



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

**Bundesamt für Strassen ASTRA**

## **RICHTLINIE**

# **SYSTEMARCHITEKTUR LEIT- UND STEUERSYSTEME DER BETRIEBS- UND SICHERHEITSAUSRÜSTUNGEN**

---

*Ausgabe 2025 V2.10*  
*ASTRA 13031*

# Impressum

## Autoren

|                  |                           |
|------------------|---------------------------|
| Geringer Jolanda | ASTRA DS-DTI              |
| Crausaz Bernard  | ASTRA DS-UARS             |
| Gähwiler Daniel  | CSI Consulting AG, Zürich |
| Indergand Stefan | GEXI                      |

## Begleitgruppe

|                  |               |
|------------------|---------------|
| Pfammatter Mario | ASTRA DS-UARS |
| Claude Stéphane  | ASTRA DS-DTI  |
| Paolo Maltese    | ASTRA N-VIM   |
| Demont Olivier   | ASTRA I-FU    |
| Kundert Renato   | ASTRA I-FU    |
| Berger Markus    | ASTRA I-FU    |
| Wyss Martin      | ASTRA I-B     |
| Bregy Valentin   | ASTRA I-F2    |

## Originalsprache

Deutsch

## Herausgeber

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

## Bezugsquelle

Das Dokument kann kostenlos von [www.astra.admin.ch](http://www.astra.admin.ch) heruntergeladen werden.

© ASTRA 2025

Abdruck - ausser für kommerzielle Nutzung - unter Angabe der Quelle gestattet.

## Vorwort

Die Betriebs- und Sicherheitsausrüstungen (BSA) tragen einen erheblichen Teil zur Sicherheit der Tunnel und offenen Strecken des schweizerischen Nationalstrassennetzes bei. Die BSA mit seinen OT (Operational Technology) Systemen stellt den sicheren und rund um die Uhr überwachten Betrieb sicher.

Auch im Verkehrsmanagement spielen die BSA eine wichtige Rolle bei der Gewährleistung eines möglichst gleichmässigen und störungsfreien Verkehrsflusses.

Die vorliegende Richtlinie beschreibt eine schweizweit einheitliche und durchgängige Struktur der BSA-Leittechnik. Sie bildet eine tragfähige und modulare Basis, welche es dem ASTRA ermöglicht, die BSA weiter auszubauen, aber auch neue Lösungen im Bereich Verkehrsmanagement oder Vernetzung der Fahrzeuge mit der Infrastruktur zu realisieren.

### **Bundesamt für Strassen**

Jürg Röthlisberger  
Direktor



# Inhaltsverzeichnis

|   |           |
|---|-----------|
| <b>Impressum .....</b>  | <b>2</b>  |
| <b>Vorwort.....</b>   | <b>3</b>  |
| <b>Abbildungsverzeichnis.....</b>   | <b>9</b>  |
| <b>Tabellenverzeichnis .....</b>  | <b>10</b> |
| <br>  |           |
| <b>1      Einleitung .....</b>  | <b>11</b> |
| 1.1    Zweck der Richtlinie .....   | 11        |
| 1.2    Geltungsbereich .....  | 11        |
| 1.3    Adressaten .....   | 11        |
| 1.4    Inkrafttreten und Änderungen .....   | 11        |
| <br>  |           |
| <b>2      Architekturgrundsätze.....</b>  | <b>12</b> |
| 2.1    Zielbild Leit- und Steuersysteme .....   | 12        |
| 2.2    Produktions-, Integrations-, Test- und Schulungsumgebung.....                      | 12        |
| 2.3    Grundstruktur Systemarchitektur .....  | 14        |
| 2.3.1    IP-Netz BSA (Kommunikationsnetzwerk) .....                                       | 14        |
| 2.3.2    Managementebene .....  | 15        |
| 2.3.3    Basisdienste / Zentrale Dienste .....  | 15        |
| 2.3.4    Verkehrsmanagementebene Schweiz .....  | 15        |
| 2.3.5    Verkehrsregion .....   | 15        |
| 2.3.6    Regionale Managementebene .....  | 16        |
| 2.3.7    BSA-Abschnitt / IP-Abschnitt.....  | 16        |
| 2.3.8    Systeme Bund, Drittsysteme und Sonderanlagen .....                               | 19        |
| 2.4    Wirkungsperimeter .....  | 20        |
| <br>  |           |
| <b>3      Architektur SA-CH.....</b>  | <b>21</b> |
| 3.1    Managementebene .....  | 21        |
| 3.1.1    Applikationsebene .....  | 21        |
| 3.1.2    Fachdienstebene.....   | 22        |
| 3.1.3    BSA Datawarehouse (DWH).....   | 23        |
| 3.2    Basisdienstebene / Zentrale Dienste .....  | 23        |
| 3.2.1    OT-Management .....  | 24        |
| 3.2.2    OT-Dienste .....   | 26        |
| 3.3    Verkehrsmanagementebene Schweiz .....  | 27        |
| 3.4    Verkehrsregionen .....   | 28        |
| 3.4.1    Streckenbasiert bis schweizweite Verkehrslenkung .....                           | 29        |
| 3.4.2    Beispiel von streckenbasiertem Verkehrsmanagement.....                           | 29        |
| 3.4.3    Streckenbasierte Architekturelemente der spezifischen Verkehrsmanagementsicht .. | 31        |
| 3.5    Regionale Managementebene GE.....  | 32        |
| 3.5.1    Verkehrsinformationssystem (VIS).....  | 32        |
| 3.5.2    Regionale Verkehrsdatenerfassung (rvDE).....                                     | 32        |
| 3.5.3    UeLS-CH .....  | 32        |
| 3.5.4    Meteouberwachungs und -warnsystem (GFS) .....                                    | 32        |
| 3.5.5    Videosystem.....   | 32        |
| 3.5.6    Operatoren Arbeitsplätze .....   | 33        |
| 3.5.7    Technische Betriebstools .....   | 33        |
| 3.5.8    Notruftelefonanlage (NT).....  | 33        |
| 3.5.9    Weitere Systeme .....  | 33        |
| 3.5.10    Sub-Domänendienste / IAM BSA.....   | 33        |
| 3.5.11    DD(I).....  | 33        |
| 3.5.12    Remote Zugang (OT-Notsysteme).....  | 33        |
| 3.6    BSA-Abschnitt .....  | 33        |
| 3.6.1    Abschnittsrechner (AR) .....   | 33        |
| 3.6.2    Anlage- und Lokalsteuerung .....   | 34        |
| 3.6.3    Aktoren und Sensoren .....   | 35        |
| 3.7    Bundessysteme.....   | 35        |

|          |  |           |
|----------|--|-----------|
| 3.8      | Drittsysteme .....   | 35        |
| 3.9      | Sonderanlagen .....  | 35        |
| <b>4</b> | <b>Leistungsanforderungen .....</b>  | <b>36</b> |
| 4.1      | Einsatz der Virtualisierung .....  | 36        |
| 4.1.1    | OT-Technikraum .....   | 36        |
| 4.1.2    | Technikräume/Technische Zentralen .....  | 36        |
| 4.2      | Betriebssysteme und Redundanzen .....  | 37        |
| 4.2.1    | Betriebssysteme und Virtualisierungsplattform .....  | 37        |
| 4.2.2    | Redundante AR .....  | 37        |
| 4.2.3    | AS in redundanter Ausführung .....   | 38        |
| 4.3      | Virtualisierungsanwendung .....  | 38        |
| 4.3.1    | Autonomie und Rückfallebenen .....   | 38        |
| 4.3.2    | Virtualisierung der Leit- und Steuersysteme .....  | 39        |
| 4.3.3    | Darstellung der AR-Virtualisierung (Zielfokus) .....   | 39        |
| 4.3.4    | UeLS-CH (BL) im OT-Technikraum .....   | 41        |
| 4.4      | Aufbau des AR (einzelner Rechner als Beispiel) .....   | 42        |
| 4.4.1    | WEB-Browser Kompatibilität für GUI-MMI .....   | 43        |
| 4.5      | Aufbau der AS .....  | 43        |
| 4.5.1    | Sicherheitskritische AS (inkl. LS) .....   | 43        |
| 4.5.2    | Anforderungen an AS (SPS) .....  | 43        |
| 4.5.3    | SPS .....  | 44        |
| 4.5.4    | Virtuelle SPS .....  | 44        |
| 4.5.5    | IPC .....  | 44        |
| 4.5.6    | MMI (GUI) .....  | 45        |
| 4.6      | Aufbau der LS .....  | 45        |
| 4.6.1    | Anforderungen an LS .....  | 45        |
| 4.7      | Lizenzen .....   | 45        |
| 4.7.1    | Lizenzen ohne Hardwarebindung .....  | 45        |
| 4.8      | Verfügbarkeit der Elemente .....   | 45        |
| 4.8.1    | Servicezeit .....  | 45        |
| 4.8.2    | Supportzeit .....  | 46        |
| 4.8.3    | Verfügbarkeit .....  | 46        |
| 4.9      | Anlagespezifische Anwendung der Technologien .....   | 48        |
| 4.9.1    | Einsatz Verfügbarkeitsfunktionen im OT-Technikraum .....   | 48        |
| 4.9.2    | Einsatz Verfügbarkeitsfunktionen AR .....  | 49        |
| 4.9.3    | Einsatz Verfügbarkeitsfunktionen AS/LS .....   | 49        |
| 4.10     | Konsolidierung der unterschiedlichen Anlagefunktionen auf der<br>Virtualisierungsplattform ..... | 50        |
| 4.10.1   | OT-Technikraum (zwei Standorte pro GE in einem oder zwei dedizierten IP-<br>Abschnitten) .....   | 50        |
| 4.10.2   | Technikräume (zwei Standorte innerhalb des IP-Abschnitts) .....                                  | 50        |
| 4.10.3   | Anforderungen Wartung- und Supportgewährleistung (SLA) .....                                     | 51        |
| 4.11     | Datenhaltung .....   | 51        |
| 4.11.1   | Eigentums- und Nutzungsrecht .....   | 52        |
| 4.11.2   | Software und Anwendungsprogramm .....  | 52        |
| 4.12     | Nachvollziehbarkeit .....  | 52        |
| 4.12.1   | Logging .....  | 52        |
| 4.12.2   | System Protokollierung .....   | 53        |
| 4.12.3   | Datenhierarchie und -aggregation .....   | 53        |
| 4.12.4   | Archivierung .....   | 53        |
| 4.12.5   | Backup und Recovery .....  | 54        |
| 4.13     | Zeitsynchronisation .....  | 54        |
| 4.14     | Reporting .....  | 54        |
| 4.15     | OT Security .....  | 54        |
| 4.15.1   | Weisungen 73006 .....  | 54        |
| 4.15.2   | Richtlinie 13030 .....   | 55        |
| 4.15.3   | Dokumentation 83042 .....  | 55        |
| 4.15.4   | Dokumentation 83056 .....  | 55        |
| 4.15.5   | Fachhandbuch 23001-11880 physische OT Security und Richtlinie 13009 .....                        | 55        |

|          |   |            |
|----------|---|------------|
| <b>5</b> | <b>Funktionale Anforderungen .....</b>  | <b>56</b>  |
| 5.1      | Zugriff .....   | 56         |
| 5.1.1    | Nutzergruppen.....  | 56         |
| 5.1.2    | Benutzerrollen .....  | 56         |
| 5.2      | Benutzerschnittstellen .....  | 56         |
| 5.2.1    | Visualisierungsprinzip .....  | 56         |
| 5.2.2    | Bedienmöglichkeiten .....   | 58         |
| 5.2.3    | Benutzeroberflächen .....   | 59         |
| 5.3      | Steuerung.....  | 59         |
| 5.3.1    | Betriebsarten .....   | 59         |
| 5.3.2    | Steuerungsarten.....  | 61         |
| 5.3.3    | Funktionen.....   | 62         |
| 5.4      | Monitoring.....   | 63         |
| 5.5      | Reporting.....  | 63         |
| 5.6      | Rückfallebene.....  | 64         |
| 5.7      | Betriebsrelevante WEB-Links .....   | 65         |
| 5.8      | Autonomie .....   | 65         |
| 5.8.1    | Anlagefunktion in Bezug auf das Betriebsszenario .....                        | 65         |
| 5.8.2    | Betriebsszenarien in Bezug auf die Abschnittsautonomie .....                  | 66         |
| 5.8.3    | Normalbetrieb.....  | 66         |
| 5.8.4    | Eingeschränkter Betrieb .....   | 66         |
| 5.8.5    | Notbetrieb.....   | 67         |
| 5.8.6    | Kein Betrieb.....   | 67         |
| 5.8.7    | Übersicht Betriebsszenarien .....   | 67         |
| 5.8.8    | Anwendbarkeit.....  | 68         |
| 5.9      | IP-Netz BSA .....   | 68         |
| 5.10     | Kommunikationsgrundsätze.....   | 68         |
| 5.10.1   | Grundsätze und Anforderungen.....   | 68         |
| 5.10.2   | Protokolle .....  | 69         |
| 5.11     | Datenmodell und Datenpunkte.....  | 69         |
| 5.12     | Datenaustausch .....  | 69         |
| 5.12.1   | UeLS-CH.....  | 69         |
| 5.12.2   | Abschnittsrechner .....   | 70         |
| 5.12.3   | Anlagen- / Lokalsteuerung .....   | 70         |
| 5.13     | Reflexe .....   | 71         |
| 5.13.1   | Art der Reflexe .....   | 71         |
| 5.13.2   | Reflex Typen .....  | 71         |
| 5.13.3   | Zielarchitektur.....  | 72         |
| 5.14     | Zugangsportale OT/BSA und Remote Zugang (OT-Notsysteme) .....                 | 73         |
| 5.15     | Anbindung von Umsysteme .....   | 73         |
| 5.16     | Mobile Kommunikation .....  | 73         |
| <b>6</b> | <b>Migration .....</b>  | <b>74</b>  |
| 6.1      | Organisatorische Anpassungen Geschäfts- und Betriebsorganisation BSA-OT ..... | 74         |
| 6.2      | Generelles zum Migrationskonzept.....   | 74         |
| 6.3      | Kommunikation und Leittechnik .....   | 74         |
| 6.3.1    | Leittechnik (UeLS-CH und Systemintegration) .....                             | 75         |
| 6.4      | Verkehrsmanagementsysteme .....   | 76         |
| 6.4.1    | Vehicle-by-Vehicle System (VBV).....  | 76         |
| 6.4.2    | Verkehrsinformationssystem (VIS).....   | 76         |
| 6.4.3    | Regionale Verkehrlenkung (rVL).....   | 76         |
| 6.4.4    | Regionale Verkehrsdatenerfassung (rvDE).....                                  | 76         |
| 6.4.5    | Regionale Verkehrsrechner (VR).....   | 76         |
|          | <b>Anhänge .....</b>  | <b>77</b>  |
|          | <b>Glossar .....</b>  | <b>97</b>  |
|          | <b>Literaturverzeichnis .....</b>   | <b>103</b> |
|          | <b>Auflistung der Änderungen.....</b>   | <b>105</b> |





