertrauensverlust gegenüber einem Großteil der Kunden/Mitarbeitende mit erheblichen Zweifeln an die Zuverlässigkeit des Betreibers der Bundesautobahn.

	Szenario	Normal	Hoch	Sehr hoch
			Der Vertrauensverlust ist nur mit hohem Aufwand auszugleichen. Es entsteht ein Imageverlust, der sich auf weitere Teile des Betreibers der Bundesautobahn auswirkt. Einzelne Kunden/Mitarbeitende beenden oder weigern die Nutzung des Verfahrens.	Das Image wird erheblich beschädigt und wirkt sich auf die gesamte Bundesautobahn aus. Der Imageverlust kann auf unbestimmte Zeit nicht ausgeglichen werden.
	Finanzielle Auswirkungen	Der finanzielle Schaden beläuft sich für den Haushalt auf ≤ €€.	Der finanzielle Schaden beläuft sich für den Haushalt auf ≤ €€€€.	Der finanzielle Schaden beläuft sich für den Haushalt auf ≥ €€€€.

Tabelle 8: Sicherheitsziel Verfügbarkeit - Informationsklassifizierung und Kritikalitätsmatrix

	Szenario	Normal	Hoch	Sehr hoch
	Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden.	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt.	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden.

	Szenario	Normal	Hoch	Sehr hoch
Vertraulichkeit	Verstöße gegen Gesetze, Vorschriften und Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. Vertragsverletzungen mit hohen Konventionalstrafen.	Fundamentaler Verstoß gegen Vorschriften und Gesetze. Daten, die besonderen rechtlichen Verschwiegenheitsbeschränkungen unterliegen und deren Preisgabe einen Straftatbestand darstellen. Vertragsverletzungen, deren Haftungsschäden sehr hoch sind.
	Beeinträchtigung der informationellen Selbstbestimmung	Eine Veröffentlichung personenbezogener Daten hätte für die Betroffenen hinsichtlich ihrer gesellschaftlichen Stellung oder ihrer wirtschaftlichen Verhältnisse nur geringfügige Konsequenzen. Es handelt sich nicht um personenbezogene Daten.	Beeinträchtigungen hätten gravierende wirtschaftliche und/oder soziale Konsequenzen für die Betroffenen und sind unter keinen Umständen zu tolerieren. Im Falle der erheblichen Beeinträchtigung handelt es sich um personenbezogene Daten. Es kann sich hierbei auch um besondere Kategorien personenbezogener Daten gemäß Artikel 9 oder Daten gemäß Artikel 10 DSGVO handeln.	Beeinträchtigungen hätten gravierende wirtschaftliche und/oder soziale Konsequenzen für die Betroffenen und sind unter keinen Umständen zu tolerieren. Im Falle der erheblichen Beeinträchtigung handelt es sich um personenbezogene Daten. Es kann sich hierbei auch um besondere Kategorien personenbezogener Daten gemäß Artikel 9 oder Daten gemäß Artikel 10 DSGVO handeln.
	Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.	Eine Beeinträchtigung der persönlichen Unversehrtheit	Es besteht unmittelbare Gefahr für Leib und Leben.

	Szenario	Normal	Hoch	Sehr hoch
			ist möglich. Es besteht erhöhte Gefahr für Leib und Leben.	
	Negative Außenwirkung	Es ist eine nur geringe negative Außenwirkung bzw. ein interner Vertrauensverlust anzunehmen. Beeinträchtigungen werden von Kunden/Mitarbeitende als bedeutungslos eingeschätzt bzw. gar nicht wahrgenommen. Das Vertrauen ist punktuell beeinträchtigt (einzelne Mitarbeitende /Service) und nicht flächendeckend auf den Betreiber der Bundesautobahn bezogen.	Ein erheblicher öffentlicher sowohl temporärer als auch dauerhafter Vertrauensverlust für den Betreiber der Bundesautobahn ist anzunehmen. Der fehlende Zugriff auf Daten bzw. der Ausfall des Verfahrens wird von Kunden/Mitarbeitende bemerkt und wahrgenommen. Das Vertrauen in den Betreiber der Bundesautobahn ist bei einzelnen Kunden/Mitarbeitende beeinträchtigt. Es entsteht ein Imageverlust, der sich auf weitere Teile des Betreibers der Bundesautobahn auswirkt.	Ein enormer öffentlicher Vertrauensverlust ist anzunehmen. Es drohen politische Konsequenzen. Es entsteht ein Vertrauensverlust gegenüber einem Großteil der Kunden/Mitarbeitende mit erheblichen Zweifeln an die Verschwiegenheit beim Umgang mit vertraulichen Daten. Das Image wird erheblich beschädigt und wirkt sich auf den Betreiber der Bundesautobahn aus. Der Imageverlust kann auf unbestimmte Zeit nicht ausgeglichen werden.
	Finanzielle Auswirkungen	Der finanzielle Schaden beläuft sich für den Haushalt auf ≤ €€.	Der finanzielle Schaden beläuft sich für den Haushalt auf ≤ €€€€.	Der finanzielle Schaden beläuft sich für den Haushalt auf ≥ €€€€.

Tabelle 9: Sicherheitsziel Vertraulichkeit - Informationsklassifizierung und Kritikalitätsmatrix

	Szenario	Normal	Hoch	Sehr hoch
Integrität	Beeinträchtigung der Aufgabenerfüllung	Bei Eintritt einer Verfälschung und/oder Löschung Daten sind die Schäden begrenzt. Es entstehen Beeinträchtigungen in der Bearbeitung von Aufgaben (z.B. längere Bearbeitungszeit, umständlicherer Bearbeitung, höherer Aufwand bei der Beschaffung von Informationen). Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen einer Stunde und in der Serviceklasse Bronze festgelegter Parameter.	Bei Eintritt einer Verfälschung und/oder Löschung Daten sind die Schäden begrenzt. Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Die Verfälschung und/oder Löschung führt zu erheblichen Arbeitseinschränkungen. Eine schnelle Erkennung und Behebung der Verfälschung / Schäden ist erforderlich. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen einer Stunde und in der Serviceklasse Silber festgelegter Parameter.	Vorsätzliche oder durch Fehlfunktion verursachte Verfälschungen von Daten führen zu Schäden in sehr großem Ausmaß. Bei Eintritt einer Verfälschung und/oder Löschung entsteht eine Arbeitsunfähigkeit und/oder Unmöglichkeit der Leistungserbringung. Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Eine Verfälschung der Daten ist zu verhindern. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen 30 Minuten und in der Serviceklasse Gold festgelegter Parameter.
	Verstöße gegen Gesetze, Vorschriften und Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. Vertragsverletzungen mit hohen Konventionalstrafen.	Fundamentaler Verstoß gegen Vorschriften und Gesetze. Daten, die besonderen rechtlichen Verschwiegenheitsbeschränkungen unterliegen und deren Preisgabe einen Straftatbestand darstellen.

	Szenario	Normal	Hoch	Sehr hoch
				Vertragsverletzungen, deren Haftungsschäden sehr hoch sind.
	Beeinträchtigung der informationellen Selbstbestimmung	Eine Veränderung, Verfälschung und/oder Löschung personenbezogener Daten hätte für die Betroffenen hinsichtlich ihrer gesellschaftlichen Stellung oder ihrer wirtschaftlichen Verhältnisse nur geringfügige Konsequenzen. Es handelt sich nicht um personenbezogene Daten.	Beeinträchtigungen hätten gravierende wirtschaftliche und/oder soziale Konsequenzen für die Betroffenen und sind unter keinen Umständen zu tolerieren. Im Falle der erheblichen Beeinträchtigung handelt es sich um personenbezogene Daten. Es kann sich hierbei auch um besondere Kategorien personenbezogener Daten gemäß Artikel 9 oder Daten gemäß Artikel 10 DSGVO handeln.	Beeinträchtigungen hätten gravierende wirtschaftliche und/oder soziale Konsequenzen für die Betroffenen und sind unter keinen Umständen zu tolerieren. Im Falle der erheblichen Beeinträchtigung handelt es sich um personenbezogene Daten. Es kann sich hierbei auch um besondere Kategorien personenbezogener Daten gemäß Artikel 9 oder Daten gemäß Artikel 10 DSGVO handeln.
	Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.	Eine Beeinträchtigung der persönlichen Unversehrtheit ist möglich. Es besteht erhöhte Gefahr für Leib und Leben.	Es besteht unmittelbare Gefahr für Leib und Leben.