# Abbildungsverzeichnis

|   |    |
|---|----|
| Abbildung 1: Grundstruktur der Architektur .....  | 14 |
| Abbildung 2: Übersicht IP-Netz BSA mit den zwei Standorten Basisdienst A und B und den beiden abzulösenden Standorten RZ BSA A und B (ABX) .....  | 15 |
| Abbildung 3: Räumliche Ausdehnung der Architekturelemente (logische Darstellung) .....  | 16 |
| Abbildung 4: Räumliche Ausdehnung der spezifischen Verkehrsmanagement-Architekturelemente (logische Darstellung) .....                            | 18 |
| Abbildung 5: Übersicht Systeme Bund und Drittsysteme .....  | 19 |
| Abbildung 6: Applikationsebene .....  | 21 |
| Abbildung 7: Fachdienstebene .....  | 22 |
| Abbildung 8: OT-Management .....  | 24 |
| Abbildung 9: OT-Dienste .....   | 26 |
| Abbildung 10: Verkehrsmanagementebene Schweiz .....   | 27 |
| Abbildung 11: Wirkungssperimeter der FA VL-CH .....   | 29 |
| Abbildung 12: Streckenbasiertes Verkehrsmanagement .....  | 29 |
| Abbildung 13: Beispiel «Dedizierte Anlagen» und «Kombinierte Anlagen» .....   | 31 |
| Abbildung 14: Beispiel GHGW mit «Dedizierte Anlagen» und «Kombinierte Anlagen» .....  | 31 |
| Abbildung 15: Regionale Managementebene Gebietseinheiten .....  | 32 |
| Abbildung 16: OT-Technikraum .....  | 36 |
| Abbildung 17: Technikraum/Technische Zentrale .....   | 37 |
| Abbildung 18: Darstellung Zielfokus AR Virtualisierung - AR , AR MMI und AS MMI auf VM getrennt .....   | 39 |
| Abbildung 19: Darstellung Zielfokus AR Virtualisierung AR und AR MMI auf gemeinsamer VM .....   | 40 |
| Abbildung 20: Variante 1 Darstellung für nicht virtualisierten AR (in Ausnahmefällen) .....   | 40 |
| Abbildung 21: Variante 2 Zugriffselemente sind herstellersistezifisch und funktionsgebunden .....   | 41 |
| Abbildung 22: Grundaufbau eines AR Host: Trennung der Funktionen der VMs Variante 1 .....   | 42 |
| Abbildung 23: Grundaufbau eines AR Host: Trennung der Funktionen der VMs Variante 2 .....   | 43 |
| Abbildung 24: Darstellung der Technologieanwendung (einer Röhre) .....  | 50 |
| Abbildung 25: Datenpyramide .....   | 53 |
| Abbildung 26: Prinzip der mehrschichtigen Security-Anforderungen / Massnahmen – «Defense-in-Depth»-Prinzip .....                                  | 55 |
| Abbildung 27: Visualisierungsprinzipien .....   | 57 |
| Abbildung 28: Rückfallebenen SA-CH .....  | 64 |
| Abbildung 29: UeLS-CH-Datenaustausch .....  | 70 |
| Abbildung 30: AR-Datenaustausch .....   | 70 |
| Abbildung 31: AS/LS – Datenaustausch .....  | 71 |
| Abbildung 32: Reflex Typ 1 .....  | 72 |
| Abbildung 33: Reflex Typ 2 .....  | 73 |
| Abbildung 34: Umsetzungsvarianten Leittechnik (UeLS-CH und Systemintegration) wobei neu = SA-CH-konform und bestehend = nicht SA-CH-konform ..... | 75 |

## Tabellenverzeichnis

|  |    |
|--|----|
| Tabelle 1: Räumliche Ausdehnung Verkehrsmanagement .....                         | 17 |
| Tabelle 2: Wirkungssperimeter aus Nutzersicht.....                               | 20 |
| Tabelle 3: Wirkungssperimeter Systemsicht .....                                  | 20 |
| Tabelle 4: Einsatz der Virtualisierung in den Systemebenen der Architektur ..... | 39 |
| Tabelle 5: Service Level Servicezeit.....  | 45 |
| Tabelle 6: Service Level Supportzeiten .....                                     | 46 |
| Tabelle 7: Service Level gemessen in Downtime.....                               | 46 |
| Tabelle 8: Standardverfügbarkeit gemessen in Downtime.....                       | 47 |
| Tabelle 9: Teilanlagen und deren Teilfunktionen .....                            | 48 |
| Tabelle 10: Übersicht Virtualisierung der Teilanlage.....                        | 48 |
| Tabelle 11: Life-Cycle von «nicht Personendaten».....                            | 52 |
| Tabelle 12: Visualisierungsprinzipien .....                                      | 57 |
| Tabelle 13: Bedienmöglichkeiten.....   | 58 |
| Tabelle 14: Betriebsarten .....  | 59 |
| Tabelle 15: Betriebsarten ebenenspezifisch .....                                 | 60 |
| Tabelle 16: BSA-Anlagen & VM-Anlagen.....  | 60 |
| Tabelle 17: Steuerungsarten .....  | 61 |
| Tabelle 18: Teilanlagen für minimalen sicheren Betrieb .....                     | 65 |
| Tabelle 19: Übersicht der Betriebsszenarien .....                                | 67 |
| Tabelle 20: Übersicht zur Anwendbarkeit in Abhängigkeit der Tunnelkategorie..... | 68 |

# 1 Einleitung

## 1.1 Zweck der Richtlinie

Diese Richtlinie standardisiert den Aufbau der Leittechnik von Betriebs- und Sicherheitsausrüstungen (BSA) und deren OT-Systemen für die Nationalstrassen und definiert Vorgaben für deren Planung, Projektierung und Realisierung.

Es wird die Ausprägung der Leit- und Steuersysteme und der Schnittstellen beschrieben.

Es werden grundsätzlich die Funktionen, nicht die Hardware, beschrieben. Es wird explizit erwähnt, was nicht zugelassen ist, ansonsten wird der Rahmen, in welchem man sich bewegen kann, beschrieben.

## 1.2 Geltungsbereich

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

## 1.3 Adressaten

Diese Richtlinie richtet sich an alle internen und externen Personen, welche sich mit OT-Systemen und BSA sowohl in der Projektierung als auch im Betrieb befassen.

Die Richtlinie wendet sich an:

- Projektleiter des ASTRA (bei Projekten mit Steuer- und Leittechnik);
- Planer und Unternehmungen, die im Auftrag des ASTRA Tätigkeiten an den OT (Operational Technology) /BSA ausführen;
- Fachspezialisten und Erhaltungsplaner BSA des ASTRA;
- Projektleiter SA-CH des ASTRA;
- Fachspezialisten OT/BSA der Gebietseinheiten.
- Und alle weiteren Stakeholder der Geschäfts- und Betriebsorganisation OT-BSA (GBO)

## 1.4 Inkrafttreten und Änderungen

Die Richtlinie tritt am 16.12.2025 in Kraft. Die «Auflistung der Änderungen» ist auf Seite 105 zu finden.

## 2 Architekturgrundsätze

Die Systemarchitektur Schweiz beschreibt die Leit- und Steuersysteme der Nationalstrassen. Sie stellt ein Modell dar, das den Zusammenhang und die Eigenschaften der verschiedenen Elemente und ihrer Funktionen beschreibt. Weiter werden die unmittelbaren Bundessysteme, Drittsysteme und Sonderanlagen beschrieben.

Dieses Kapitel behandelt die Ziele der Systemarchitektur Schweiz (SA-CH) sowie die zugehörigen allgemeinen Anforderungen. Darüber hinaus wird ein Gesamtüberblick über die Systemarchitektur gegeben. Eine detaillierte Beschreibung der Ebenen erfolgt im Kapitel 3.

### 2.1 Zielbild Leit- und Steuersysteme

Für die Systemarchitektur wird folgender Zielzustand angestrebt:

- Eine homogene, modulare und erweiterbare Architektur;
- Die Autonomie der Regionen, Objekte als auch Anlagen;
- Die Standardisierung der Anforderungen und Schnittstellen zwischen den Systemen;
- Eine Herstellerunabhängigkeit;
- Die Bereitschaft der Architektur zur Implementierung neuer Technologien;
- Eine Steigerung der Effizienz der Leistungen.

Die nachfolgenden Rahmenbedingungen sind einzuhalten:

- Die schweizweite Konnektivität ist über ein einheitliches technisches Netzwerk (IP-Netz BSA) gewährleistet;
- Die Leit- und Steuersysteme der BSA werden schweizweit homogen gestaltet, d.h. deren Aufbau und insbesondere deren Schnittstellen richten sich nach einheitlichen Vorgaben;
- Umsysteme Dritter (ausserhalb des Gültigkeitsbereichs der Systemarchitektur) sind über standardisierte Schnittstellen angebunden;
- Die Systemarchitektur ist offen für die Einbindung zusätzlicher Systeme und den Einsatz neuer Technologien;
- Services werden zentral zur Verfügung gestellt oder es erfolgen klare funktionale Vorgaben zur Bereitstellung der dezentralen Services;
- Die Kommunikation zwischen den Ebenen erfolgt gemäss Vorgaben der OT-Security und der Network Security Policy;
- Für Verkehrsmanagement-Anlagen und das Verkehrsmonitoring gelten die fachlichen Ziele der Richtlinie 15003 sowie 15007.

### 2.2 Produktions-, Integrations-, Test- und Schulungsumgebung

Es ist bei Bedarf eine Produktions-, Integrations-, Test- und Schulungsumgebung für die regionale Managementebene, die Basisdienste als auch für die Managementebene einzurichten. Dieser Entscheid wird im jeweiligen Projekt gefällt und ist in den Projektunterlagen (Hermes: PA, SIA: MP/DP) auszuweisen.

Die Schulungsumgebung kann als Simulation bereitgestellt werden. In dieser Umgebung muss die volle Funktionalität der Fachanwendungen verfügbar sein. Deren Bedienung darf keine Auswirkungen auf die Anlagen haben.

Bei schweizweit einheitlichen Systemen reichen eine Testumgebung und eine Schulungsumgebung aus (auch wenn sie an unterschiedlichen Standorten installiert sind).

Für die Anlagen- und Steuerungsebene der BSA sind integrative Tests in der Integrationsumgebung, sowie in der Produktionsumgebung durchzuführen. Es handelt sich gemäss Richtlinie 13028 um Anlagentests mit allen betroffenen Schnittstellen.

Die Testprotokolle müssen projektspezifisch für jedes Projekt durch den Unternehmer (UN) oder Projektverfasser (PV) erstellt werden, so dass der UN oder der PV die durch den Bauherrn bestellte Funktionen nach der Umsetzung zusammen mit den tangierten Systemen vollumfänglich testen und prüfen kann (Vorgaben bauseits sind zu berücksichtigen).

Beim Test in der Integrationsumgebung handelt es sich in der Regel um:

- einen Test im Werk des BSA-Unternehmers (Integrierter Werktest, IWT / Factory Integration Test, FIT) in der ersten Phase
- und um einen Test vor Ort in der effektiven Umgebung mit allen relevanten Systemumgebungen in der zweiten Phase.

Dieser Test erfolgt nach dem erfolgreich durchgeführten FAT (Siehe Richtlinie 13028).

Beim Test in der Produktionsumgebung handelt es sich um einen Test im Echtsystem (Echtzeittest, EZT / Site Integration Test, SIT) Dieser Test erfolgt nach dem erfolgreich durchgeführten SAT (Siehe Richtlinie 13028).

## 2.3 Grundstruktur Systemarchitektur

Die Systemarchitektur Schweiz (SA-CH) ist mehrstufig aufgebaut und entsprechend technisch so aufgebaut, dass der 7x24 Stunden Betrieb gewährleistet werden kann. Nachfolgend ist die Grundstruktur der Architektur in Abbildung 1 ersichtlich (Siehe Anhang IV.1):

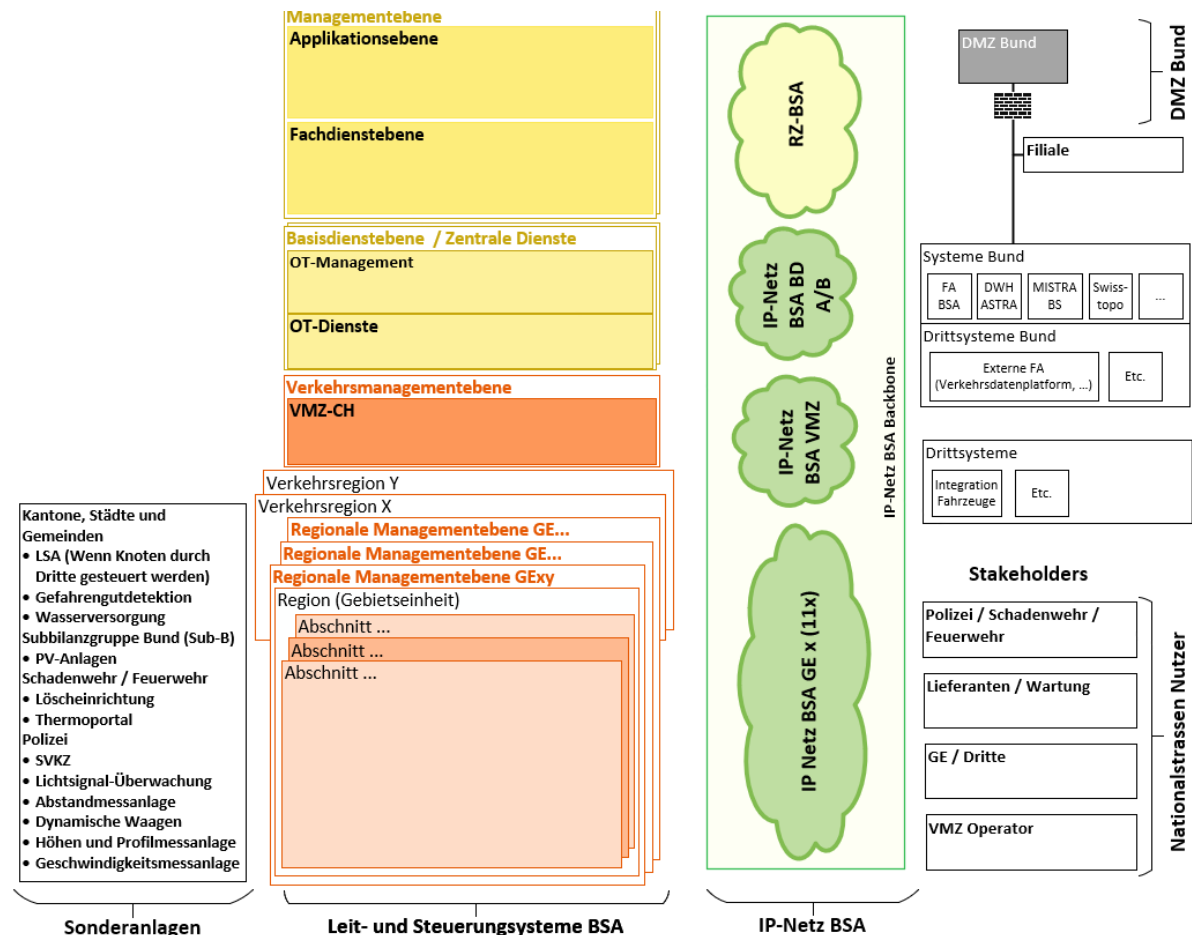


Abbildung 1: Grundstruktur der Architektur

### 2.3.1 IP-Netz BSA (Kommunikationsnetzwerk)

Die Kommunikationsinfrastruktur für die Betriebs- und Sicherheitsausrüstungen (BSA) der Nationalstrassen wird in den kommenden Jahren laufend an die ASTRA Richtlinie 13040 IP-Netz BSA angepasst. Mit dem IP-Netz BSA werden gezielt die Netzarchitektur, die Netzwerkgeräteanforderungen, die Services im IP-Netz BSA standardisiert und auf ein modernes in die Zukunft gerichtetes Fundament gestellt. Die heute bestehenden IPv4-Netze (alte Technologie) werden durch IPv6-Netze (neue Technologie) ersetzt und die bestehenden VDV-Anschlüsse wurden auf das IP-Netz BSA Backbone (Backbone Bund) migriert.

Mit diesen Neuerungen werden zentrale Basisdienste und Tools notwendig, um den sicheren (IT/OT-Sicherheit und Verfügbarkeit) und effizienten Betrieb des IP-Netz BSA zu garantieren. Die Betriebsverantwortung der IP-Netz BSA GE bleibt weiterhin bei den Gebiets-einheiten und des neuen IP-Netz BSA Backbone bei BIT/KdoCy.

Für den Betrieb der neuen Basisdienste und zentralen Tools ergeben sich neue Aufgaben, welche in der Folge beschrieben werden.

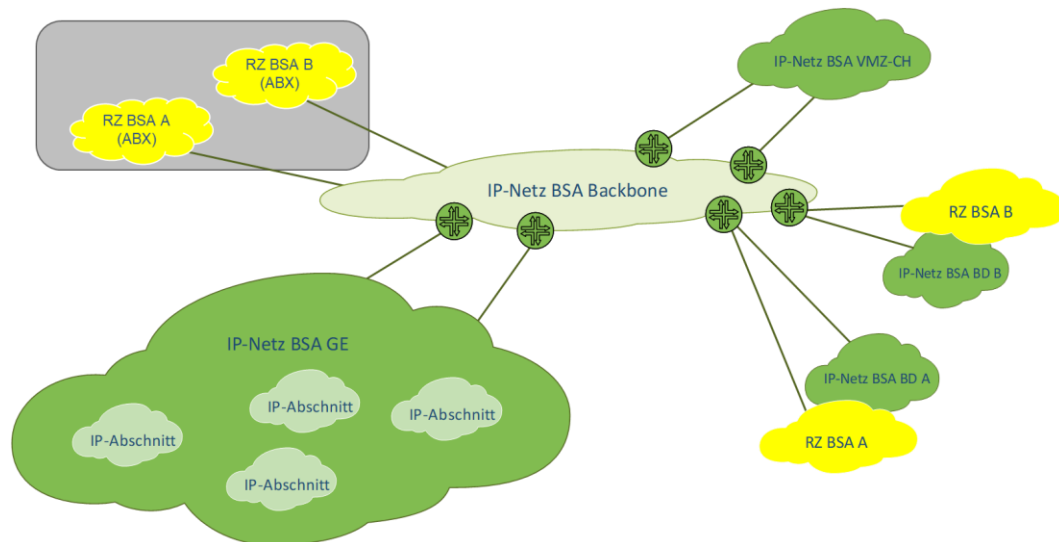


Abbildung 2: Übersicht IP-Netz BSA mit den zwei Standorten Basisdienst A und B und den beiden abzulösenden Standorten RZ BSA A und B (ABX)

## 2.3.2 Managementebene

Auf der Managementebene sind die übergeordneten Fachdienste und die Fachapplikationen für den operativen, übergeordneten Betrieb angesiedelt. Dabei wird zwischen der Fachdienst- und Applikationsebene unterschieden.

### 2.3.2.1 Applikationsebene

Diese Ebene wird hauptsächlich für die Fachapplikationen des Verkehrsmanagements als auch für die Informationsbereitstellung zur Übertragung an die Umsysteme-Bund genutzt.

### 2.3.2.2 Fachdienstebene

In dieser Ebene werden die Daten und Informationen für die Applikationsebene verarbeitet und aufbereitet. Ebenfalls werden hier Informationen für Analysen bereitgestellt.

## 2.3.3 Basisdienste / Zentrale Dienste

Die Basisdienste sind integraler Bestandteil des IP-Netzes BSA und sind notwendig, um das Netz effizient, effektiv und sicher zu betreiben. Die Dienste/Services werden in allen Teilnetzen IP-Netz BSA GE, IP-Netz BSA RZ, IP-Netz BSA Backbone und IP-Netz BSA VMZ-CH benötigt. In der Unterebene OT-Management werden die für das technische Management relevanten Systeme und in der Unterebene OT-Dienste werden die für das technische Management relevanten Dienste bereitgestellt.

## 2.3.4 Verkehrsmanagementebene Schweiz

Die Verkehrsmanagementzentrale Schweiz (VMZ-CH) nutzt die Verkehrsmanagementebene zum Schalten von Meldungen, zum Beispiel auf Wechseltextanzeigen (WTA) sowie zum Schalten von Signalisationen beispielsweise bei der Umnutzung des Pannestreifens (PUN) zu Stosszeiten.

## 2.3.5 Verkehrsregion

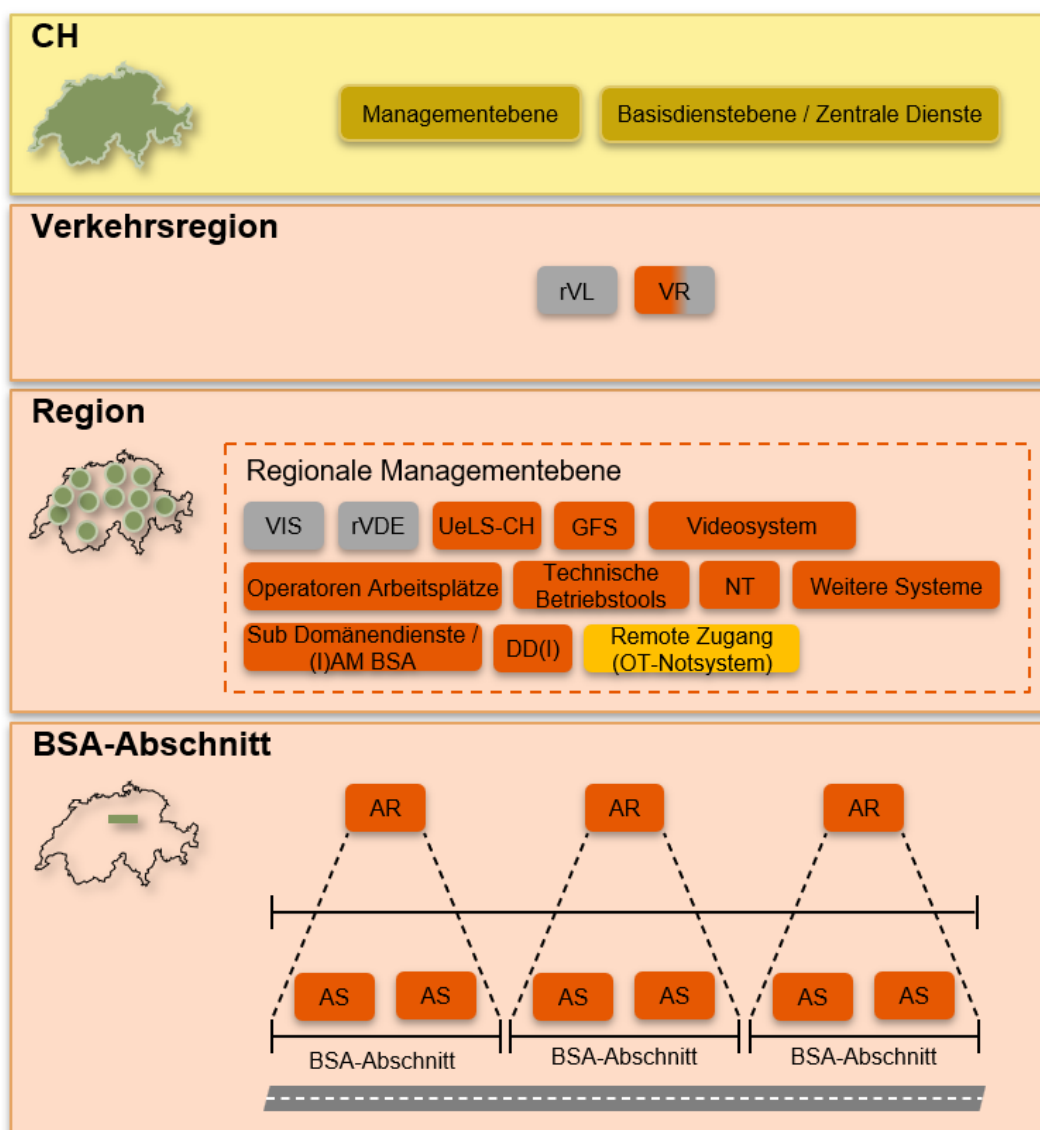
Die Verkehrsregion hat einen definierten Perimeter, welcher über die Gebietseinheits- und Filialgrenzen hinaus geht. Die Verkehrsregion vereint alle Verkehrsmanagement-Massnahmen. Die Verkehrsregion wird verkehrslogisch definiert. Sie umfasst alle relevanten Gebiete, die funktional zusammengehören, auch wenn sie zu unterschiedlichen Projekt- und Betriebsorganisation gehören.

### 2.3.6 Regionale Managementebene

Die Gebietseinheiten sind ab der Regionalen Managementebene für ihren jeweiligen Wirkungsbereich zuständig. Die Gebietseinheiten sind verantwortlich für den Betrieb und Unterhalt der Betriebs- und Sicherheitsausrüstungen als auch der OT in ihrem Perimeter. Die Gebietseinheiten sorgen für die Verfügbarkeit dieser Systeme und stellen, wo notwendig, Redundanzen bereit.

### 2.3.7 BSA-Abschnitt / IP-Abschnitt

Der Wirkungsbereich BSA-Abschnitt ist ein Teil der Nationalstrasse. Dieser bildet funktional eine autonomiefähige Einheit für die Betriebs- und Sicherheitsausrüstungen. Ein Abschnittsrechner übernimmt die Überwachung und übergeordnete Steuerung der Anlagen im BSA-Abschnitt sowie die Anbindung an das Übergeordnete Leitsystem Schweiz (UeLS-CH) der entsprechenden Gebietseinheit. Aus der Netzwerksicht wird vom IP-Abschnitt gesprochen, welcher zu 95% dem BSA-Abschnitt entspricht. In Einzelfällen ist der IP-Abschnitt grösser als der BSA-Abschnitt.



Legende:

- Fachdienste
- Fachapplikationen
- OT Dienste
- OT-Management Dienste
- Temporäre Systeme
- Systeme
- OT-Notsysteme

Abbildung 3: Räumliche Ausdehnung der Architekturelemente (logische Darstellung)



### 2.3.7.1 Räumliche Ausdehnung der spezifischen Verkehrsmanagement- und – Monitoring (Architekturelemente)

Für das Verkehrsmanagement und das Verkehrsmonitoring gibt es einen anderen Architekturaufbau, so gibt es auf offener Strecke kein spezifischer AR und nur bedingt einen AS. Im Folgenden ist diese logische Architektur beschrieben:

Die räumliche Ausdehnung der spezifischen Verkehrsmanagement-Architektur ist wie folgt definiert:

*Tabelle 1: Räumliche Ausdehnung Verkehrsmanagement*

| Räumliche Ausdehnung | Wirkungsfeld  |
|----------------------|---|
| CH                   | Operative Steuerung sämtlicher VM-Anlagen   |
| Verkehrsregion       | Temporäre regional wirkende Verkehrslenkungen oder Verkehrsrechner werden durch die FA VL-CH abgelöst werden.   |
| Region               | Temporäre regional wirkende Steuerungen von WTA/WWW als auch Verkehrsdatenerfassung für die Verkehrssteuerung werden durch die FA VL-CH abgelöst werden.  |
| IP-Abschnitt         | Das VM operiert basierend auf den IP-Abschnitten. Der Grossteil der VM-Anlagen (Bestandteil der BSA) befindet sich auf der offenen Strecke. Im Tunnel wird die weitere BSA, welche dem VM zudienen, mitbenutzt. |

Die Beschreibung der Bausteine erfolgt im Kapitel 3.

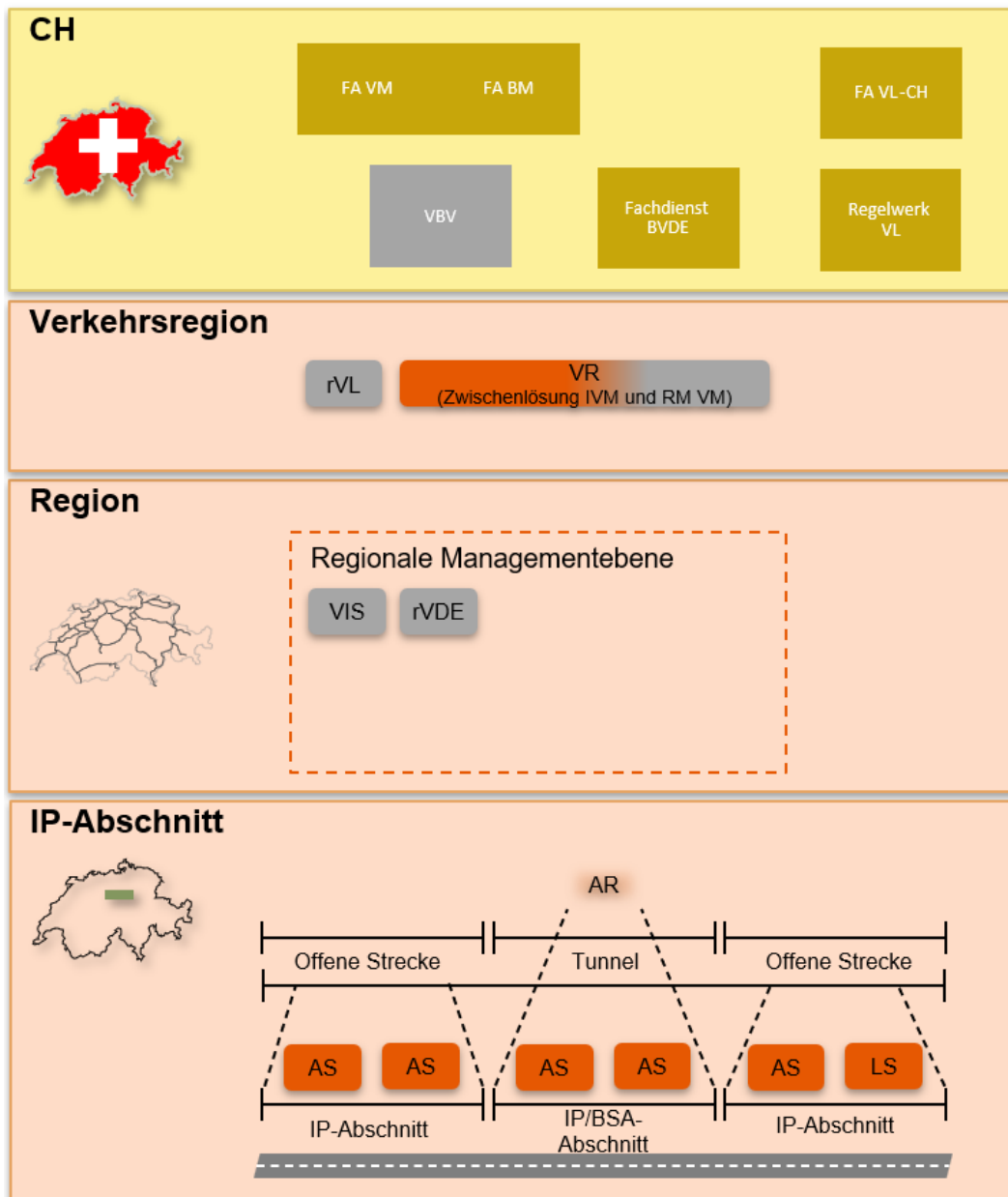


Abbildung 4: Räumliche Ausdehnung der spezifischen Verkehrsmanagement-Architekturelemente (logische Darstellung)

## 2.3.8 Systeme Bund, Drittsysteme und Sonderanlagen

Die Systemarchitektur sieht Schnittstellen vor, mit denen interne Systeme Bund oder Drittsysteme ausserhalb des IP-Netz BSA mit Informationen und Daten versorgt werden können. Sonderanlagen werden je nach Situation über das IP-Netz verbunden oder als Drittsysteme geführt, was durch das jeweilige BSA-Projekt der Filiale zu definieren ist.

### 2.3.8.1 Systeme Bund und Drittsysteme

Jede Anbindung wird individuell geprüft und entsprechend architektiert. Es werden ausschliesslich unidirektionale Verbindungen mittels «Service User» umgesetzt, welche vorgängig durch das CAB OT-Security zu bewilligen sind.