	Szenario	Normal	Hoch	Sehr hoch
	Negative Außenwirkung	Es ist eine nur geringe negative Außenwirkung bzw. ein interner Vertrauensverlust anzunehmen. Beeinträchtigungen werden von Kunden/Mitarbeitende als bedeutungslos eingeschätzt bzw. gar nicht wahrgenommen. Das Vertrauen ist punktuell beeinträchtigt (einzelne Mitarbeitende, einzelner Bereich/Service) und nicht flächendeckend auf den Betreiber der Bundesautobahn bezogen.	Ein erheblicher öffentlicher sowohl temporärer als auch dauerhafter Vertrauensverlust für den Betreiber der Bundesautobahn ist anzunehmen. Der fehlende Zugriff auf Daten bzw. der Ausfall des Verfahrens wird von Kunden/Mitarbeitenden bemerkt und wahrgenommen. Das Vertrauen in den Betreiber der Bundesautobahn ist bei einzelnen Kunden/Mitarbeitende beeinträchtigt. Es entsteht ein Imageverlust, der sich auf weitere Teile des Betreibers der Bundesautobahn auswirkt.	Ein enormer öffentlicher Vertrauensverlust ist anzunehmen. Es drohen politische Konsequenzen. Es entsteht ein Vertrauensverlust gegenüber einem Großteil der Kunden/Mitarbeitende mit erheblichen Zweifeln an die Verschwiegenheit beim Umgang mit vertraulichen Daten. Das Image wird erheblich beschädigt und wirkt sich auf den Betreiber der Bundesautobahn aus. Der Imageverlust kann auf unbestimmte Zeit nicht ausgeglichen werden.
	Finanzielle Auswirkungen	Der finanzielle Schaden beläuft sich für den Haushalt auf ≤ €€.	Der finanzielle Schaden beläuft sich für den Haushalt auf ≤ €€€€.	Der finanzielle Schaden beläuft sich für den Haushalt auf ≥ €€€€.

Tabelle 10: Sicherheitsziel Integrität - Informationsklassifizierung und Kritikalitätsmatrix

	Szenario	Normal	Hoch	Sehr hoch
Authentizität	Beeinträchtigung der Aufgabenerfüllung	Der Verlust der Eigenschaft, die Aussagen, Quellen, Dingen oder Orten zukommt, um ihre Echtheit, Glaubwürdigkeit oder Zuverlässigkeit zu kennzeichnen (Authentizität) verlangsamt interne Geschäftsprozesse des Betreibers der Bundesautobahn. Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Daten können durch Abgleich mit integren Daten innerhalb der festgelegten Parameter wieder hergeleitet werden. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen einer Stunde und in der Serviceklasse Gold festgelegter Parameter.	Der Verlust der Authentizität verzögert Geschäftsprozesse. Eine negative Innen- und Außenwirkung kann für die Betreiber der Bundesautobahn nicht ausgeschlossen werden. Mangelnde Authentizität beeinflusst im geringen bis mittleres Maß die Aufgabenerfüllung. Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Daten können durch Abgleich mit integren Daten innerhalb der festgelegten Parameter wieder hergeleitet werden. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen einer Stunde und in der Serviceklasse Silber festgelegter Parameter.	Der Verlust der Authentizität verhindert Geschäftsprozesse. Mangelnde Korrektheit und Vollständigkeit der Daten beeinflusst die Aufgabenerfüllung bis hin zur Aufgabenverhinderung und führt zu sehr schwerwiegenden Schäden. Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Eine Verfälschung der Daten ist zu verhindern. Ein Großteil der Daten kann durch Abgleich mit integren Daten innerhalb der festgelegten Parameter wieder hergeleitet werden. Die maximal tolerierbare Ausfallzeit (MTA) liegt zwischen 30 Minuten und in der Serviceklasse Gold festgelegter Parameter.

	Szenario	Normal	Hoch	Sehr hoch
	Verstöße gegen Gesetze, Vorschriften und Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. Vertragsverletzungen mit hohen Konventionalstrafen.	Fundamentaler Verstoß gegen Vorschriften und Gesetze. Daten, die besonderen rechtlichen Verschwiegenheitsbeschränkungen unterliegen und deren Preisgabe einen Straftatbestand darstellen. Vertragsverletzungen, deren Haftungsschäden sehr hoch sind.
	Beeinträchtigung der informationellen Selbstbestimmung	Eine Veränderung, Verfälschung und/oder Löschung personenbezogener Daten hätte für die Betroffenen hinsichtlich ihrer gesellschaftlichen Stellung oder ihrer wirtschaftlichen Verhältnisse nur geringfügige Konsequenzen. Es handelt sich nicht um personenbezogene Daten.	Beeinträchtigungen hätten gravierende wirtschaftliche und/oder soziale Konsequenzen für die Betroffenen und sind unter keinen Umständen zu tolerieren. Im Falle der erheblichen Beeinträchtigung handelt es sich um personenbezogene Daten. Es kann sich hierbei auch um besondere Kategorien personenbezogener Daten gemäß Artikel 9 oder Daten gemäß Artikel 10 DSGVO handeln.	Beeinträchtigungen hätten gravierende wirtschaftliche und/oder soziale Konsequenzen für die Betroffenen und sind unter keinen Umständen zu tolerieren. Im Falle der erheblichen Beeinträchtigung handelt es sich um personenbezogene Daten. Es kann sich hierbei auch um besondere Kategorien personenbezogener Daten gemäß Artikel 9 oder Daten gemäß Artikel 10 DSGVO handeln.
	Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.	Eine Beeinträchtigung der persönlichen Unversehrtheit	Es besteht unmittelbare Gefahr für Leib und Leben.

	Szenario	Normal	Hoch	Sehr hoch
			ist möglich. Es besteht erhöhte Gefahr für Leib und Leben.	
	Negative Außenwirkung	Es ist eine nur geringe negative Außenwirkung bzw. ein interner Vertrauensverlust anzunehmen. Beeinträchtigungen werden von Kunden/Mitarbeitende als bedeutungslos eingeschätzt bzw. gar nicht wahrgenommen. Das Vertrauen ist punktuell beeinträchtigt (einzelne Mitarbeitende, einzelner Bereich/Service) und nicht flächendeckend auf den Betreiber der Bundesautobahn bezogen.	Ein erheblicher öffentlicher sowohl temporärer als auch dauerhafter Vertrauensverlust für den Betreiber der Bundesautobahn ist anzunehmen. Der fehlende Zugriff auf Daten bzw. der Ausfall des Verfahrens wird von Kunden/Mitarbeitenden bemerkt und wahrgenommen. Das Vertrauen in den Betreiber der Bundesautobahn ist bei einzelnen Kunden/Mitarbeitende beeinträchtigt. Es entsteht ein Imageverlust, der sich auf weitere Teile des Betreibers der Bundesautobahn auswirkt.	Ein enormer öffentlicher Vertrauensverlust ist anzunehmen. Es drohen politische Konsequenzen. Es entsteht ein Vertrauensverlust gegenüber einem Großteil der Kunden/Mitarbeitende mit erheblichen Zweifeln an die Verschwiegenheit beim Umgang mit vertraulichen Daten. Das Image wird erheblich beschädigt und wirkt sich auf den Betreiber der Bundesautobahn aus. Der Imageverlust kann auf unbestimmte Zeit nicht ausgeglichen werden.
	Finanzielle Auswirkungen	Der finanzielle Schaden beläuft sich für den Haushalt auf ≤ €€.	Der finanzielle Schaden beläuft sich für den Haushalt auf ≤ €€€€.	Der finanzielle Schaden beläuft sich für den Haushalt auf ≥ €€€€.

Tabelle 11: Sicherheitsziel Authentizität - Informationsklassifizierung und Kritikalitätsmatrix

3.1 Schutzbedarfserhebung für die Prozesse

3.1.1 Prozess: Durchführung des Straßenbetriebsdienstes (P-0001)

Grundwert	Schutzbedarf	Begründung
Verfügbarkeit	normal	Im Rahmen der Einsatzplanung und Umfeldbeobachtung kommen unterschiedliche Informationsbasen (neben den Wetterinformationen und Sensordaten [SWIS]) zum Einsatz. Sollten einzelne Informationen kurzfristig ausfallen, werden auf Basis der Erfahrungen der Mitarbeitenden der Autobahnmeisterei anhand der Wetter und Baustellensituation entsprechende Maßnahmen, welche Kurz- bis Langfristig durchzuführen sind, initiiert. Hieraus ableitend, führt ein Ausfall einzelner Informationssätze nicht zur Unterbrechung des Service an sich.
Integrität	normal	Die Daten der Sensoren weisen auf Grund ihres Verwendungszweckes eine Kurzlebigkeit auf. Ebenfalls werden diese Daten kontinuierlich aktualisiert. Hieraus ableitend wäre der Verlust der Integrität einzelner Datensätze nicht von Relevanz im Rahmen der Umfeldbeobachtung sowie der Begutachtung des Straßenzustands.
Vertraulichkeit	hoch (ggf. normal)	Im Rahmen der Einsatzplanung und Umfeldbeobachtung werden personenbeziehbare Daten wie KFZ-Kennzeichen sowie Gesichter der Kraftfahrzeugführer erfasst. Sollten unberechtigte Dritte auf die erhobenen Daten zugreifen, muss der Betreiber der kritischen Anlage mit erheblichen Konsequenzen auf Grund von Verstößen gegen Vorschriften und Gesetze rechnen. In der Regel sollen die personenbezogenen Daten jedoch nur intern in den Kameras erfasst werden. Ist dies immer der Fall, kann der Schutzbedarf für diesen Prozess auf normal gesetzt werden. Für die Kamera ist er hingegen immer noch hoch.
Authentizität	normal	Die gewonnenen Sensordaten weisen bedingt durch die Art der Erhebung und des Verwendungszweckes eine Kurzlebigkeit auf. Zum Zwecke der Authentizität werden die eingesetzten Sensoren an Industrielle Komponenten (SPS) hardwareseitig verknüpft. Hieraus ableitend wäre der Verlust der Authentizität nicht von Relevanz bei der Begutachtung des Straßenzustands.

Tabelle 12: Schutzbedarfserhebung - Prozess P-0001

3.1.2 Prozess: Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur (P-0002)

Grundwert	Schutzbedarf	Begründung
Verfügbarkeit	normal	Insofern der Verkehrsfluss auf der Bundesautobahn nicht durch die Risiken von Gefahrguttransporten gefährdet

Grundwert	Schutzbedarf	Begründung
		bzw. die Relevanz des Bauwerkes für den Verkehrsfluss im Rahmen der Versorgung einer Stadt bzw. Region oder eines kritischen Dienstleisters oder eines Dienstleisters im besonderen öffentlichen Interesse von Relevanz ist, würde eine Beeinträchtigung von den Betroffenen als tolerabel nach derzeitiger Informationslage eingeschätzt werden.
Integrität	hoch	Manipulierte oder verfälschte Softwarekomponenten der Tunnelsteuerung können zu nicht akzeptierbaren Personenschäden (persönliche Unversehrtheit) führen.
Vertraulichkeit	hoch (ggf. normal)	Im Rahmen der Funktionsprüfung können personenbeziehbare Daten wie KFZ-Kennzeichen sowie Gesichter der Kraftfahrzeugführer eingesehen werden. Sollten unberechtigte Dritte auf die erhobenen Daten zugreifen, muss der Betreiber der kritischen Anlage mit erheblichen Konsequenzen auf Grund von Verstößen gegen Vorschriften und Gesetze rechnen. In der Regel sollen die personenbezogenen Daten jedoch nur intern im erfassenden System verarbeitet werden. Ist dies immer der Fall, kann der Schutzbedarf für diesen Prozess auf normal gesetzt werden. Für das erfassende System ist er hingegen immer noch hoch.
Authentizität	hoch	Durch nicht erkannte Manipulierte oder verfälschte Softwarekomponenten der Tunnelsteuerung besteht die Gefahr des Verlustes der gewünschten Berechtigung und der hiermit meist einhergehenden unberechtigten Verwendung von personenbezogenen Daten. Dieses Fehlverhalten der Systeme und deren Software kann zu nicht akzeptierbaren Personenschäden (persönliche Unversehrtheit) führen.

Tabelle 13: Schutzbedarfserhebung - Prozess P-0002

3.1.3 Prozess: Operatives Verkehrsmanagement (P-0003)

Grundwert	Schutzbedarf	Begründung
Verfügbarkeit	normal	Insofern der Verkehrsfluss auf der Bundesautobahn nicht durch die Risiken von Gefahrguttransporten gefährdet bzw. die Relevanz des Bauwerkes für den Verkehrsfluss im Rahmen der Versorgung einer Stadt bzw. Region oder eines kritischen Dienstleisters oder eines Dienstleisters im besonderen öffentlichen Interesse von Relevanz ist, würde eine Beeinträchtigung von den Betroffenen als tolerabel nach derzeitiger Informationslage eingeschätzt werden.
Integrität	hoch	Manipulierte oder verfälschte Softwarekomponenten der Tunnelsteuerung können zu nicht akzeptierbaren Personenschäden (persönliche Unversehrtheit) führen.

Grundwert	Schutzbedarf	Begründung
Vertraulichkeit	hoch	Es entsteht ein erheblicher Vertrauens- und Imageverlust für den Betreiber der Autobahn, etwa durch die unberechtigte Nutzung der Notfallbedienkonsole am Tunnelportal oder am Tunnelbetriebsgebäude. Im Rahmen der Verkehrsbeobachtung (temporäre Seitenstreifenfreigabe, Tunnel, Strecke) können personenbezogene Daten wie KFZ-Kennzeichen sowie Gesichter der Kraftfahrzeugführer eingesehen werden. Sollten unberechtigte Dritte auf die erhobenen Daten zugreifen, muss der Betreiber der kritischen Anlage mit erheblichen Konsequenzen auf Grund von Verstößen gegen Vorschriften und Gesetze rechnen.
Authentizität	hoch	Durch nicht erkannte manipulierte oder verfälschte Softwarekomponenten der Tunnelsteuerung besteht die Gefahr des Verlustes der gewünschten Berechtigung und der hiermit meist einhergehenden unberechtigten Verwendung von personenbezogenen Daten. Dieses Fehlverhalten der Systeme und deren Software kann zu nicht akzeptierbaren Personenschäden (persönliche Unversehrtheit) führen.

Tabelle 14: Schutzbedarfserhebung - Prozess P-0003

3.1.4 Zusammenfassung der Schutzbedarfserhebung für die Prozesse

Prozess	Verfügbarkeit	Integrität	Vertraulichkeit	Authentizität	Maximum
P-0001 - Durchführung des Straßenbetriebsdienstes	normal	normal	hoch	normal	**hoch**
P-0002 - Instandhaltung von verkehrs-, betriebs-, nachrichten- und elektrotechnischer Infrastruktur	normal	hoch	hoch	hoch	**hoch**
P-0003 - Operatives Verkehrsmanagement	normal	hoch	hoch	hoch	**hoch**

Tabelle 15: Zusammenfassung der Schutzbedarfserhebung – Prozesse

3.2 Abgeleiteter Schutzbedarf für die Anwendungen

Anwendung	Verfügbarkeit	Integrität	Vertraulichkeit	Authentizität	Maximum
APP-0001 – Datenbank – Server zentrale Steuerung/Anzeige	normal	hoch	hoch	hoch	**hoch**
APP-0002 - Domain Name Service (DNS) - KRITIS	normal	hoch	hoch	hoch	**hoch**
APP-0003 - Network Time Protocol (NTP) - KRITIS	normal	hoch	hoch	hoch	**hoch**
APP-0004 - Dynamic Host Configuration Protocol (DHCP) - KRITIS	normal	hoch	hoch	hoch	**hoch**
APP-0005 – Verzeichnisdienst	normal	hoch	hoch	hoch	**hoch**
APP-0006 - Visualisierung Prozessleitsystem (Server)	normal	hoch	hoch	hoch	**hoch**
APP-0007 - Datenbank vom Prozessleitsystem	normal	hoch	hoch	hoch	**hoch**
APP-0008 - Visualisierung Prozessleitsystem (Client)	normal	hoch	hoch	hoch	**hoch**
APP-0009 - Videomanagement (Client-Anwendung)	normal	hoch	hoch	hoch	**hoch**
APP-0010 - Videomanagement (Server-Anwendung)	normal	hoch	hoch	hoch	**hoch**
APP-0011 – Steuerungssoftware-Server (gemäß MARZ)	normal	hoch	hoch	hoch	**hoch**
APP-0012 - Datenbank von Steuerungssoftware	normal	hoch	hoch	hoch	**hoch**
APP-0013 - Steuerungssoftware-Client (gemäß MARZ)	normal	hoch	hoch	hoch	**hoch**

Anwendung	Verfügbarkeit	Integrität	Vertraulichkeit	Authentizität	Maximum
APP-0014 - Kommunikationsrechner Inselbus (gemäß TLS)	normal	hoch	hoch	hoch	**hoch**
APP-0015 - Streckenstationssoftware (gemäß TLS)	normal	hoch	hoch	hoch	**hoch**
APP-0016 - Office-Anwendung	normal	hoch	hoch	hoch	**hoch**
APP-0017 - Web-Browser	normal	hoch	hoch	hoch	**hoch**