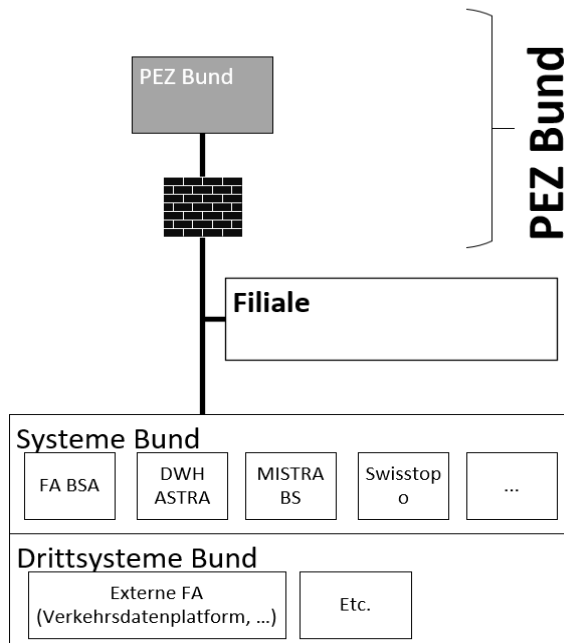


Abbildung 5: Übersicht Systeme Bund und Drittsysteme

### 2.3.8.2 Sonderanlagen

Diese Anlagen werden im Regelfall ausschliesslich von externem Betriebspersonal (siehe Geschäfts- und Betriebsorganisation BSA-OT) betrieben und sind Teil eines komplexen Gesamtregelwerks des spezifischen Gewerkes. Diese Anlagen werden projektspezifisch, sowohl auf die generelle Integration als auch auf die Kommunikationsintegration geprüft. Die spezifischen Vorgaben der jeweiligen Gewerke sind in den entsprechenden Richtlinien/Vereinbarungen enthalten. Nachfolgend die Übersicht der Sonderanlagen:

#### Kantone, Städte und Gemeinden:

- Lichtsignalanlage (LSA) (Wenn Knoten durch Dritte gesteuert werden);
- Gefahrgutdetektion;
- Wasserversorgung;

#### Subbilanzgruppe Bund (Sub-B):

- PV-Anlagen;

#### Schadenwehr / Feuerwehr:

- Löscheinrichtung;
- Thermoportal;

**Polizei:**

- Schwerverkehrskontrollzentren (SVKZ);
- Lichtsignal-Überwachung;
- Abstandmessenanlage;
- Dynamische Waagen;
- Höhen- und Profilmessenanlage;
- Geschwindigkeitsmessenanlage.

## 2.4 Wirkungssperimeter

Die Systemarchitektur hat verschiedene geografische Wirkungssperimeter, die in der Regel mit den Filial- oder Gebietseinheitsgrenzen übereinstimmen und sich auf die Strassenkilometer der Nationalstrassen beziehen. Die Wirkungssperimeter sind für die Nutzer der Systeme, wie Verkehrsmanagementzentrale, Polizei und Gebietseinheiten, wichtig. Daher ist es bei der Planung und Umsetzung der Systeme entscheidend, die Wirkungssperimeter der verschiedenen Systeme sorgfältig zu berücksichtigen, damit die Nutzer ihre Aufgaben in ihrem Verantwortungsbereich erfüllen können.

Folgende Wirkungssperimeter sind aus Sicht Nutzer zu beachten:

*Tabelle 2: Wirkungssperimeter aus Nutzersicht*

| Nutzer           | Wirkungssperimeter  |
|------------------|---|
| VMZ-CH           | Alle VM-Anlagen auf den Nationalstrassen der 1., 2. und 3. Klasse der Schweiz |
| Polizeien        | Mitnutzung der BSA für Verkehrssicherheit innerhalb der kantonalen Grenzen    |
| Gebietseinheiten | Alle OT-Systeme und BSA innerhalb der Gebietseinheit                          |

Für die Planung und Realisierung der BSA sind folgende Wirkungssperimeter aus Sicht der Systeme zu beachten:

*Tabelle 3: Wirkungssperimeter Systemsicht*

| Systeme                    | Wirkungssperimeter   |
|----------------------------|--|
| Fachapplikation            | In der Regel: schweizweit  |
| VR                         | Es ist in Ausnahmefällen erlaubt (temporär/Übergangsphase), mehrere Verkehrsrechner (VR) innerhalb einer Verkehrsregion zu platzieren. Dies ist jedoch eine Ausnahme, die begründet werden muss. Diese VR werden mit der FA VL-CH abgelöst werden. |
| UeLS-CH                    | gebietseinheitsweit  |
| rVDE, VIS, NT              | gebietseinheitsweit  |
| BSA-Abschnitt/IP-Abschnitt | objektweit   |

## 3 Architektur SA-CH

Dieses Kapitel beschreibt die Ebenen und die darin enthaltenen Elemente der Architektur. Die Anforderungen an die Elemente innerhalb jeder Ebene werden nicht detailliert beschrieben. Die Beschreibung der Leistungsanforderungen sowie der funktionalen Anforderungen folgt in den Kapiteln 4 und 5.

### 3.1 Managementebene

Die Managementebene ist die oberste Ebene der BSA. Sie ist die zentrale, übergeordnete Leit- und Steuerebene für die gesamte Schweiz. Den Nutzern können Funktionen und geografische Wirkungssperimeter anhand ihrer Rollen und Aufgaben zugewiesen werden. Die Managementebene umfasst die Applikations- und die Fachdienstebene.

#### 3.1.1 Applikationsebene

Die Applikationsebene enthält die Funktionen der Fachapplikationen mit schweizweiter Verwendung und schweizweiter Wirkung, mit welchen die Nutzer mit bestimmten Rollen über Benutzeroberflächen mit dem System kommunizieren. Die Nutzer der Applikationen können die VMZ-CH, die Polizeien und die Gebietseinheiten sein.

Die Fachapplikationen (FA) unterstützen die Geschäftsprozesse für alle involvierten Benutzer. Jede FA verfügt über eine Benutzeroberfläche und eine dazugehörige Steuerungslogik, die die darunterliegenden Fach- oder Basisdienste aufruft. Jeder Benutzer und jede Benutzergruppe hat entsprechend ihrer Rolle und Zugriffsrechte im Benutzermodell (siehe Kapitel 3.2.1.4) spezifische Ansichten in einer oder mehreren Fachapplikationen. Neu zu erstellende Fachapplikationen müssen, wo möglich, die bereits implementierten Basis- und Fachdienste verwenden, anstatt gleiche Funktionalitäten nochmals umzusetzen.

Folgende FA sind heute realisiert oder geplant:

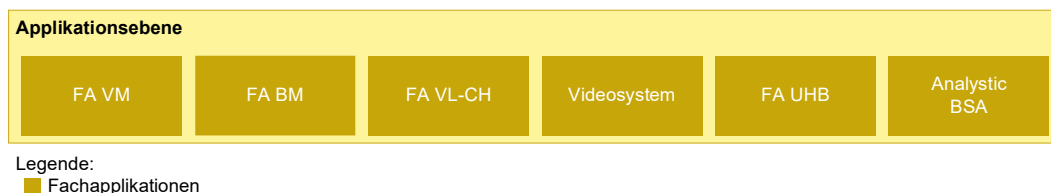


Abbildung 6: Applikationsebene

##### 3.1.1.1 FA VM

Die FA Verkehrsmanagement (FA VM) unterstützt die Informationsverbreitung und Verkehrsbeeinflussung für einen möglichst flüssigen Verkehr auf dem Nationalstrassennetz (MIV und Schwerverkehr).

##### 3.1.1.2 FA BM

Die FA Baustellenmanagement (FA BM) sorgt für einen ständig aktuellen Überblick über alle auf der Nationalstrasse geplanten und laufenden Baustellen. Dies beinhaltet Informationen über die Dauer der Baustelle sowie über die Einschränkungen bezüglich der Befahrbarkeit des betroffenen Abschnitts.

##### 3.1.1.3 FA VL-CH

Die FA Verkehrslenkung Schweiz (FA VL-CH) dient zur schweizweiten Information, Lenkung, Leitung und Steuerung des Verkehrsflusses. Sie beinhaltet das automatisierte Lenken, Leiten und Steuern mittels Algorithmen (vgl. ASTRA Richtlinie 15019) und erlaubt den Nutzern den Zugriff und die Steuerung aller VM-Anlagen auf den Nationalstrassen (vgl. ASTRA Richtlinie 15003).

### 3.1.1.4 Videosystem

Die Videosysteme der Managementebene sind Teil des Videosystems VIDEO-CH für die manuelle Archivierung von ausgewählten, ereignisbezogenen Bildsequenzen. Die Bildsequenzen werden bei Archivwürdigkeit nach einer Bestätigung der GE aus den lokalen Bildspeichern der GE in das zentrale Archiv verschoben. Die Bewirtschaftung des Archivs erfolgt nach festgelegten Regeln und im Einklang mit den Datenschutzbestimmungen.

### 3.1.1.5 FA UHB

Die Fachapplikation Unterhalt und Betrieb (FA UHB) unterstützt die Gebietseinheiten beim operativen Betrieb und bei der Erhaltung der BSA. Bei Ereignissen können die BSA-Anlagen durch die Gebietseinheiten gesteuert werden und dabei die Ereignisdienste vor Ort unterstützen. Zudem trägt die FA UHB zu einem effizienten Asset-Management bei, indem Betriebsdaten der BSA gesammelt und ausgewertet werden können. Eine Detaillierung dieses Aspekts erfolgt im Rahmen der Fortschreibung der Richtlinie zu einem späteren Zeitpunkt.

### 3.1.1.6 Analytics BSA

Die Analytics BSA stellt die Auswertbarkeit der Datenbasis sicher. Hierbei können ein oder mehrere Tools zum Einsatz kommen, die aber alle an den Fachdiensten «Datenbasis Analyse» und «BSA Datawarehouse» ansetzen.

Mit den Analytics-Tools können auch moderne Technologien der Datenanalyse genutzt werden wie z.B. auch Artificial Intelligence (AI) Funktionalitäten. Eine Detaillierung dieses Aspekts erfolgt im Rahmen der Fortschreibung der Richtlinie zu einem späteren Zeitpunkt.

## 3.1.2 Fachdienstebene

Die Fachdienste stellen gekapselte, fachliche Funktionalitäten oder Fachdaten bereit. Eine Gesamt-Fachfunktionalität im Umfeld eines Themas (z.B. Verkehrslenkung) umfasst einerseits die Fachapplikation, wie auch einen oder mehrere Fachdienste. In den Fachdiensten werden ASTRA-spezifische Funktionen der Managementebene wie z.B. Verkehrsprognosen zur Verfügung gestellt.

Die Funktionen und Daten aus den Fachdiensten haben grundsätzlich eine schweizweite Abdeckung und stehen allen Fachapplikationen zur Verfügung. Folgende Fachdienste sind geplant oder realisiert:

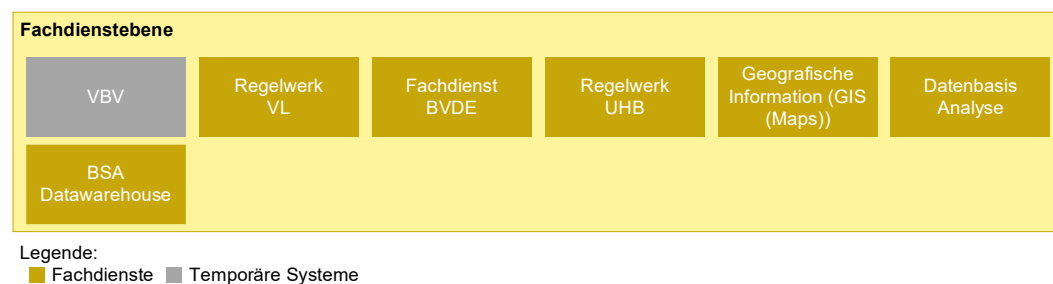


Abbildung 7: Fachdienstebene

### 3.1.2.1 VBV

Vehicle-By-Vehicle (VBV) ist ein System, welches Einzelfahrzeug-Rohdaten der Zählstellen oder Zählstellencontroller (ZSC) entgegennimmt, verarbeitet und den Fachapplikationen zur Verfügung stellt. Die ZSC sind in Abstimmung mit der IP-Netz BSA Migration abzubauen.

**3.1.2.2 Regelwerk VL (Verkehrstechnische Regelungslogik)**

Das Regelwerk Verkehrslenkung (VL) umfasst die fachlichen Funktionen der FA VL-CH. Dazu gehören die fachspezifische Algorithmik und die benötigten Regelungsverfahren, um eine verkehrsabhängige Regelung anhand aktueller Verkehrsdaten zu erreichen und die verkehrlich notwendigen Massnahmen zu ermitteln. Das Regelwerk VL gleicht manuelle und automatische regelungsbasierte Schaltwünsche miteinander ab. Es folgt dabei festgelegten Prioritäten und parametrisierbaren Regeln. Die Richtlinie 15019 beschreibt die entsprechenden Vorgaben und Anforderungen.

**3.1.2.3 Fachdienst BVDE**

Der Fachdienst Betriebs- und Verkehrsdaten Erhebung (BVDE) löst das VBV ab. Er verarbeitet alle Verkehrsdaten aus verschiedenen Quellen und stellt sie den Applikationen in den gewünschten Formaten und Aggregationen zur Verfügung (inkl. der logischen Verkehrszähler).

**3.1.2.4 Regelwerk UHB**

Dieser Fachdienst hängt von der Umsetzung der FA UHB ab. Eine Detaillierung dieses Aspekts erfolgt im Rahmen der Fortschreibung der Richtlinie zu einem späteren Zeitpunkt.

**3.1.2.5 Geografische Informationen (GIS (Maps))**

Zentral bereitgestellte geografische Informationen in Form von Raster- oder Vektordaten (z.B. Luftbilder oder Maps/Karten) für die Positionierung resp. Verortung von Objekten, wie sie in Geoinformationssystemen (GIS) oder durch andere Anwendung für den georäumlichen Kontext verwendet werden (z.B. als Hintergrundlayer eines Kartenfensters). Dieser Service wird für alle innerhalb des IP-Netz BSA verwendeten geografische Informationen verwendet werden.

**3.1.2.6 Datenbasis Analyse**

In diesem Fachdienst werden unterschiedliche Analysen basierend auf den innerhalb des IP-Netz BSA vorhandenen Daten ermöglicht. Eine Detaillierung dieses Aspekts erfolgt im Rahmen der Fortschreibung der Richtlinie zu einem späteren Zeitpunkt.

**3.1.3 BSA Datawarehouse (DWH)**

In diesem Fachdienst werden unterschiedliche Daten zusammengeführt, allfällig veredelt und zur Weiterbearbeitung bereitgestellt. Eine Detaillierung dieses Aspekts erfolgt im Rahmen der Fortschreibung der Richtlinie zu einem späteren Zeitpunkt.

**3.2 Basisdienstebene / Zentrale Dienste**

Auf der Ebene der Basisdienste und Zentralen Dienste befinden sich die Grunddienste für das Management der für den Betrieb relevanter Systeme. Hier werden netzwerkübergreifende Funktionen ausgeführt (unter anderem das Abgleichen der einheitlichen Zeit). Ebenfalls auf dieser Ebene sind die übergeordneten Betriebsdienste eingebettet, welche den verschiedenen Anspruchsgruppen die Möglichkeit bieten, Einblick in die Systeme zu nehmen.

Die Basisdienste sind integraler Bestandteil des IP-Netzes BSA und sind notwendig, um das Netz effizient, effektiv und sicher zu betreiben.

### 3.2.1 OT-Management

Das OT-Management stellt in den Basisdiensten zentrale Systeme bereit, die für den Betrieb der Netzwerkkommunikation und der OT-Systeme unabdingbar sind. Zudem werden zentrale Portale bereitgestellt, die den Zugriff auf Fachapplikationen ermöglichen. Es wird angestrebt, die Zugriffsberechtigungen so weit wie möglich einzuschränken, um die Sicherheit zu gewährleisten.