Tabelle 16: Abgeleiteter Schutzbedarf – Anwendungen

3.3 Abgeleiteter Schutzbedarf für die IT-Systeme

IT-Systeme	Verfügbarkeit	Integrität	Vertraulichkeit	Authentizität	Maximum
SYS-0001 - Kommunikationsrechner Inselbus (KRI) / Portserver Seriell	normal	hoch	hoch	hoch	**hoch**
SYS-0002 – Server Unterzentrale	normal	hoch	hoch	hoch	**hoch**
SYS-0003 – Drucker	normal	hoch	hoch	hoch	**hoch**
SYS-0004 – Operatoren-PC	normal	hoch	hoch	hoch	**hoch**
SYS-0005 – Videowand	normal	hoch	hoch	hoch	**hoch**
SYS-0006 – Console Videowand	normal	hoch	hoch	hoch	**hoch**
SYS-0007 – elektronische Streckenstation	normal	hoch	hoch	hoch	**hoch**
SYS-0008 – Wechselverkehrszeichen	normal	hoch	hoch	hoch	**hoch**
SYS-0009 – dWista-Anzeigesystem	normal	hoch	hoch	hoch	**hoch**
SYS-0010 – Kamera	normal	hoch	hoch	hoch	**hoch**
SYS-0011 – Zentrale Services	normal	hoch	hoch	hoch	**hoch**
SYS-0012 – Zentrale Protokollierung	normal	hoch	hoch	hoch	**hoch**
SYS-0013 – Virtualisierungsinfrastruktur	normal	hoch	hoch	hoch	**hoch**
SYS-0014 – Server zentrale Steuerung/Anzeige	normal	hoch	hoch	hoch	**hoch**
SYS-0015 –Bedienrechner ZLT	normal	hoch	hoch	hoch	**hoch**
SYS-0016 – Brandmeldeanlage (TBG)	normal	hoch	hoch	hoch	**hoch**
SYS-0017 – BOS Notfallbedienkonsole	normal	hoch	hoch	hoch	**hoch**
SYS-0018 – Branderkennung und Brandmeldeanlage (Tunnel)	normal	hoch	hoch	hoch	**hoch**

IT-Systeme	Verfügbarkeit	Integrität	Vertraulichkeit	Authentizität	Maximum
SYS-0019 – Videoüberwachung	normal	hoch	hoch	hoch	**hoch**
SYS-0020 – Rundfunkversorgung	normal	hoch	hoch	hoch	**hoch**
SYS-0021 – Elektroakustische Anlage	normal	hoch	hoch	hoch	**hoch**
SYS-0022 – Verkehrsbeeinflussung inkl. Tunnelsperranlage	normal	hoch	hoch	hoch	**hoch**
SYS-0023 - Ringspeicher	normal	hoch	hoch	hoch	**hoch**

Tabelle 17: Abgeleiteter Schutzbedarf – IT-Systeme

3.4 Abgeleiteter Schutzbedarf für die Industrielle IT

Industrielle IT	Verfügbarkeit	Integrität	Vertraulichkeit	Authentizität	Maximum
IND-0001 SPS / Automatisierungsebene	normal	hoch	hoch	hoch	**hoch**
IND-0002 – Beleuchtung	normal	hoch	hoch	hoch	**hoch**
IND-0003 – Lüftung	normal	hoch	hoch	hoch	**hoch**
IND-0004 – Aktive Leiteinrichtung, Fluchtwegkennzeichnung	normal	hoch	hoch	hoch	**hoch**
IND-0005 – Verkehrsdetektoren	normal	hoch	hoch	hoch	**hoch**
IND-0006 – Wettersensoren	normal	hoch	hoch	hoch	**hoch**
IND-0007 – SPS (Pumpensteuerung)	normal	hoch	hoch	hoch	**hoch**
IND-0008 – Pumpe (Entwässerung)	normal	hoch	hoch	hoch	**hoch**

Tabelle 18: Abgeleiteter Schutzbedarf – Industrielle IT

3.5 Abgeleiteter Schutzbedarf für die Netzkomponenten

Netzkomponente	Verfügbarkeit	Integrität	Vertraulichkeit	Authentizität	Maximum
NET-0001 – CE-Router (Betriebsnetz)	normal	hoch	hoch	hoch	**hoch**

Netzkomponente	Verfügbarkeit	Integrität	Vertraulichkeit	Authentizität	Maximum
NET-0002 – Firewall	normal	hoch	hoch	hoch	**hoch**
NET-0003 – Switch	normal	hoch	hoch	hoch	**hoch**
NET-0004 – Analoges Modem	normal	hoch	hoch	hoch	**hoch**
NET-0005 – xDSL-Modem	normal	hoch	hoch	hoch	**hoch**
NET-0006 – Tunnelnotruf	normal	hoch	hoch	hoch	**hoch**
NET-0007 – BOS-Funk, Betriebsfunk (Tunnel)	normal	hoch	hoch	hoch	**hoch**

Tabelle 19: Abgeleiteter Schutzbedarf – Netzkomponenten

3.6 Abgeleiteter Schutzbedarf für die Kommunikationsverbindungen

Der Schutzbedarf für die Kommunikationsverbindungen ergibt sich aus dem Schutzbedarf der jeweils abhängigen Anwendungen bzw. der übertragenen Daten.

3.7 Abgeleiteter Schutzbedarf für die Infrastruktur

Der Schutzbedarf für die Infrastruktur (Gebäude, Räume) ergibt sich aus dem abgeleiteten Schutzbedarf der Geschäftsprozesse, der Anwendungen, der IT-Systeme, der Industrielle-IT sowie der Netz-Komponenten.

Gebäude/Raum	Verfügbarkeit	Integrität	Vertraulichkeit	Authentizität	Maximum
INF-0001 - Autobahnmeisterei (AM) / Kabelhaus (KH)	normal	hoch	hoch	hoch	**hoch**
INF-0002 - Verkehrszentrale (VZ)	normal	hoch	hoch	hoch	**hoch**
INF-0003 - Ersatz-Verkehrszentrale (VZ)	normal	hoch	hoch	hoch	**hoch**
INF-0004 – Netzanschlussraum	normal	hoch	hoch	hoch	**hoch**
INF-0005 - Rechenzentrum/Technikraum (AM/KH)	normal	hoch	hoch	hoch	**hoch**
INF-0006 - Büro Verkehrsmanagement	normal	hoch	hoch	hoch	**hoch**
INF-0007 – Leitstelle	normal	hoch	hoch	hoch	**hoch**
INF-0008 – Streckenstation (extern)	normal	hoch	hoch	hoch	**hoch**

Gebäude/Raum	Verfügbarkeit	Integrität	Vertraulichkeit	Authentizität	Maximum
INF-0009 – Rechenzentrum/Technikraum (VZ)	normal	hoch	hoch	hoch	**hoch**
INF-0010 – Tunnelbetriebsgebäude (TBG)	normal	hoch	hoch	hoch	**hoch**
INF-0011 – lokale Ersatz-Leitstelle	normal	hoch	hoch	hoch	**hoch**
INF-0012 – Rechenzentrum/Technikraum (TBG)	normal	hoch	hoch	hoch	**hoch**
INF-0013 – Tunnel	normal	hoch	hoch	hoch	**hoch**
INF-0014 – Tunnelleitzentrale (TLZ)	normal	hoch	hoch	hoch	**hoch**
INF-0015 – Rechenzentrum/Technikraum (TLZ)	normal	hoch	hoch	hoch	**hoch**
INF-0016 – Ersatz-Tunnelleitzentrale (eTLZ)	normal	hoch	hoch	hoch	**hoch**
INF-0017 – Büro Disponent	normal	hoch	hoch	hoch	**hoch**
INF-0018 – Pumpenhaus	normal	hoch	hoch	hoch	**hoch**
INF-0019 – Büro Tunnelmanagement	normal	hoch	hoch	hoch	**hoch**

Tabelle 20: abgeleiteter Schutzbedarf – Infrastrukturen (Gebäude/Räume)

4. Modellierung nach IT-Grundschutz

Die Modellierung nach IT-Grundschutz umfasst die Abbildung der in Kapitel 2 identifizierten Zielobjekte auf Bausteine des BSI IT-Grundschutz-Kompendium (siehe 8.3, Buchstabe f) in der Version 02/2021. Die folgenden Tabellen in den Kapiteln 4.1 bis 4.9 beschreiben, welche Bausteine in diesem Sicherheitskonzept betrachtet werden.

4.1 Schicht ISMS

Baustein	Ja	Nein	Begründung
ISMS.1 Sicherheitsmanagement		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.

Tabelle 21: Modellierung - Schicht ISMS

4.2 Schicht ORP (Organisation und Personal)

Baustein	Ja	Nein	Begründung
ORP.1 Organisation		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
ORP.2 Personal		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
ORP.4 Identitäts- und Berechtigungsmanagement	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.
ORP.5 Compliance Management (Anforderungsmanagement)		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.

Tabelle 22: Modellierung - Schicht ORP (Organisation und Personal)

4.3 Schicht CON (Konzepte und Vorgehensweisen)

Baustein	Ja	Nein	Begründung
CON.1 Kryptokonzept	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.
CON.2 Datenschutz		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
CON.3 Datensicherungskonzept	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.
CON.6 Löschen und Vernichten		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
CON.7 Informationssicherheit auf Auslandsreisen		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
CON.8 Software-Entwicklung	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.
CON.9 Informationsaustausch		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
CON.10 Entwicklung von Webanwendungen	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.

Tabelle 23: Modellierung - Schicht CON (Konzepte und Vorgehensweisen)

4.4 Schicht OPS (Betrieb)

Baustein	Ja	Nein	Begründung
OPS.1.1.2 Ordnungsgemäße IT-Administration		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
OPS.1.1.3 Patch- und Änderungsmanagement	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.
OPS.1.1.4 Schutz vor Schadprogrammen	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.
OPS.1.1.5 Protokollierung	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.
OPS.1.1.6 Software-Tests und –Freigaben	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.
OPS.1.2.2 Archivierung		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
OPS.1.2.4 Telearbeit		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
OPS.1.2.5 Fernwartung	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.
OPS.2.1 Outsourcing für Kunden	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.

Baustein	Ja	Nein	Begründung
OPS.2.2 Cloud-Nutzung		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
OPS.3.1 Outsourcing für Dienstleister		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.

Tabelle 24: Modellierung - Schicht OPS (Betrieb)

4.5 Schicht DER (Detektiv und Reaktion)

Baustein	Ja	Nein	Begründung
DER.1 Detektion von sicherheitsrelevanten Ereignissen	X		Die Betrachtung dieses Bausteines erfolgt in Bezug auf die für dieses Sicherheitskonzept involvierten Zielobjekte der kritischen Infrastrukturen.
DER.2.1 Behandlung von Sicherheitsvorfällen		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
DER.2.2 Vorsorge für die IT-Forensik		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
DER.3.1 Audits und Revisionen		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
DER.4 Notfallmanagement		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.

Tabelle 25: Modellierung - Schicht DER (Detektiv und Reaktion)

4.6 Schicht APP (Anwendungen)

Baustein	Ja	Nein	Begründung
APP.1.1 Office-Produkte	**X**		Der Baustein APP.1.1 „Office-Produkte“ ist für jedes installierte Office Produkt auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • APP-0016 - Office-Anwendung
APP.1.2 Web-Browser	**X**		Der Baustein APP.1.2 „Webbrowser“ ist für jeden installierten Webbrowser auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • APP-0017 - Web-Browser
APP.1.4 Mobile Anwendungen (Apps)		**X**	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
APP.2.1 Allgemeiner Verzeichnisdienst	**X**		Der Baustein APP.2.1 „Allgemeiner Verzeichnisdienst“ ist auf alle verwendeten Verzeichnisdienste des Informationsverbundes anzuwenden. Hieraus ableitend ist dieser mindestens einmal auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • APP-0005 – Verzeichnisdienst
APP.2.2 Active Directory	**X**		Insofern der Betreiber von kritischen Infrastrukturen im Geltungsbereich ein Microsoft Active Directory betreibt ist zusätzlich zum Baustein APP.2.1 der Baustein APP.2.2 auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • APP-0005 – Verzeichnisdienst Sollten zusätzlich noch ein Verzeichnisdienst auf Basis von OpenLDAP parallel betrieben werden, sind pro Verzeichnisdienst ein eigenständiges Zielobjekt zu erstellen.
APP.2.3 OpenLDAP	**X**		Insofern der Betreiber von kritischen Infrastrukturen im Geltungsbereich kein Microsoft Active Directory, sondern ein OpenLDAP betreibt ist zusätzlich zum Baustein APP.2.1 der Baustein APP.2.3 auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • APP-0005 – Verzeichnisdienst

Baustein	Ja	Nein	Begründung
			Sollten zusätzlich noch ein Verzeichnisdienst auf Basis von Microsoft Active Directory parallel betrieben werden, sind pro Verzeichnisdienst ein eigenständiges Zielobjekt zu erstellen.
APP.3.1 Webanwendungen		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
APP.3.2 Webserver		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
APP.3.3 Fileserver		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
APP.3.4 Samba		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
APP 3.6 DNS-Server	X		Der Baustein APP.3.6 „DNS-Server“ ist auf jeden im Informationsverbund eingesetzten DNS-Server durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein APP.3.6 auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • APP-0002 - Domain Name Service (DNS) - KRITIS
APP.4.2 SAP-ERP-System		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
APP.4.3 Relationale Datenbanksysteme	X		Der Baustein APP.4.3 „Relationale Datenbanksysteme“ ist auf jedes relationale Datenbanksystem im Informationsverbund einmal durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein APP.4.3 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • APP-0001 - Datenbank – Server zentrale Steuerung/Anzeige

Baustein	Ja	Nein	Begründung
			• APP-0007 - Datenbank vom Prozessleitsystem • APP-0012 - Datenbank von Steuerungssoftware
APP.4.6 SAP ABAP-Programmierung		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
APP.5.2 Microsoft Exchange und Outlook		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
APP.5.3 Allgemeiner E-Mail-Client und -Server		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
APP.6 Allgemeine Software	X		Der Baustein APP.6 „Allgemeine Software“ ist grundsätzlich für jede Software im Informationsverbund durch den Betreiber der kritischen Infrastruktur anzuwenden. Ausgenommen hiervon sind Betriebssysteme, die auf geschlossenen Systemen wie IoT-Geräten, Routern, Druckern oder eingebetteten Systemen ausgeführt werden. Hieraus ableitend ist der Baustein APP.6 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • APP-0001 - Datenbank – Server zentrale Steuerung/Anzeige • APP-0002 - Domain Name Service (DNS) - KRITIS • APP-0003 - Network Time Protocol (NTP) - KRITIS • APP-0004 - Dynamic Host Configuration Protocol (DHCP) - KRITIS • APP-0005 – Verzeichnisdienst

Baustein	Ja	Nein	Begründung
			• APP-0006 - Visualisierung Prozessleitsystem (Server) • APP-0007 - Datenbank vom Prozessleitsystem • APP-0008 - Visualisierung Prozessleitsystem (Client) • APP-0009 - Videomanagement (Client-Anwendung) • APP-0010 - Videomanagement (Server-Anwendung) • APP-0011 – Steuerungssoftware-Server (gemäß MARZ) • APP-0012 - Datenbank von Steuerungssoftware • APP-0013 - Steuerungssoftware-Client (gemäß MARZ) • APP-0014 - Kommunikationsrechner Inselbus (gemäß TLS) • APP-0015 - Streckenstationssoftware (gemäß TLS) • APP-0016 - Office-Anwendung • APP-0017 - Web-Browser
APP.7 Entwicklung von Individualsoftware	**X**		Der Baustein APP.7 „Entwicklung von Individualsoftware“ ist für jede Entwicklung einer Individualsoftware im Informationsverbund durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein APP.7 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • APP-0006 - Visualisierung Prozessleitsystem (Server) • APP-0008 - Visualisierung Prozessleitsystem (Client) • APP-0011 - Steuerungssoftware (gemäß MARZ) • APP-0013 - Steuerungssoftware-Client (gemäß MARZ) • APP-0014 - Kommunikationsrechner Inselbus (gemäß TLS) • APP-0015 - Streckenstationssoftware (gemäß TLS)

Tabelle 26: Modellierung - Schicht APP (Anwendungen)

4.7 Schicht SYS (IT-Systeme)

Baustein	Ja	Nein	Begründung
SYS.1.1 Allgemeiner Server	**X**		Der Baustein SYS.1.1 „Allgemeiner Server“ ist für alle Server im Geltungsbereich unabhängig vom konkreten Betriebssystem durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein SYS.1.1 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • SYS-0011 – Zentrale Services • SYS-0012 – Zentrale Protokollierung • SYS-0013 – Virtualisierungsinfrastruktur • SYS-0014 – Server zentrale Steuerung/Anzeige
SYS.1.2.2 Windows Server 2012	**X**		Der Baustein SYS.1.2.2 „Windows Server 2012“ ist für alle Server im Geltungsbereich anzuwenden, auf denen das Betriebssystem Microsoft Windows Server 2012 R2 durch den Betreiber der kritischen Infrastruktur eingesetzt wird. Hieraus ableitend ist der Baustein SYS.1.2.2 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • SYS-0011 – Zentrale Services • SYS-0012 – Zentrale Protokollierung • SYS-0013 – Virtualisierungsinfrastruktur-SYS-0014 – Server zentrale Steuerung/Anzeige Sollten zusätzlich noch Server unter Windows Server 2016 oder 2019 oder Linux parallel betrieben werden, sind pro Betriebssystem ein eigenständiges Ziel-Objekt zu erstellen.
SYS.1.3 Server unter Linux und Unix	**X**		Der Baustein SYS.1.3 „Server unter Linux und Unix“ ist für alle Server im Geltungsbereich anzuwenden, auf denen eine Variante des Betriebssystemderivates Linux oder Unix durch den Betreiber der kritischen Infrastruktur eingesetzt wird. Hieraus ableitend ist der Baustein SYS.1.3 auf die nachfolgend aufgeführten Zielobjekte anzuwenden:

Baustein	Ja	Nein	Begründung
			• SYS-0011 – Zentrale Services • SYS-0012 – Zentrale Protokollierung • SYS-0013 – Virtualisierungsinfrastruktur • SYS-0014 – Server zentrale Steuerung/Anzeige Sollten zusätzlich noch Server unter Windows Server 2012 R2 oder 2016 oder 2019 parallel betrieben werden, sind pro Betriebssystem ein eigenständiges Ziel-Objekt zu erstellen.
SYS.1.5 Virtualisierung	**X**		Der Baustein SYS.1.5 „Virtualisierung“ ist für alle Virtualisierungsserver im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein SYS.1.5 auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • SYS-0013 – Virtualisierungsinfrastruktur
SYS.1.7 IBM Z-System		**X**	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
SYS.1.8 Speicherlösungen	**X**		Der Baustein SYS.1.8 „Speicherlösung“ ist für alle Speicherlösungen (Network-Attached-Storage-(NAS)-Systeme, Storage-Area-Networks-(SAN)-Systeme, Hybrid Storage, Objekt Storage oder Cloud Storage) im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein SYS.1.8 auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • SYS-0023 – Ringspeicher
SYS.2.1 Allgemeiner Client	**X**		Der Baustein SYS.2.1 „Allgemeiner Client“ ist für alle Clients im Geltungsbereich unabhängig vom konkreten Betriebssystem durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein SYS.2.1 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • SYS-0004 - Operatoren-PC • SYS-0015 – Operatoren-PC/Bedienrechner ZLT

Baustein	Ja	Nein	Begründung
SYS.2.2.2 Clients unter Windows 8.1	X		Insofern der Betreiber von kritischen Infrastrukturen im Geltungsbereich Clients unter Windows 8.1 bis zum 10. Januar 2023 (EoL[1]) betreibt, ist der Baustein SYS.2.2.2 „Clients unter Windows 8.1“ für alle Client-Systeme anzuwenden. Hieraus ableitend ist der Baustein SYS.2.2.3 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • SYS-0004 - Operatoren-PC • SYS-0015 – Operatoren-PC/Bedienrechner ZLT Sollten zusätzlich noch Clients unter Windows 10 oder Linux parallel betrieben werden, ist pro Betriebssystem ein eigenständiges Zielobjekt zu erstellen.
SYS.2.2.3 Clients unter Windows 10	X		Der Baustein SYS.2.2.3 „Clients unter Windows 10“ ist für alle Clients im Geltungsbereich anzuwenden, auf denen das Betriebssystem Microsoft Windows 10 durch den Betreiber der kritischen Infrastruktur eingesetzt wird. Hieraus ableitend ist der Baustein SYS.2.2.3 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • SYS-0004 - Operatoren-PC • SYS-0015 – Operatoren-PC/Bedienrechner ZLT Sollten zusätzlich noch Clients unter Windows 8.1 oder Linux parallel betrieben werden, ist pro Betriebssystem ein eigenständiges Zielobjekt zu erstellen.
SYS.2.3 Clients unter Linux und Unix	X		Der Baustein SYS.2.3 „Clients unter Linux und Unix“ ist für alle Clients im Geltungsbereich des anzuwenden, auf denen Linux bzw. Unix durch den Betreiber der kritischen Infrastruktur eingesetzt wird. Hieraus ableitend ist der Baustein SYS.2. auf die nachfolgend aufgeführten Zielobjekte anzuwenden:

[1] Windows 8.1 - Microsoft Lifecycle | Microsoft Docs

Baustein	Ja	Nein	Begründung
			• SYS-0004 - Operatoren-PC • SYS-0015 – Operatoren-PC/Bedienrechner ZLT Sollten zusätzlich noch Clients unter Windows 8.1 oder 10 parallel betrieben werden, ist pro Betriebssystem ein eigenständiges Zielobjekt zu erstellen.
SYS.2.4 Clients unter macOS		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
SYS.3.1 Laptops		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
SYS.3.2 Tablet und Smartphone		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
SYS.3.2.1 Allgemeine Smartphones und Tablets		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
SYS.3.2.2 Mobile Device Management		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
SYS.3.2.3 iOS (for Enterprise)		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
SYS.3.2.4 Android		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
SYS.3.3 Mobiltelefon		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	X		Der Baustein SYS.4.1 „Drucker, Kopierer und Multifunktionsgeräte“ ist für jeden Drucker, Kopierer oder jedes Multifunktionsgerät immer dann im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein SYS.4.3 auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • SYS-0003 – Drucker

Baustein	Ja	Nein	Begründung
SYS.4.3 Eingebettete Systeme	**X**		Der Baustein SYS.4.3 „Eingebettete Systeme“ ist immer dann im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden, wenn eingebettet Systeme eingesetzt werden. Hieraus ableitend ist der Baustein SYS.4.3 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • NET-0004 – analoges Modem • NET-0005 – xDSL-Modem • IND-0002 – Beleuchtung • IND-0004 – Aktive Leiteinrichtung, Fluchtwegkennzeichnung • SYS-0001 – Kommunikationsrechner Inselbus (KRI) / Portserver Seriell • SYS-0002 – Server Unterzentrale • SYS-0005 – Videowand • SYS-0006 – Console Videowand • SYS-0007 – Elektronische Streckenstation • SYS-0008 – Wechselverkehrszeichen • SYS-0009 – dWista-Anzeigesystem • SYS-0010 – Kamera • SYS-0016 – Brandmeldeanlage (TBG) • SYS-0017 – BOS Notfallbedienkonsole • SYS-0018 – Branderkennung und Brandmeldeanlage (Tunnel) • SYS-0019 – Videoüberwachung • SYS-0020 – Rundfunkversorgung • SYS-0021 – Elektroakustische Anlage • SYS-0022 – Verkehrsbeeinflussung inkl. Tunnelsperranlage
SYS.4.4 Allgemeines IoT-Gerät		**X**	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
SYS.4.5 Wechseldatenträger		**X**	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.

Tabelle 27: Modellierung - Schicht SYS (IT-Systeme)

4.8 Schicht IND (Industrielle IT)

Baustein	Ja	Nein	Begründung
IND.1 Prozessleit- und Automatisierungstechnik	X		Der Baustein IND.1 „Prozessleit- und Automatisierungstechnik“ ist im Geltungsbereich durch den Betreiber der kritischen Infrastruktur auf jedes IT-System mit Prozessleit- und Automatisierungstechnik mindestens einmal anzuwenden. Hieraus ableitend ist der Baustein IND.1 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • IND-0001 – SPS / Automatisierungsebene • IND-0007 – SPS (Pumpensteuerung) • SYS-0022 – Verkehrsbeeinflussung inkl. Tunnelsperranlage
IND.2.1 Allgemeine ICS-Komponente	X		Der Baustein IND.2.1 „Allgemeine ICS-Komponente“ ist auf jede ICS-Komponente im Geltungsbereich durch den Betreiber der kritischen Infrastruktur einmal anzuwenden. Hieraus ableitend ist der Baustein IND.2.1 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • IND-0001 – SPS / Automatisierungsebene • IND-0003 – Lüftung • IND-0005 – Verkehrsdetektion • IND-0006 – Wettersensoren • IND-0007 – SPS (Pumpensteuerung) • IND-0008 – Pumpe (Entwässerung) • SYS-0022 – Verkehrsbeeinflussung inkl. Tunnelsperranlage
IND.2.2 Speicherprogrammierbare Steuerung (SPS)	X		Der Baustein IND.2.2 „Speicherprogrammierbare Steuerung (SPS)“ ist auf jede SPS-Komponente“ im Geltungsbereich durch den Betreiber der kritischen Infrastruktur auf jede Komponente mindestens einmal anzuwenden. Hieraus ableitend ist der Baustein IND.2. auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • IND-0001 – SPS / Automatisierungsebene • IND-0007 – SPS (Pumpensteuerung) • SYS-0022 – Verkehrsbeeinflussung inkl. Tunnelsperranlage

Baustein	Ja	Nein	Begründung
IND.2.3 Sensoren und Aktoren	**X**		Der Baustein IND.2.3 „Sensoren und Aktoren“ ist auf Sensoren und Aktoren im Geltungsbereich durch den Betreiber der kritischen Infrastruktur einmal anzuwenden. Hieraus ableitend ist der Baustein IND.2.3 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • IND-0003 – Lüftung • IND-0005 – Verkehrsdetektoren • IND-0006 – Wettersensoren
IND.2.4 Maschine	**X**		Der Baustein IND.2.4 „Maschine“ ist auf jede Maschine im Geltungsbereich durch den Betreiber der kritischen Infrastruktur einmal anzuwenden. Hieraus ableitend ist der Baustein IND.2.4 auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • IND-0008 – Pumpe (Entwässerung)
IND.2.7 Safety Instrumented Systems		**X**	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.