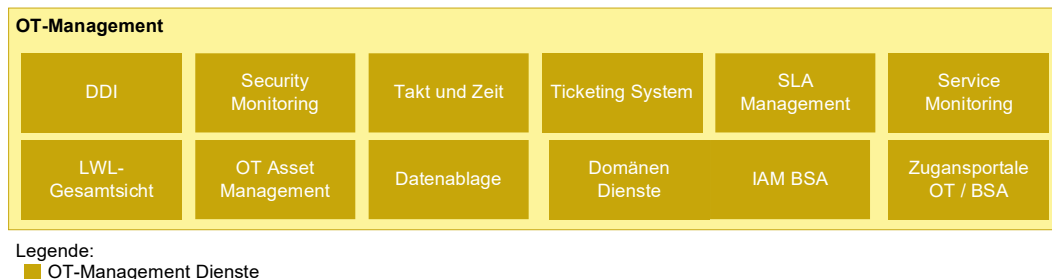


Abbildung 8: OT-Management

#### 3.2.1.1 DDI

Das DNS-, DHCP-, IP-Adress-Management-Tool (DDI) ist das zentrale IP-Adressverwaltungssystem, das allen Gebietseinheiten zur Verfügung steht. Neben der IP-Adressverwaltung werden auch die DNS- und DHCP-Server der Gebietseinheiten mit den notwendigen Daten bspw. für die Namensauflösung versorgt. Den Gebietseinheiten steht jeweils ein eigener Mandant zur Verfügung.

#### 3.2.1.2 Security Monitoring

Das Security Monitoring dient dazu, die kontinuierliche Überwachung der Sicherheit der OT-Systeme sicherzustellen. Zu diesem Zweck werden Informationen aus unterschiedlichen (Log-) Quellen gesammelt und analysiert. Ziel ist es, Anomalien, verdächtige Vorgänge oder nicht autorisierte Systemänderungen in den OT-Systemen oder dem Netzwerk zu erkennen und geeignete Massnahmen ergreifen zu können.

#### 3.2.1.3 Takt und Zeit

Die OT-Managementebene stellt eine Takt- und Zeitquelle bereit. Unter «Zeit» wird die übliche Systemzeit aus einer 24-Stunden-Tageszeit und aus Datum verstanden. Unter «Takt» wird ein technisches Referenzsignal verstanden, aus dem sich Frequenz und Phase ableiten lassen, aber keine Information zur absoluten Zeit enthält.

Die weiteren Vorgaben sind in der ASTRA Dokumentation 83044 ersichtlich.

#### 3.2.1.4 Domänen Dienst und IAM BSA

Für die BSA steht eine eigene Domain «nationalstrassen.admin.ch» mit je einer Subdomain für die GE, die VMZ-CH und die BD zur Verfügung. Die Domain «nationalstrassen.admin.ch» ist exklusiv für BSA reserviert und wird durch das ASTRA zentral administriert. Die unterliegenden Domänen inkl. der entsprechenden AD- und DNS-Server der GE und VMZ-CH werden durch die GE/VMZ-CH betrieben.

Sämtliche User-Objekte und User-Groups (Rollengruppen) werden zentral im IAM BSA verwaltet. Der Abgleich zwischen den Active Directory (AD) in den GE und dem zentralen IAM BSA wird durch das IAM BSA sichergestellt. Ebenso werden die notwendigen DNS- und DHCP Dienste durch das DDI aktualisiert.



### 3.2.1.5 IAM BSA

Das IAM (Identity and Access Management) BSA ist das zentrale Identitäts- und Zugriffsmanagement der OT/BSA. Es gewährleistet die Verwaltung aller User und Rollen der Nationalstrassen-Domäne. Identitäten werden nur einmal verwaltet und die Berechtigungen werden von jeder GE und der VMZ-CH sowie BD/RZ BSA individuell erteilt. Das IAM BSA ist ausschliesslich für die OT/BSA innerhalb des IP-Netz BSA genutzt und hat keine Verbindung zu anderen Verzeichnisdiensten des Bundes.

### 3.2.1.6 Zugangsportale OT/BSA

Zentral werden in den Basisdiensten IP-Netz BSA verschiedene Zugangsportale für autorisierte Benutzer zur Verfügung gestellt. Die Zugangsportale stellen den Zugang von ausserhalb des IP-Netzes BSA wie beispielsweise dem Internet auf die zugelassenen Systeme innerhalb des IP-Netzes BSA sicher (Privileged Access Management, PAM). Die Zugänge dienen zur Wartung von Systemen (Remote Access) oder auch für den Zugang auf Fachapplikationen. Sie sind gemäss ASTRA Dokumentation 83042 Network Security Policy (NSP) besonders geschützt. Es werden sämtliche Aktivitäten geloggt und sind nachvollziehbar.

### 3.2.1.7 LWL-Gesamtsicht

Die Lichtwellenleiter (LWL)-Gesamtsicht bietet eine umfassende Übersicht der LWL-Infrastruktur und dient den Betreibern und den Projekten als Unterstützung. Das ASTRA ist der Leistungserbringer für den Bund und stellt verschiedene LWL-Verbindungen für das Optische Behördennetz Bund (OBNB) bereit. Die Verwaltung der LWL-Kabel liegt in der Verantwortung der Gebietseinheiten des ASTRA. Hier geht es ausschliesslich um eine übergeordnete Gesamtsicht ohne Detailinformationen (diese sind bei den Gebietseinheiten).

### 3.2.1.8 OT Asset Management

Das OT Asset Management dient zur Erfassung und Pflege des OT-Inventars sowohl in den Gebietseinheiten als auch in den Basisdiensten. Den Gebietseinheiten steht jeweils ein eigener Mandant zur Verfügung.

### 3.2.1.9 Datenablage

Die Datenablage beinhaltet übergeordnete Dokumente, die schwerpunktmässig auf den Betrieb IP-Netz BSA ausgerichtet sind und für die Betreiber bereitgestellt werden.

### 3.2.1.10 SLA Management (Service Level Agreement Management)

Ein Service Level Agreement (SLA) bezeichnet eine Vereinbarung zwischen einem Leistungserbringer und einem Leistungsbezüger und regelt die zugesicherte Leistungseigenschaften. Das SLA Management definiert die Begrifflichkeiten wie Servicezeit oder Reaktionszeit als auch die Wiederherstellungszeit für die BSA und legt die möglichen Ausprägungen der verschiedenen Leistungseigenschaften fest. Ziel ist, standardisierte SLA zu vereinbaren und zu verwalten, damit die unterschiedlichen Leistungserbringungen ineinandergreifen können und betrieblich aufeinander abgestimmt sind.

### 3.2.1.11 Ticketing System

Das Ticketing System dient der Unterstützung der wichtigsten Betriebsprozesse wie Incident Management, Problem Management, Change Management und Service Request. Dieses übergeordnete Ticketingsystem erhält die für den übergeordneten Betrieb notwendigen Meldungen der GE-Ticketingsysteme.

### 3.2.1.12 Service Monitoring

Das Service Monitoring bietet einen Überblick über den Status des IP-Netzwerks BSA GE, der Verbindungen zum Backbone IP-Netz BSA und der zentralen Dienste und Tools. Diese End-2-End Service-Sicht ist immer dann zwingend notwendig, wenn im Störfall mehr als eine GE betroffen ist und eine übergeordnete Störungsanalyse und -behebung notwendig wird (Störungseskalation).

Das Service Monitoring ist ein zentrales Tool, welches durch die zentrale Organisation (resp. durch den übergeordneten Betrieb) betrieben und genutzt wird.

## 3.2.2 OT-Dienste

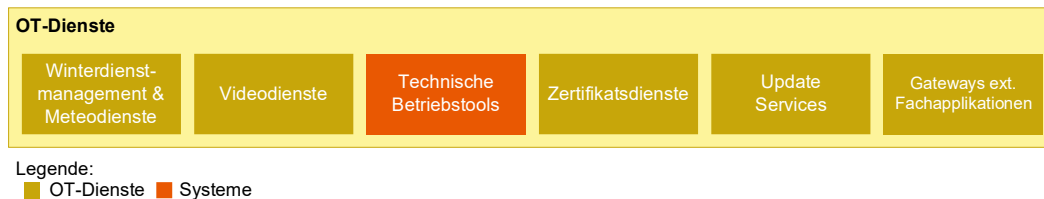


Abbildung 9: OT-Dienste

### 3.2.2.1 Winterdienstmanagement und Meteodienste

Das Winterdienstmanagement umfasst Systeme und Dienste, um gefährliche Fahrbahnen und Wettersituationen frühzeitig zu erkennen und Winterdienstmassnahmen optimal planen und steuern zu können. Die Meteodienste umfassen die zentralen Komponenten zur Erfassung der Wetterdaten auf den Nationalstrassen. Dazu gehören bspw. die Glatteis-Frühwarnsysteme.

### 3.2.2.2 Zertifikatsdienste

Um einen sicheren Datenverkehr auch innerhalb des IP-Netz BSA sicherzustellen, werden grundsätzlich nur sichere Protokolle zugelassen. Dazu sind digitale Zertifikate notwendig, die über eine eigene private Zertifizierungsstelle (Certificate Authority, CA) ausgestellt werden. Mit Hilfe dieser Zertifikate wird die elektronische Identität von Kommunikationspartnern bescheinigt. Die private CA ist ebenfalls als Service in den Basisdiensten ausgelegt. Die von dieser CA ausgestellten Zertifikate dienen ausschliesslich für die Kommunikation der BSA innerhalb des IP-Netz BSA und sind speziell auf die spezifischen Bedürfnisse der BSA ausgelegt.

### 3.2.2.3 Videodienste

Die Videodienste sind Teil des Videosystems VIDEO-CH und dienen dazu, Videobilder und Videostreams an verschiedene Stakeholder ausserhalb des IP-Netz BSA bzw. des ASTRA weiterzugeben. Dabei werden die Videobilder entsprechend der geltenden Datenschutzbestimmungen für die jeweiligen Abnehmergruppe und unter Einhaltung der Sicherheitsbestimmungen OT-Security zur Verfügung gestellt.

### 3.2.2.4 Update Services

Verschiedene Update Services dienen dazu, relevante Softwareupdates bzw. Security Patches oder Signatur Files für den Virenschutz auf dem aktuellen Stand zu halten. Da kein direkter Zugriff von den OT-Systemen auf die Update Server der Hersteller zugelassen ist, stellen die Update Services die notwendigen Daten über spezifische Sicherheitsmechanismen zentral zur Verfügung.

### 3.2.2.5 Gateways externe Fachapplikationen

Gateways ermöglichen den Fachapplikationen den Austausch mit spezifischen Services und Fachapplikationen ausserhalb des Perimeters IP-Netz BSA. Die Gateways sind Teil der Sicherheitsinfrastruktur des IP-Netz BSA. Die Details zu den einzelnen Gateways werden in der Systemarchitektur der BD oder in den Systemarchitekturen der FA beschrieben.

### 3.2.2.6 Technische Betriebstools

Die technischen Betriebstools dienen der Verwaltung und der Überwachung des IP-Netzes BSA Basisdienste, der Virtualisierungsumgebungen in den Basisdiensten und den Sicherheitselementen. Die Systeme werden hauptsächlich zur Unterstützung von Betriebsprozessen, zur Pflege des Hard- und Softwarebestands und zur Konfiguration von Systemkomponenten verwendet. Zudem sind sie wesentliche Elemente in der Störungserkennung und -behebung und dienen der Netzwerk- und Systemsicherheit.

Zu den technischen Betriebstools gehören insbesondere das Netzwerkmanagementsystem (NMS) oder das Monitoring und Alarming. Die Definition und die Anforderungen zum NMS sind der ASTRA Richtlinie 13040 zu entnehmen.

## 3.3 Verkehrsmanagementebene Schweiz

Die VMZ-CH nutzt verschiedene Elemente der Systemarchitektur auf der Verkehrsmanagementebene damit die Aufgaben der Operatoren, Verkehrsingenieure und Administratoren erfüllt werden können. Die VMZ-CH hat Zugriff auf verschiedene Fachapplikationen sowie auf die VM-Sicht im UeLS-CH und zum Teil direkt auf VM-Anlagen.

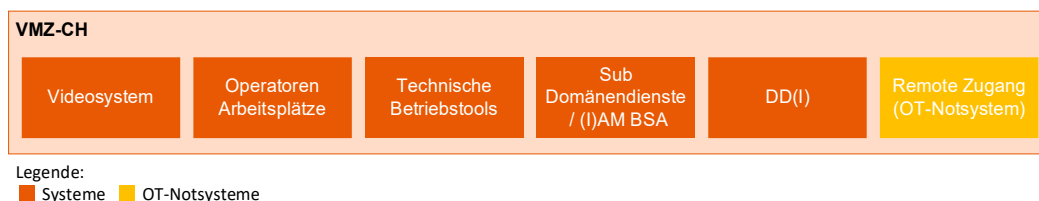


Abbildung 10: Verkehrsmanagementebene Schweiz

### 3.3.1.1 Videosystem

Das Videosystem der VMZ-CH ist Teil des Videosystems VIDEO-CH und dient dazu, Videostreams auf den Operator Arbeitsplätzen und der Videowand der VMZ-CH darstellen zu können. Die Auswahl der Videostreams kann manuell oder automatisch basierend auf Ereignissen vorkonfiguriert werden. Dabei können sowohl Live-Bilder als auch gespeicherte Bilder aus dem Ringspeicher ausgewählt werden.

### 3.3.1.2 Operatoren Arbeitsplätze

Die Operatoren Arbeitsplätze dienen den Nutzern zur Überwachung, Verwaltung sowie Nutzung hauptsächlich der Verkehrsmanagementsysteme. Dies sind keine Bundesverwaltungs-Arbeitsplätze, sondern dedizierte Arbeitsplätze in der OT-BSA.

### 3.3.1.3 Technische Betriebstools

Die technischen Betriebstools dienen der Verwaltung und der Überwachung des IP-Netzes BSA VMZ-CH, der Virtualisierungsumgebungen in der VMZ-CH und den Sicherheitselementen. Die Systeme werden hauptsächlich zur Unterstützung von Betriebsprozessen, zur Pflege des Hard- und Softwarebestands und zur Konfiguration von Systemkomponenten verwendet. Zudem sind sie wesentliche Elemente in der Störungserkennung und -behebung und dienen der Netzwerk- und Systemsicherheit.

Zu den technischen Betriebstools gehören insbesondere das Netzwerkmanagementsystem (NMS) oder das Monitoring und Alarming. Die Definition und die Anforderungen zum NMS sind der ASTRA Richtlinie 13040 zu entnehmen.

### 3.3.1.4 Sub-Domänendienste / (I)AM BSA

Die Sub-Domänendienste beinhalten die Subdomain «vmzch.nationalstrassen.admin.ch» mit dem entsprechenden Active Directory und den Diensten DNS und DHCP. Die AD wird direkt durch das IAM BSA mit den aktuellen Daten zu Usern und Usergroups versorgt.

### 3.3.1.5 DD(I)

Die DNS- und DHCP-Server der VMZ-CH werden mit den notwendigen Daten bspw. für die Namensauflösung durch das zentrale DDI versorgt. Bei einem Ausfall der zentralen Komponenten IAM BSA und DDI funktionieren die lokalen Dienste wie AD, DNS und DHCP weiterhin ohne Einschränkungen für den Tagesbetrieb.

### 3.3.1.6 Remote Zugang (OT-Notsystem)

Der lokale Remote Zugang der VMZ-CH dient als Notzugang bei einem Ausfall des Dienstes «Zugangsportale OT-BSA» auf der übergeordneten Ebene Basisdienste. Die Zugriffsberechtigungen sind auf das Nötige eingeschränkt, um die Sicherheit zu gewährleisten.

## 3.4 Verkehrsregionen

Eine Region, die verkehrlich eng verknüpft ist und verkehrlich als Einheit gesehen wird, ist eine Verkehrsregion. Diese kann sich über GE oder auch Filialgrenzen hinweg erstrecken (Siehe Abbildung 5) oder für das Verkehrsmanagement als auch für Verkehrsmonitoring die ganze Schweiz betreffen. Die Verkehrsregion wird verkehrslogisch definiert, nicht verwaltungslogisch. Sie umfasst alle relevanten Gebiete, die funktional zusammengehören. Ziel ist eine kohärente Betrachtung und Planung des Verkehrsraums auf Basis realer Verkehrsbeziehungen.

Der Verkehrsrechner (VR) übernimmt als Übergangslösung die abschnittsübergreifende Koordination der darunterliegenden (Anlagesteuerung Signalisation (AS-S) oder Lokalsteuerung (LS)), falls in der Verkehrsregion solche verkehrstechnischen Funktionen verlangt sind (z.B. Betriebszustände mit grosser Ausdehnung oder abschnittsübergreifende Geschwindigkeitsharmonisierung (über mehrere Abschnitte oder Anschlüsse/Verzweigungen); i.d.R. erforderlich in verkehrstechnisch komplexeren BSA-Regionen). Es wird das Ziel verfolgt, nur wenige VR pro Region zu realisieren, um die nachfolgenden Hauptfunktionen zu erhalten.

- Koordination und Steuerung der untergeordneten AS (insbesondere bei Überlappungen und Abhängigkeiten);
- Schaltung von kombinierten (Standard) Betriebszuständen aller Verkehrsmanagement-Massnahmen mittels Vorschau/Ist-Bild Ansicht gemäss Richtlinie 15019;
- Realisierung von Abhängigkeiten zwischen Abschnitten (Gefahrensignalisation, Geschwindigkeitssignale);
- Steuern der PUN und Rampendosierungen.

Nicht Rili 15019-konforme Anlagen:

- Zeitgeschaltetes Verkehrs-Regime bei Ausfall der Verkehrsdatenerfassung;
- Flächendeckende Betriebszustände (80km/h, Schleudergefahr, etc.);
- Abgleich zwischen mehreren benachbarten VR muss sichergestellt werden.

Die VR sind eine Zwischenlösung und werden später durch die FA VL-CH abgelöst (siehe Kapitel 6 Migration).

### 3.4.1 Streckenbasiert bis schweizweite Verkehrslenkung

Das Verkehrsmanagement kann sowohl streckenbasierend als auch schweizweit erfolgen. Im Zielausbau wird die FA-VL-CH mindestens GHGW, RaDo und PUN gemäss der verkehrstechnischen Regelungslogik sowie WTA steuern.

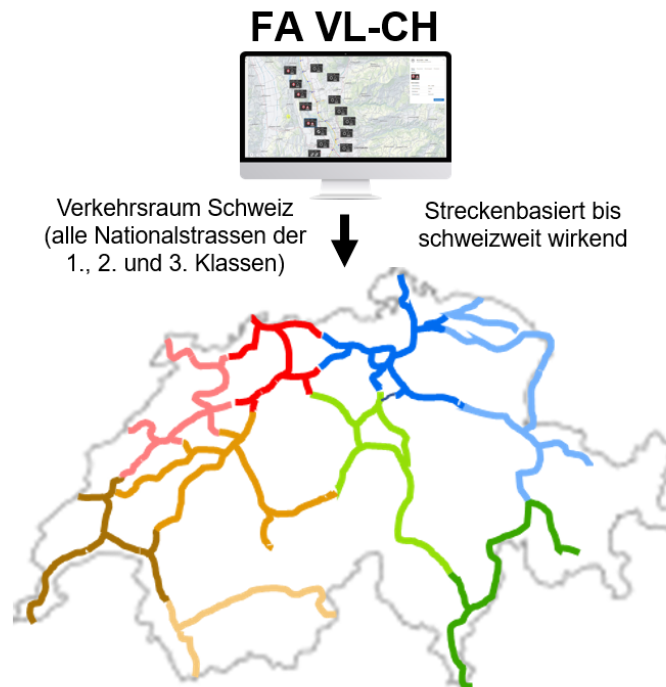


Abbildung 11: Wirkungssperimeter der FA VL-CH

### 3.4.2 Beispiel von streckenbasiertem Verkehrsmanagement

Einige Beispiele der aktuell vorhandenen VM-Anlagen im streckenbasierten Verkehrsmanagement sind nachfolgend ersichtlich.

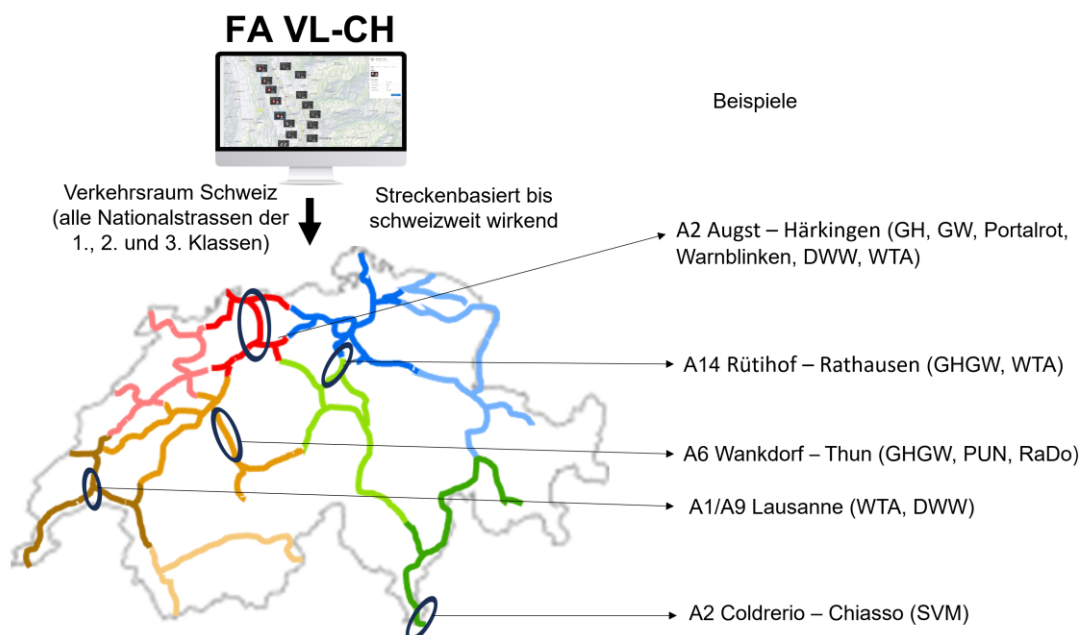


Abbildung 12: Streckenbasiertes Verkehrsmanagement

**3.4.2.1 A2 Augst – Härkingen (GH, GW, Portalrot, Warnblinken, DWW, WTA)**

Die Reduktion auf einen Fahrstreifen Richtung Bern (Verbindungsrampe von der A2 in die A1) und die grossen Verkehrsmengen auf der A1 selbst führen zu einem Rückstau, der sich auf die A2 Belchensüdrampe fortsetzt. Die verkehrstechnische Regelungslogik setzt automatisch die Geschwindigkeit runter. Erreicht der Rückstau eine gewisse Länge, setzt die VMZ-CH die Geschwindigkeit im Belchen-Tunnel und dessen Nach- und Vorzone runter und schaltet die Stauwarnung sowie das Warnblinken im Tunnel. Wird der Stau noch länger, wird der Tunnel temporär gesperrt (Portalrot). Verlängert sich der Stau noch weiter, dann werden ähnliche Massnahmen an den weiteren drei Tunnels Oberburg, Ebenrain und Arisdorf getroffen. Ab einem gewissen Zeitverlust werden zudem die Fernziele Chiasso (I) Gotthard Luzern über die A3 und die Verzweigung Birrfeld zur Verzweigung A1 Wiggertal mittels WTA umgeleitet.

**3.4.2.2 A14 Rütihof – Rathausen (GHGW, WTA)**

Der tägliche Pendler-Stau auf der A14 vor der Verzweigung Rotsee wird über ein GHGW-System geregelt. Die VMZ-CH beobachtet die Entwicklung und trifft weitere Massnahmen falls notwendig. Dies kann WTAs vor dem Stauende betreffen, um davor zu warnen bis zu Umleitungen ab Zürich via Wiggertal – sofern die Umleitungsrouten frei ist.

**3.4.2.3 A6 Wankdorf-Thun (GHGW, PUN, RaDo)**

Auf der ganzen Strecke ist ein automatisiertes GHGW sowie am Anschluss Rubigen eine automatisch funktionierende Rampendosierung (RaDo) auf der Einfahrt vorhanden. Im Falle eines Unfalles auf der Einfahrtsrampe muss für die Polizei und die VMZ-CH die Möglichkeit bestehen, die RaDo ausser Betrieb zu nehmen. Die PUN-Strecken zwischen Muri und Wankdorf werden von der VMZ-CH bei Bedarf visuell geprüft und anschliessend freigegeben (oder nicht).

**3.4.2.4 A1/A9 Lausanne (WTA, DWW)**

Die VMZ-CH hat in der Westschweiz heute nur wenige Kameras und keine Systeme zur Verfügung – mit Ausnahme der WTA und DWW. Diese werden insbesondere dann kombiniert verwendet, wenn auf der A1 nach Bern, der A9 zwischen Lausanne und Vevey oder auf der A12 Verkehrsstörungen festgestellt oder Sperrungen eingerichtet werden. Die regionalen Systeme werden durch die regionale Leitzentrale bedient. Zukünftig werden diese ebenfalls via FA VL-CH bedient werden.

**3.4.2.5 A2 Coldrerio – Chiasso (SVM)**

Zwischen der Raststätte Coldrerio und dem Warenzoll in Chiasso besteht ein Dosiersystem/ein Tropfenzähler für den Schwerverkehr. Dieser wird bei Rückstau aus dem Warenzoll Chiasso auf die A2 manuell durch die VMZ-CH eingeschaltet. Das System kann auch für die Geschwindigkeitsreduktion und Gefahrenwarnung verwendet werden, wenn an der Zollstelle Chiasso-Brogeda ein Stau des Gesamtverkehrs festgestellt wird.

### 3.4.3 Streckenbasierte Architekturelemente der spezifischen Verkehrsmanagementsicht

Der grösste Teil der Architekturelemente des Verkehrsmanagements befinden sich auf der «offenen Strecke» und sind dort als dedizierte Anlagen (Hauptverwendung im Normalbetrieb) aufgebaut. Insofern auf der definierten Strecke auch Tunnel vorhanden sind, werden in diesem Bereich die dem Verkehrsmanagement zudienenden Anlagen mitberücksichtigt (Kombinierte Anlagen, z.B. Portalrot, Kameras, Geschwindigkeitssignal usw.).

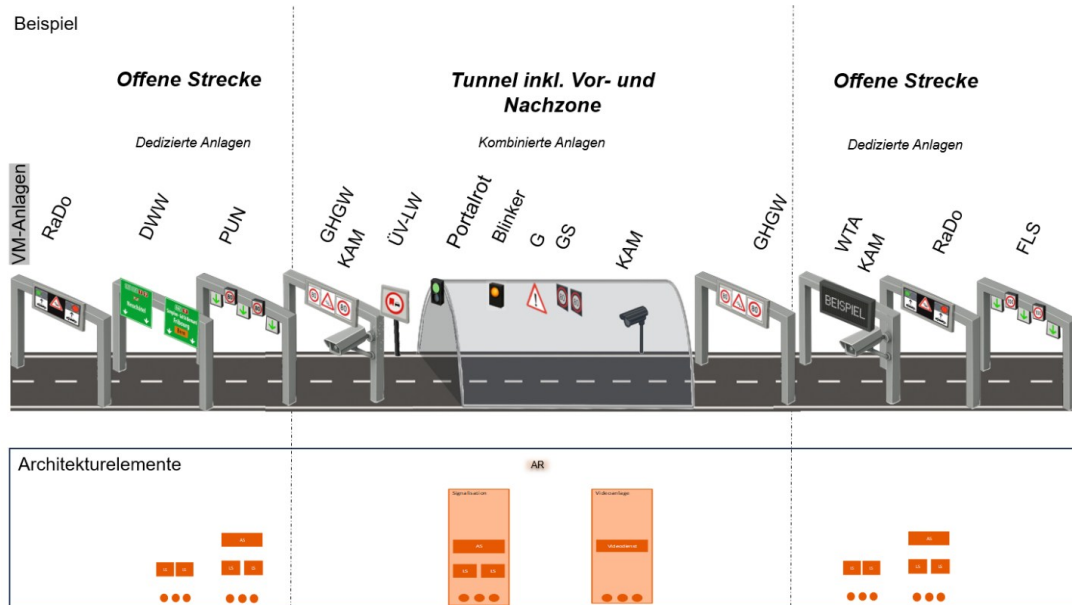


Abbildung 13: Beispiel «Dedizierte Anlagen» und «Kombinierte Anlagen»

Nachfolgend ein Beispiel GHGW mit dem Verlauf über offenen Strecken und einem Tunnel:

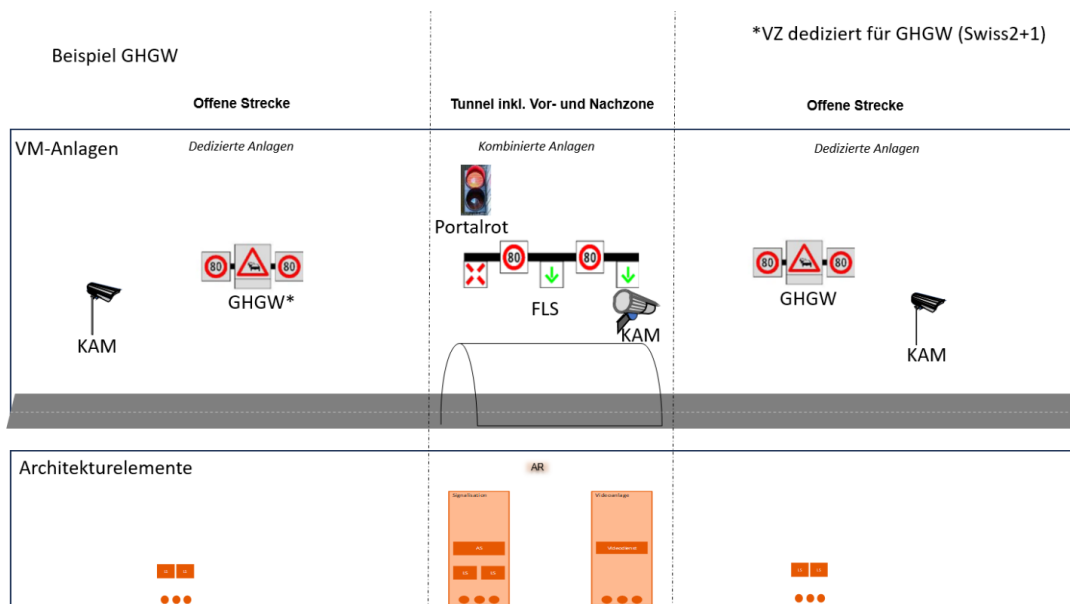


Abbildung 14: Beispiel GHGW mit «Dedizierte Anlagen» und «Kombinierte Anlagen»

## 3.5 Regionale Managementebene GE

Die regionale Managementebene GE beinhaltet die OT/BSA, welche innerhalb einer Gebietseinheit angesiedelt sind. Dazu gehören das UeLS-CH und die generellen fachspezifischen regionalen OT/BSA-Systeme.