Tabelle 28: Modellierung - Schicht IND (Industrielle IT)

4.9 Schicht NET (Netze und Kommunikation)

Baustein	Ja	Nein	Begründung
NET.1.1 Netzarchitektur und -design	**X**		Der Baustein NET.1.1 „Netzarchitektur und -design“ ist auf das Gesamtnetz inklusive aller Teilnetze im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden.
NET.1.2 Netzmanagement	**X**		Der Baustein NET.1.2 „Netzmanagement“ ist auf jedes Management-System im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein NET.1.2 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • NET-0001 - CE-Router (Betriebsnetz) • NET-0003 - Switch

Baustein	Ja	Nein	Begründung
NET.2.1 WLAN-Betrieb		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
NET.2.2 WLAN-Nutzung		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
NET.3.1 Router und Switches	X		Der Baustein NET.3.1 „Router und Switches“ ist auf jeden eingesetzten Router und Switch bzw. auf jede Gruppe einmal im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein NET.3.1 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • NET-0001 - CE-Router (Betriebsnetz) • NET-0003 - Switch
NET.3.2 Firewall	X		Der Baustein NET.3.2 „Firewall“ ist auf jede eingesetzte Firewall bzw. auf jede Gruppe (Cluster) im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein NET.3.2 auf das nachfolgend aufgeführte Zielobjekt anzuwenden: • NET-0002 - Firewall
NET.3.3 VPN		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.
NET.4.1 TK-Anlagen		X	Der Baustein NET.4.1 „TK-Anlagen“ ist auf alle Elemente der TK-Anlage im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein NET.4.1 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • NET-0006 – Tunnelnotruf • NET-0007 – BOS-Funk, Betriebsfunk (Tunnel)
NET.4.2 VoIP	X		Der Baustein NET.4.2 „VoIP“ ist auf alle Kommunikationsnetze im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden, in denen VoIP eingesetzt wird. Hieraus ableitend ist der Baustein NET.4.2 auf das nachfolgend aufgeführte Zielobjekt anzuwenden:

Baustein	Ja	Nein	Begründung
			• NET-0007 – BOS-Funk, Betriebsfunk (Tunnel)
NET.4.3 Faxgeräte und Faxserver		X	Dieser Baustein muss im Rahmen der übergreifenden Sicherheitskonzepte der Institution umgesetzt werden.

Tabelle 29: Modellierung - Schicht NET (Netze und Kommunikation)

4.10 Schicht INF (Infrastruktur)

Baustein	Ja	Nein	Begründung
INF.1 Allgemeines Gebäude	X		Der Baustein INF.1 „Allgemeines Gebäude“ ist für jedes Gebäude einmal im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein INF.1 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • INF-0001 - Autobahnmeisterei (AM) / Kabelhaus (KH) / FIT • INF-0002 - Verkehrszentrale (VZ) • INF-0003 - Ersatz-Verkehrszentrale (VZ) • INF-0010 - Tunnelbetriebsgebäude (TBG) • INF-0013 - Tunnel • INF-0014 – Tunnelleitzentrale (TLZ) • INF-0016 – Ersatz-Tunnelleitzentrale (eTLZ) • INF-0018 – Pumpenhaus
INF.2 Rechenzentrum sowie Serverraum	X		Der Baustein INF.2 „Rechenzentrum sowie Serverraum“ ist für jedes Rechenzentrum und jeden Serverraum im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein INF.2 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • INF-0005 - Rechenzentrum/Technikraum (AM/KH) • INF-0009 - Rechenzentrum/Technikraum (VZ) • INF-0012 - Rechenzentrum/Technikraum (TBG)

Baustein	Ja	Nein	Begründung
			• INF-0015 - Rechenzentrum/Technikraum (TLZ)
INF.5 Raum sowie Schrank für technische Infrastruktur	X		Der Baustein INF.5 „Raum sowie Schrank für technische Infrastruktur“ ist für Streckenstationen im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein INF.5 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • INF-0008 - Streckenstation (extern) • INF-0004 – Netzanschlussraum
INF.6 Datenträgerarchiv		X	Ausgehend vom Geltungsbereich ergeben sich für den Betreiber von kritischen Infrastrukturen keine Anforderungen aus den Baustein INF.6 „Datenträgerarchiv“.
INF.7 Büroarbeitsplatz	X		Der Baustein INF.7 „Büroarbeitsplatz“ ist für jeden Rechenzentrum und jeden Serverraum im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein INF.7 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • INF-0006 - Büro Verkehrsmanagement • INF-0007 - Leitstelle • INF-0011 - Lokale Ersatz-Leitstelle • INF-0017 – Büro Disponent • INF-0019 – Büro Tunnelmanagement
INF.8 Häuslicher Arbeitsplatz		X	Ausgehend vom Geltungsbereich ergeben sich für den Betreiber von kritischen Infrastrukturen keine Anforderungen aus den Baustein INF.8 „Häuslicher Arbeitsplatz“.
INF.9 Mobiler Arbeitsplatz		X	Ausgehend vom Geltungsbereich ergeben sich für den Betreiber von kritischen Infrastrukturen keine Anforderungen aus den Baustein INF.9 „Mobiler Arbeitsplatz“.
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume		X	Ausgehend vom Geltungsbereich ergeben sich für den Betreiber von kritischen Infrastrukturen keine Anforderungen aus den Baustein INF.10

Baustein	Ja	Nein	Begründung
			„Besprechungs-, Veranstaltungs- und Schulungsräume“.
INF.11 Allgemeines Fahrzeug		X	Dieser Baustein ist auf den beschriebenen Geltungsbereich nicht anwendbar.
INF.12 Verkabelung	X		Der Baustein INF.12 „Verkabelung“ ist einmal auf die IT- und elektronische Verkabelung in jedem Gebäude und Raum im Geltungsbereich durch den Betreiber der kritischen Infrastruktur anzuwenden. Hieraus ableitend ist der Baustein INF.12 auf die nachfolgend aufgeführten Zielobjekte anzuwenden: • INF-0001 - Autobahnmeisterei (AM) / Kabelhaus (KH) / FIT • INF-0002 - Verkehrszentrale (VZ) • INF-0003 - Ersatz-Verkehrszentrale (VZ) • INF-0004 - Netzanschlussraum • INF-0005 - Rechenzentrum/Technikraum (AM/KH) • INF-0006 - Büro Verkehrsmanagement • INF-0007 - Leitstelle • INF-0008 - Streckenstation (extern) • INF-0009 - Rechenzentrum/Technikraum (VZ) • INF-0010 - Tunnelbetriebsgebäude (TBG) • INF-0011 - Lokale Ersatz-Leitstelle • INF-0012 - Rechenzentrum/Technikraum (TBG) • INF-0013 - Tunnel • INF-0014 – Tunnelleitzentrale (TLZ) • INF-0015 - Rechenzentrum/Technikraum (TLZ) • INF-0016 – Ersatz-Tunnelleitzentrale (eTLZ) • INF-0017 – Büro Disponent • INF-0018 – Pumpenhaus • INF-0019 – Büro Tunnelmanagement

Tabelle 30: Modellierung - Schicht INF (Infrastruktur)

5. IT-Grundschutz-Check

5.1 Durchführung

Im IT-Grundschutz-Check wird zu allen modellierten IT-Grundschutz-Bausteinen beschrieben, wie die dort enthaltenen Sicherheitsanforderungen unter Berücksichtigung des Schutzbedarfes erfüllt werden.

Zu jeder Anforderung wird dabei erhoben, ob diese durch die vorhandene Realisierung vollständig („ja“), in Teilen („teilweise“) oder nicht („nein“) erfüllt wird, oder ob die Anforderung auf den betrachteten Informationsverbund aus bestimmten Gründen nicht anwendbar ist („entbehrlich“). Durch die Identifizierung von noch nicht oder nur teilweise erfüllten Anforderungen werden Verbesserungsmöglichkeiten aufgezeigt.