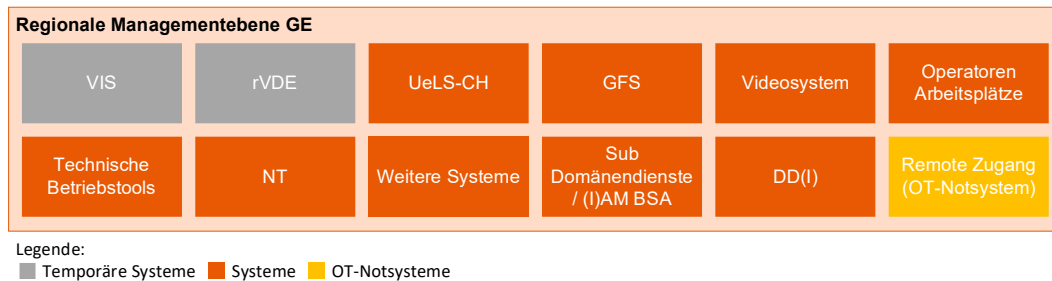


Abbildung 15: Regionale Managementebene Gebietseinheiten

### 3.5.1 Verkehrsinformationssystem (VIS)

Das Verkehrsinformationssystem (VIS) steuert und koordiniert Wechseltextanzeige (WTA) und Wechselwegweisung (WWW), die in BSA-Abschnitten ohne VR (Verkehrsrechner) zu finden sind. Die Verkehrsinformationssysteme warnen vor Verkehrsstörungen, Baustellen, aussergewöhnlichen Strassenverhältnissen oder sonstigen Gefahren auf den Nationalstrassen.

Das VIS sind eine Zwischenlösung und werden später durch die FA VL-CH abgelöst (siehe Kapitel 6 Migration).

### 3.5.2 Regionale Verkehrsdatenerfassung (rVDE)

Die regionale Verkehrsdatenerfassung oder die Zählstellencontroller (ZSC) sammeln und verarbeitet die Daten der Zählstellen und stellen sie den Fachdiensten zur Verfügung. Die ZSC sind in Abstimmung mit der IP-Netz BSA Migration abzubauen.

### 3.5.3 UeLS-CH

Das übergeordnete Leitsystem Schweiz (UeLS-CH) unterstützt die Benutzer bei der Überwachung und Steuerung der Betriebs- und Sicherheitsausrüstungen innerhalb einer Gebietseinheit. Weitere Informationen sind der ASTRA Dokumentation 83054 zu entnehmen.

Die UeLS-CH sind über das IP-Netz BSA mit den Abschnittsrechnern (AR) verbunden.

### 3.5.4 Meteoüberwachungs und -warnsystem (GFS)

Die Daten der Meteoüberwachungs und -warnsystem (auch Glatteisfrühwarnsystem genannt) auf den Nationalstrassen wird innerhalb des IP-Netz BSA verarbeitet und allen berechtigten Stakeholder zur Verfügung gestellt.

### 3.5.5 Videosystem

Das Videosystem der Regionalen Managementebene besteht aus verschiedenen Elementen und ist Teil des Videosystems VIDEO-CH. Das System ist so aufgebaut, dass ein autonomer Betrieb der Videofunktionalität innerhalb einer GE gewährleistet wird.

Das System stellt Funktionen zur Bildanalyse und Ereignisdetektion in den Objekten zur Verfügung und es werden Ringspeicher für die Videobildspeicherung bereitgestellt. Für die Bedienung der Nutzer stehen Video-Clients zur Verfügung. Sie ermöglichen den Benutzern die sofortige Steuerung von Kameras und den Zugriff auf Livebilder sowie auf aufgezeichnete Videos und Metadaten.

Die Definition und die Anforderungen zu VIDEO-CH sind der ASTRA Richtlinie 13005 zu entnehmen.



### 3.5.6 Operatoren Arbeitsplätze

Die Operatoren Arbeitsplätze dienen den Nutzern zur Überwachung, Verwaltung sowie Nutzung der Systeme. Davon sind Bundesarbeitsplätze exkludiert.

### 3.5.7 Technische Betriebstools

Die technischen Betriebstools dienen der Verwaltung und der Überwachung des IP-Netzes BSA GE sowie den Virtualisierungsumgebungen in den OT-Technikräumen und den Sicherheitselementen. Die Systeme werden hauptsächlich zur Unterstützung von Betriebsprozessen, zur Pflege des Hard- und Softwarebestands und zur Konfiguration von Systemkomponenten verwendet. Zudem sind sie wesentliche Elemente in der Störungserkennung und -behebung und dienen der Netzwerk- und Systemsicherheit.

Zu den technischen Betriebstools gehören insbesondere das Netzwerkmanagementsystem (NMS), das System für das Monitoring und Alarming und ein Ticketing-System. Die Definition und die Anforderungen zum NMS sind der ASTRA Richtlinie 13040 zu entnehmen.

### 3.5.8 Notruftelefonanlage (NT)

Die aktuellen Vorgaben sind im Fachhandbuch im Technischen Merkblatt 23 001-11650 zu finden. Eine Detaillierung dieses Aspekts erfolgt im Rahmen der Fortschreibung der Richtlinie zu einem späteren Zeitpunkt.

### 3.5.9 Weitere Systeme

Unter weitere Systeme sind regionale Systeme zu verstehen, die spezifische Fachaufgaben unterstützen.

### 3.5.10 Sub-Domänendienste / IAM BSA

Die Sub-Domänendienste beinhalten die Subdomain «ge...nationalstrassen.admin.ch» mit dem entsprechenden AD und den Diensten DNS und DHCP. Die AD wird direkt durch das IAM BSA mit den aktuellen Daten zu Usern und Usergroups versorgt.

### 3.5.11 DD(I)

Die DNS- und DHCP-Server der Gebietseinheiten werden mit den notwendigen Daten bspw. für die Namensauflösung durch das zentrale DDI versorgt. Bei einem Ausfall der zentralen Komponenten IAM BSA und DDI funktionieren die lokalen Dienste wie AD, DNS und DHCP weiterhin ohne Einschränkungen für den Tagesbetrieb.

### 3.5.12 Remote Zugang (OT-Notsysteme)

Der lokale Remote Zugang der GE dient als Notzugang bei einem Ausfall des Dienstes «Zugangsportale OT-BSA» auf der übergeordneten Ebene Basisdienste. Die Zugriffsberechtigungen sind auf das Nötige eingeschränkt, um die Sicherheit zu gewährleisten.

## 3.6 BSA-Abschnitt

Ein BSA-Abschnitt ist ein funktional abgeschlossenes Teilstück der Nationalstrasse, das Betriebs- und Sicherheitsausrüstungen umfasst. Die Ebene BSA Abschnitt ist in der Abbildung 3 in Kapitel 2.3.7 dargestellt.

### 3.6.1 Abschnittsrechner (AR)

Der Abschnittsrechner ist Teil des BSA-Abschnitts und ist die Verbindung zwischen den Anlagensteuerungen und der regionalen Managementebene. Seine Hauptaufgaben umfassen die Visualisierung des BSA-Abschnitts, die Kommunikation, die Bedienung, die Reflexbearbeitung (automatisch, halbautomatische und manuelle Reflexe) sowie die Alarm- und Meldungsverarbeitung aller ihm untergeordneter Anlagen.

### 3.6.2 Anlage- und Lokalsteuerung

Die Ebene Anlage beinhaltet die Anlagensteuerungen (AS) und Lokalsteuerungen (LS).

#### 3.6.2.1 Anlagensteuerung (AS)

Die Anlagensteuerung (AS) im BSA-Abschnitt überwacht und steuert ihre entsprechende Anlage. Sie stellt die anlagespezifische Prozesslogik und allenfalls das MMI einer Anlage zur Verfügung (Ausnahme VM-Anlagen). Folgende Anlage und Teilanlagen verfügen über eine AS.

- Energieversorgung (E);
- Beleuchtung (B);
- Lüftung (L);
- Signalisation (S), als AS-S benannt und für AS-WTA, AS-RaDo oder AS-GHGW zu verwenden;
- Bei Überwachungsanlagen (U):
  - Brandmeldeanlage Tunnel (BMT), resp. AS Rauch und AS Thermisch;
  - Videoanlagen (VMS);
  - Meteoüberwachungs und -warnsystem (GFS);
  - Warn- und Meldesystem von Naturgefahren (SLM);
  - Zentrale Einrichtung Diversanlagen (DIV);
- Bei Kommunikation & Leittechnik (KL):
  - Funkanlagen (FE via AS DIV);
  - Notruftelefon (NT).

Eine AS für Sicherheitsstollen (SISTO) ist nicht vorgesehen. Die einzelnen Teilanlagen im SISTO sind in den jeweiligen AS zu integrieren. Gegebenenfalls ist eine Integration in die AS Divers möglich.

In Ausnahmefällen können einzelne AS in die AS DIV integriert und durch diese überwacht und gesteuert werden. Die Ausnahmen sind mit dem Projektauftrag festzulegen.

Die folgende Auflistung zeigt eine Übersicht über die wichtigsten Funktionen der AS:

- Beinhaltet die Anlagenlogik, welcher Teil der Prozesslogik ist. Die Prozesslogik befindet sich auf der AS oder LS. Dies ist abhängig von der Architektur und ist projektspezifisch zu definieren;
- Stellt eine standardisierte Schnittstelle mit den vorgegebenen Datenpunkte für die Kommunikation mit dem Abschnittsrechner zur Verfügung;
- Generierung von Meldungen;
- Kommunikation mit den Lokalsteuerungen (LS);
- Austausch der Reflexe.

Die AS kommunizieren mit dem AR, sowie mit den eigenen Lokalsteuerungen (LS) und ggf. mit anderen AS (nur bei Typ 1 Reflexe).

#### 3.6.2.2 AS-Röhrentrennung

In begründeten Fällen ist eine Röhrentrennung notwendig (Komplexität, Verfügbarkeit, Migration, Umbau). Projektspezifisch kann bei röhrengetrennten Objekten die AS röhrengetrennt aufgebaut werden. Die Anlagensteuerung kann auch auf logischer Ebene eine Röhren- / Richtungstrennung berücksichtigen.

#### 3.6.2.3 Lokalsteuerung (LS)

Lokalsteuerungen überwachen oder steuern einen Anlagenteilbereich. Es kann sich sowohl um einen Teilbereich bzgl. Ausdehnung z.B. die Steuerung eines Tunnel-Teilabschnitts als auch einer Röhre oder bzgl. Funktion (Steuerung einer Teilfunktion der Anlagen) oder beidem handeln.

Die LS sind immer röhrengetrennt aufzubauen. Bei kleinen Tunnelobjekten mit einer Röhre und einer Zentrale kann die Funktion der Lokalsteuerung durch die Anlagesteuerung zu gewährleisten.

### 3.6.3 Aktoren und Sensoren

Die unterste Ebene der BSA (Feldebene) beinhalten die Aktoren und Sensoren. Diese sind fachspezifisch und sind möglichst Standardkomponenten. Beispiele: Beleuchtungskörper, Stellmotoren, Verkehrssignale, Verkehrszähler, Rauchmelder etc. Aktoren und Sensoren können auch komplexere Systeme sein. Beispiele: Türsysteme, Lüfter, WTA etc.

## 3.7 Bundessysteme

Die Bundessysteme operieren ausserhalb des Rahmens der Systemarchitektur, zum Beispiel das Datawarehouse (DWH) des ASTRA. Daher ist es erforderlich, präzise Schnittstellen festzulegen, um die Einbindung (Datentransfer unidirektional) in die Systemarchitektur zu ermöglichen.

Alle Netzübergänge von den IP-Netzen BSA GE zu den Bundessystemen und umgekehrt müssen über die Policy Enforcement Zone (PEZ) der Basisdienste ins IP-Netz BSA geführt werden.

## 3.8 Drittsysteme

Die Drittsysteme operieren ausserhalb des Rahmens der Systemarchitektur. Daher ist es erforderlich, präzise Schnittstellen inkl. klaren Verantwortlichkeiten festzulegen, um die Einbindung in die Systemarchitektur zu ermöglichen. Ein konkretes Beispiel hierfür stellt die Einbindung von Leitsystemen von externen Parteien sowie Lichtsignalanlagen von Kantonen und Gemeinden in die Systemarchitektur dar.

## 3.9 Sonderanlagen

Sonderanlagen sind Eigentum des ASTRA und werden im Normalfall ausschliesslich durch Dritte betrieben und genutzt. Je nach Situation, können diese Anlagen über das IP-Netz BSA GE mit den BSA des ASTRA verbunden werden, oder sie werden als Drittsysteme behandelt. Dies muss in den BSA Projekten jeweils festgelegt und genehmigt werden.

## 4 Leistungsanforderungen

In den nachfolgenden Subkapitel geht es um die technologische Umsetzungsmöglichkeiten, um eine möglichst hohe Betriebskontinuität als auch einen hohen Sicherheitsstandard zu erreichen. D.h. welche Technologien können unter welchen Rahmenbedingungen eingesetzt werden, um den angestrebten ununterbrochenen Betrieb zu gewährleisten.

### 4.1 Einsatz der Virtualisierung

Gemäss der Richtlinie 13009 werden in den nachfolgend beschriebenen Räumen die Unterbringung der entsprechenden Komponenten vorgesehen. Weitere Vorgaben sind in der ASTRA Richtlinie 13009 beschrieben. Ziel der Virtualisierung ist der Schutz gegen den Ausfall eines physischen Servers und Optimierung der Ressourcennutzung

#### 4.1.1 OT-Technikraum

Die Systeme der regionalen Management-Ebene werden in den OT-Technikräumen (OTTR, 2 pro GE) untergebracht. Primär sind dort Server- und Storage Systeme, teilweise ebenfalls die Backbone-Anbindung installiert.