5.2 Ergebnisse

Im Rahmen der Risikoanalyse werden ebenfalls die noch nicht vollständig bzw. noch nicht umgesetzten internen Anforderungen der Institution und den modellierten Bausteinen und dessen Vorgaben aus dem BSI IT-Grundschutz-Kompendium mit einbezogen.

6. Risikoanalyse

Die Risikoanalyse in diesem IT-Sicherheitskonzept erfolgt für den Informationsverbund nach dem BSI-Standard 200-3 (siehe 8.3, Buchstabe d) und beachtet zusätzlich die Anforderungen der KritisV hinsichtlich der zur Verfügung stehenden Risikobehandlungsoptionen.

Grundlage für die Risikoanalyse ist der Katalog „Elementare Gefährdungen“ aus dem IT-Grundschutz-Kompendium. Dazu wurden die für die betrachtete Anwendung relevanten Gefährdungen aus dem Katalog ausgewählt und für den Anwendungsfall konkretisiert. In der Konkretisierung können aus einer elementaren Gefährdung auch mehrere konkrete Gefährdungen abgeleitet werden.

Die Betrachtung zu jeder einzelnen Gefährdung erfolgt entsprechend den nachfolgend aufgeführten Kriterien

1. eine Beschreibung der konkreten Gefährdung
2. eine Bewertung der Eintrittswahrscheinlichkeit
3. eine Bewertung der Auswirkungen
4. eine Bewertung des Risikos
5. eine Beschreibung des verbleibenden Risikos
6. Benennung/Beschreibung von mitigierenden Maßnahmen

Für die meisten IT-bezogenen Risiken ist eine genauere Bewertung in der Praxis ohnehin mit sehr großen Unsicherheiten verbunden. Der Betreiber muss die Bewertungsskalen auf die eigenen Gegebenheiten anpassen. Diese sind:

Bewertung von Eintrittswahrscheinlichkeiten	**Bedeutung**
selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal im Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Tabelle 31: Risikoanalyse - Bewertung von Eintrittswahrscheinlichkeiten

Bewertung von Auswirkungen	**Bedeutung**
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.

existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 32: Risikoanalyse - Bewertung von Auswirkungen

Bewertung von Risiken	**Bedeutung**
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.

Tabelle 33: Risikoanalyse - Bewertung von Risiken

7. Anwendungshinweise für dieses IT-Grundschutz-Profil

Die hier aufgeführten Anwendungshinweise beschreiben, wie mit den aufgezeigten Anforderungen und Schutzbedarfen innerhalb des Managementsystems für Informationssicherheit (ISMS) umgegangen werden kann.

In Kapitel 3 ist die Schutzbedarfserhebung auf Basis der Geschäftsprozesse beschrieben. Die Vererbung zur Ableitung des Schutzbedarfs erfolgt im IT-Grundschutz-Profil nach dem Maximumprinzip und bezieht sich deshalb immer auf die gesamte Organisation und nicht auf Teilbereiche oder Regionen. Am Beispiel der Infrastruktur Tunnelleitzentrale bezieht sich der festgelegte Schutzbedarf deshalb auf die Gesamtheit aller Tunnelleitzentralen. Zudem gibt es verschiedene Ausprägungen von Tunnel, welche wieder Auswirkungen auf den Schutzbedarf der einzelnen TLZ hat, über welche diese Tunnel gesteuert werden. Aus diesem Grund ist die Wahl einer niedrigeren Schutzbedarfskategorie für eine einzelne TLZ durchaus möglich. Diese muss dann entsprechend begründet werden. Zudem können auch die anderen Vererbungsregeln angewendet werden.

Das IT-Grundschutz-Profil ist eine Empfehlung seitens des Bundesamtes für Sicherheit in der Informationstechnik sowie des Autors und muss deshalb nicht zwingend verwendet werden. Jedem Betreiber einer Bundesautobahn ist es freigestellt, ob er das Profil anwendet.

8. Unterstützende Informationen

Hier werden Autobahnspezifische Regelungen aufgeführt, die direkten Einfluss auf das IT-Grundschutz-Profil haben.

Allerdings wird auf eine abschließende Aufzählung allgemein anerkannter und gültiger Normen und DIN verzichtet.

8.1 Technische Standards im Bereich betriebs- und verkehrstechnische Tunnelausstattung:

a) Empfehlungen für die Ausstattung und den Betrieb von Straßentunneln (EABT)
Grundlage für das (Verkehrs-)Sicherheitsniveau von Tunneln sind die in der Bundesrepublik Deutschland geltenden „Empfehlungen für die Ausstattung und den Betrieb von Straßentunneln“ (EABT). Diese Empfehlungen beinhalten wesentliche Anforderungen an Anlagen und IT-Systeme. Die EABT-80/100, Ausgabe 2019 repräsentieren den aktuellen Stand der Technik.
Herausgeber: Forschungsgesellschaft für Strassen- und Verkehrswesen, Version EABT-80/100, Ausgabe 2019
ISBN: 978-3-86446-235-1

b) Richtlinien für die Ausstattung und den Betrieb von Straßentunneln (RABT)
Die „Richtlinien für die Ausstattung und den Betrieb von Straßentunneln (RABT)“ sind mit der Ausgabe 2006 durch ein Allgemeines Rundschreiben des BMVBS für die Bundesfernstraßen eingeführt. Ihre Anwendung ist damit rechtlich bindend.
Herausgeber: Forschungsgesellschaft für Strassen- und Verkehrswesen, Ausgabe 2006
ISBN: 3-937356-87-8

8.2 Technische Standards im Bereich Verkehrssteuerungs- und –leittechnik:

a) Technische Lieferbedingungen für Streckenstationen, Version 2012 (TLS)
Die „Technischen Lieferbedingungen für Streckenstationen (TLS)“ beschreiben den strukturellen bzw. hierarchischen Aufbau des Gesamtsystems von verkehrstelematischen Einrichtungen. Sie regeln weiterhin die Datenübertragung zwischen den einzelnen Systemkomponenten bzw. Systemebenen. In den TLS sind damit die Kommunikationsinhalte als auch die anzuwendenden Protokolle (TC57 und TCP/IP) festgelegt. Die TLS 2012 sind durch ein Allgemeines Rundschreiben des BMVBS/BMVI zur verbindlichen Anwendung im Bereich der Bundesfernstraßen eingeführt.
Herausgeber: Bundesministerium für Verkehr, Bau und Stadtentwicklung, heute BMVI Download über die Seiten der Bundesanstalt im Strassenwesen (BaSt):
BASt - Fachthemen – Verkehrstechnik - TLS 2012, zuletzt aufgerufen am 08.12.2021

b) Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen, Version 2018 (MARZ)
Im „Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen (MARZ)“ sind die notwendigen Festlegungen für Unterzentralen und Verkehrsrechnerzentralen für Bundesfernstraßen enthalten:
- Aufgaben der Zentralen,
- Beschreibung der verkehrstechnischen Anforderungen,

- Systemarchitekturentwurf aus fachlicher Sicht sowie grundsätzliche funktionale und nichtfunktionale Anforderungen an Hard- und Software,
- Art der Kommunikation innerhalb des VRZ-/UZ-Systems sowie zwischen Zentralen und mit Dritten.

Herausgeber: Bundesministerium für Verkehr, Bau und Stadtentwicklung, heute BMVI, Download über die Seiten der Bundesanstalt im Strassenwesen (BaSt): BASt - Publikationen - Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen MARZ 2018, zuletzt aufgerufen am 08.12.2021
Das MARZ 2018 ist im Bereich der Bundesfernstraßen verbindlich anzuwenden.

8.3 Dokumente des Bundesamt für Sicherheit in der Informationstechnik

a) IT-Grundschutz-Profile – Strukturbeschreibung –, Version 1.0, 28.09.2018
b) Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 200-1, Version 1.0, Oktober 2017
c) IT-Grundschutz-Methodik, BSI-Standard 200-2, Version 1.0, Oktober 2017
d) Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 200-3, Version 1.0, Oktober 2017
e) Notfallmanagement, BSI-Standard 100-4, Version 1.0, November 2008
f) IT-Grundschutz-Kompendium 2021, Stand Februar 2021

8.4 Gesetze, Verordnungen – jeweils in der zum Zeitpunkt der Erstellung des IT-Grundschutz-Profils geltenden Fassung

a) Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)
   BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert
b) Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)
   BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), zuletzt durch Artikel 1 der Verordnung vom 6. September 2021 (BGBl. I S. 4163) geändert