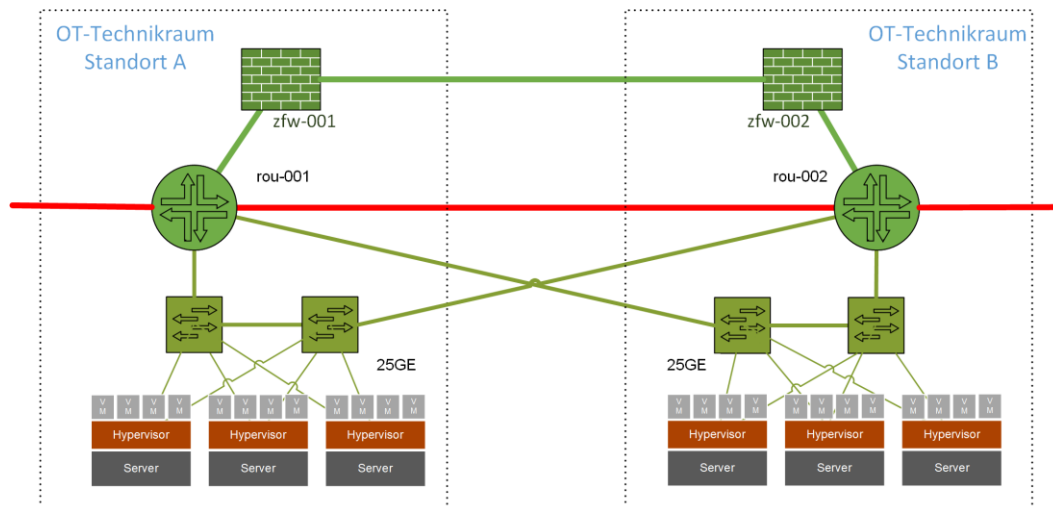


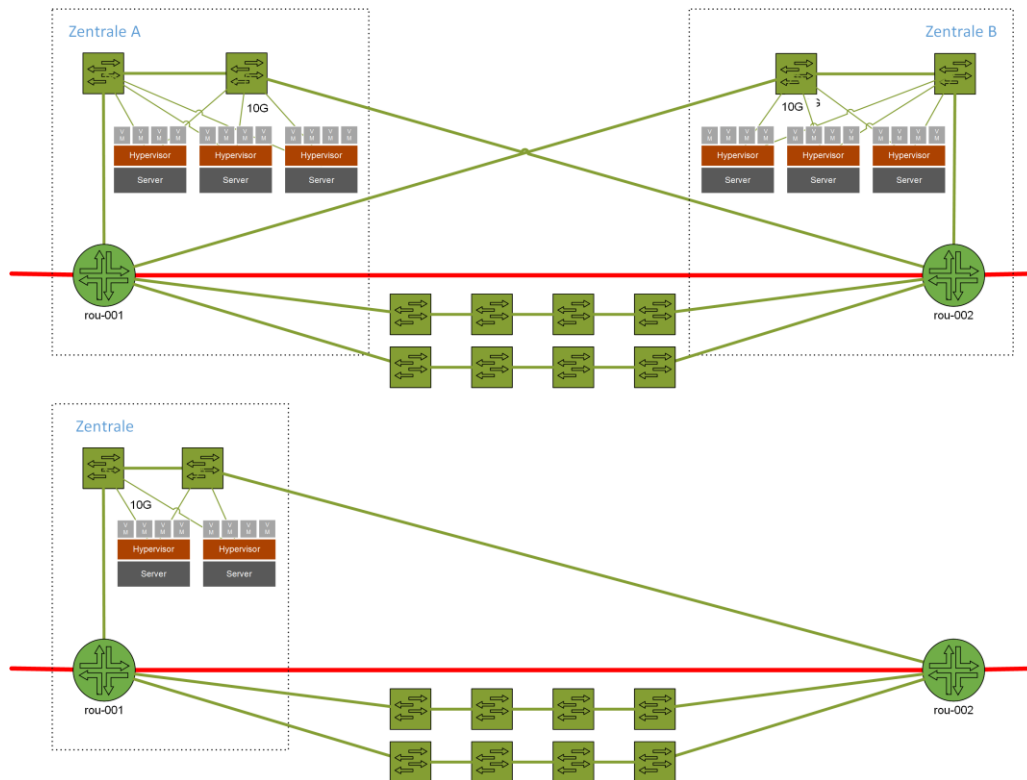
Abbildung 16: OT-Technikraum

Grundsätzlich werden in den OTTR Virtualisierungsplattformen eingesetzt. Die Virtualisierungsplattformen müssen georedundant aufgebaut werden. Die Dimensionierung ist dabei stark abhängig von den notwendigen Ressourcen. Ziel ist es, die Virtualisierungsplattformen breit zu nutzen und sämtliche virtualisierbaren Dienste und Applikationen der regionalen Management-Ebene auf diesen Plattformen aufzusetzen.

#### 4.1.2 Technikräume/Technische Zentralen

Die Technikräume/Technische Zentralen dienen primär zur Unterbringung von technischen Anlagen für die Aufrechterhaltung des Betriebes (wie Kommunikationsinfrastrukturen, Abschnittsrechnern, teilweise Anlagesteuerungen (z.B. VMS)). Dabei müssen auch hier Virtualisierungsplattformen (AR-Hosts) eingesetzt werden.

Je nach Anforderungen können diese Virtualisierungsplattformen in einer Zentrale einfach oder georedundant in zwei Zentralen ausgelegt werden. Ebenso ist die Dimensionierung der Virtualisierungsplattform stark abhängig von den notwendigen Ressourcen. Um gegen den Ausfall eines physischen Servers zu schützen, sind im Minimum zwei Server vorzusehen.



**Abbildung 17: Technikraum/Technische Zentrale**

Für die Tunnelkategorien > 600 m mit Lüftung müssen die AR und damit auch die Virtualisierungsplattformen redundant ausgelegt werden. Wenn immer möglich ist Georedundanz anzustreben. In allen anderen Fällen ist zu entscheiden, ob eine einfache Virtualisierungsplattform im Hinblick auf die Verfügbarkeit ausreicht.

## 4.2 Betriebssysteme und Redundanzen

### 4.2.1 Betriebssysteme und Virtualisierungsplattform

Aufgrund der im OT- und BSA-Umfeld vorhandener Vielzahl an eingesetzten unterschiedlichen Betriebssystemen und unterschiedlichen Generationen dieser Betriebssysteme, muss eine breite Palette an Technologien betrieben und gewartet werden können.

Durch diese breite Palette von potenziellen Guest-OS der virtuellen Maschinen (VM) muss auch die Virtualisierungsplattform ein breites Spektrum von Technologien abdecken, d.h. supporten und somit betreiben können. In diesem Bereich soll zukünftig harmonisiert und damit die Zahl der Technologien beschränkt werden. Im Speziellen sollen im Markt breit anerkannte Betriebssysteme und Datenbanken eingesetzt werden.

#### 4.2.2 Redundante AR

Für die Tunnelkategorien > 600 m mit Lüftung müssen die AR redundant ausgelegt werden. Dabei gelten folgende Vorgaben:

- Die Redundanz muss innerhalb des Objekts bzw. dem dazugehörigen IP-Abschnitt sichergestellt werden. Es ist nicht zulässig, die Redundanz mit Mitteln ausserhalb des IP-Abschnittes aufzubauen;
- Die technische Umsetzung kann mit verschiedenen Mechanismen erfolgen:
  - Applikatorisch durch die Mechanismen des AR über zwei Virtualisierungsplattformen in zwei Zentralen;
  - Nutzung der Redundanzen der Virtualisierungsplattformen. Die Hersteller dieser Plattformen bieten dazu meist plattformspezifische Möglichkeiten an (Stichwort bspw. High Availability);

- Kombinationen der beiden obigen Mechanismen.
- Der Entscheid, welche Mechanismen eingesetzt werden, ist pro Objekt bzw. IP-Abschnitt zu fällen.

### 4.2.3 AS in redundanter Ausführung

Für die Anlagensteuerungen gelten die nachfolgenden Grundsätze:

- Die AS für die Lüftungsanlage muss redundant aufgebaut werden (Steuerung);
- Die AS kann im Einzelfall redundant aufgebaut werden (Steuerung);
- Die Brandmeldeanlage Tunnel ist mit der getrennten AS Thermisch und AS Rauch (Variante 2, vgl. Anhang V, Abbildung V.9) in sich als Redundanz zu betrachten oder ist die Teilanlage Rauch in die Lüftungsanlage (Variante 3, vgl. Anhang V, Abbildung V.10) anzuordnen;
- Die AS Signalisation wird nicht redundant ausgeführt (Ausnahmen sind von der I-FU genehmigen zu lassen), aber das Portalrot muss mit Reflexen «Brand» angesteuert werden. Dazu erfolgt eine direkte Kommunikation zwischen AS BMT und LS SIG. Die Soforttaste des UeLS-CH wird nicht redundant übertragen.

Die Redundanz muss so ausgelegt werden, dass alle für den Prozess relevanten Daten immer auf beiden Steuerungen aktuell und identisch sind (Prozessabbild). Der Betriebszustand der AS wird auf beiden Steuerungen parallel und gleichwertig geführt. Der Recovery Prozess nach einer Umschaltung vom aktiven AS zum passiven AS muss ohne Datenverlust möglich sein und darf nicht zu einer automatischen «Rückschaltung» führen. Reflexe werden nur von der aktiven AS ausgeführt. Stehen nach einer Umschaltung ein oder mehrere Reflexe an, so wird der höchstwertige Reflex ausgeführt. Die Netzwerkanforderungen für den Datenaustausch müssen über das bestehende IP-Netzwerk bzw. IP-Netz BSA möglich sein.

Die Kommunikation zum AR und zu den LS ist jederzeit gewährleistet, wobei der AR immer über die aktive AS kommuniziert. Der Redundanzzustand der AS wird dem AR über Datenpunkte mitgeteilt (Aktiv/Passiv, Verfügbar). Es darf nur jeweils eine AS aktiv sein. Sind beide aktiv, so wird über die System- oder Serviceüberwachung AR - AS die effektiv Aktive ermittelt. Sind beide AS aktiv und beide System- oder Serviceüberwachungen verfügbar, so wird die normalerweise als aktiv gekennzeichnete AS zur Kommunikation verwendet. Die beschriebene Lösung ist in etwa der Applikationsredundanz im AR gleichzusetzen.

Auf Ebene Anlage werden die Hochverfügbarkeitslösungen der eingesetzten Steuerungen verwendet. Durch den Einsatz der vorgegebenen Kommunikationsarten (vgl. Kapitel 5.10) ist dies ohne weiterführende Konsequenzen möglich.

## 4.3 Virtualisierungsanwendung

### 4.3.1 Autonomie und Rückfallebenen

Um den 7x24 Stunden-Betrieb zu gewährleisten, muss gemäss Kapitel 5.8 die Autonomie im Objekt berücksichtigt werden. D.h. innerhalb des IP-Abschnitts (welches je nach Definition mehrere BSA-Abschnitte beinhalten kann, oft bei «offener Steck» müssen die Systeme (egal ob physisch oder virtuell) installiert sein. Die Autonomie der einzelnen Ebenen muss gewährleistet sein, es ist somit keine Abhängigkeit von höheren Ebenen zugelassen.

Die Rückfallebenen in Bezug auf Steuerung und Bedienung gewährleisten bei Teilausfällen den Weiterbetrieb (siehe Kapitel 5.6). Hierzu sind unterschiedliche Ebenen definiert, von der Managementebene bis hin zum AR.

Die Thematik der anlage- und objektgebunden Autonomie wird später im Rahmen der Funktionalen Anforderungen (siehe Kapitel 5) detailliert beschrieben.

### 4.3.2 Virtualisierung der Leit- und Steuersysteme

Der Einsatz der Virtualisierung hängt vom Einsatzgebiet und von der Zusicherung (Freigabe) des Herstellers ab und kann nachfolgender Tabelle entnommen werden:

*Tabelle 4: Einsatz der Virtualisierung in den Systemebenen der Architektur*

| Teil der BSA   | Virtualisierbar | Bemerkung  |
|--|-----------------|--|
| UeLS-CH (BL)   | Ja              | Zentralisiert in der regionalen Managementebene (in beiden OT-Technikräumen) |
| AR Host (Hardware) / Virtualisierungsplattform   | Nein            | Muss im IP-Abschnitt sein  |
| AR = Funktion Abschnittsrechner - Schnittstelle zwischen UeLS-CH (BL) und dem Abschnittsrechner (Virtuelle Applikation auf dem AR) | Ja              | Muss im IP-Abschnitt sein  |
| AR MMI   | Ja              | Muss im IP-Abschnitt sein  |
| AS (SPS inkl. Prozess-SW)  | Nein            | Muss im IP-Abschnitt sein  |
| AS (Guest-OS, z.B. VMS)  | Ja              | Muss im IP-Abschnitt sein  |
| AS MMI   | Ja              | Muss im IP-Abschnitt sein  |

### 4.3.3 Darstellung der AR-Virtualisierung (Zielfokus)

Die nachfolgende Darstellung erläutert den Zielfokus der AR-Systeme auf zwei unterschiedliche Arten.

Erste Art mit getrennten VM für AR und AR MMI:

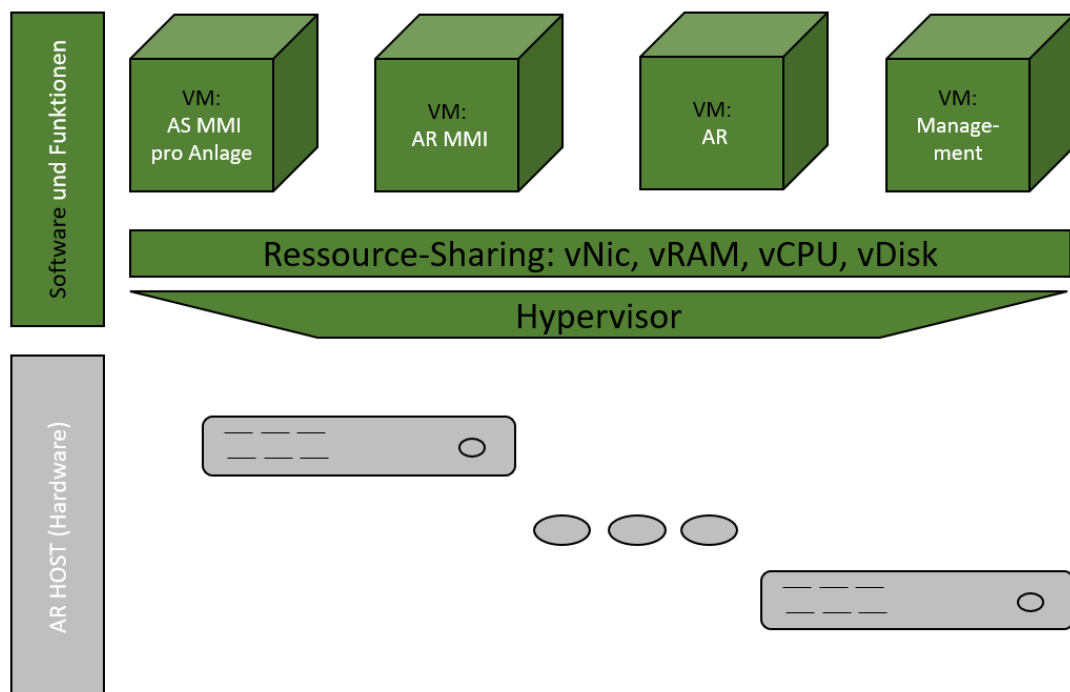


Abbildung 18: Darstellung Zielfokus AR Virtualisierung - AR, AR MMI und AS MMI auf VM getrennt

Zweite Art mit gemeinsamer VM für AR und AR MMI:

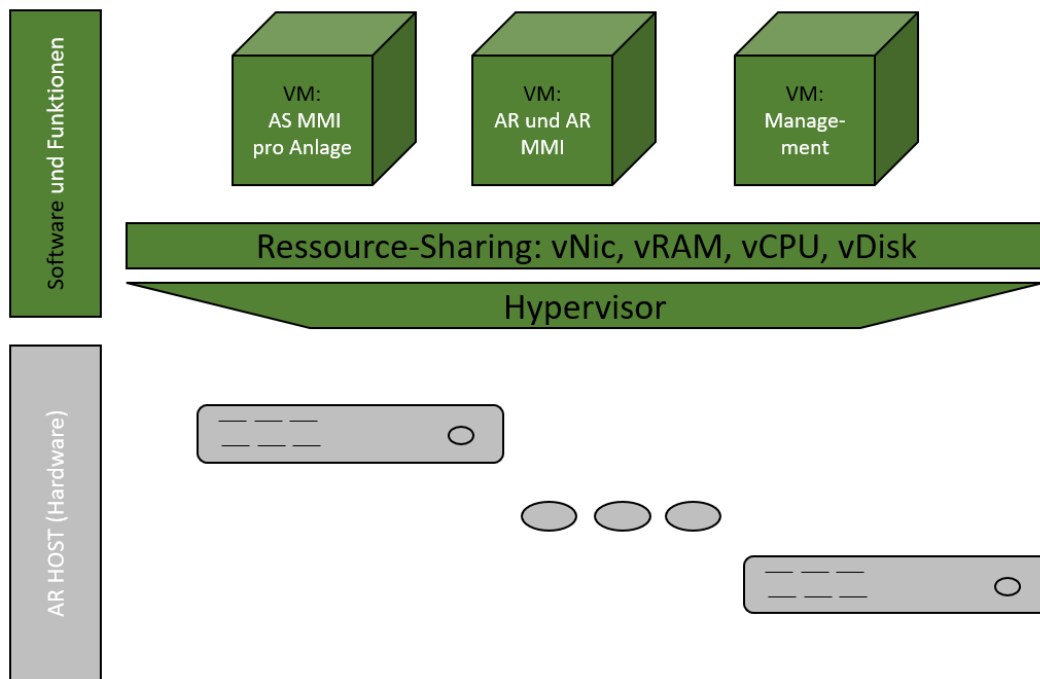


Abbildung 19: Darstellung Zielfokus AR Virtualisierung AR und AR MMI auf gemeinsamer VM

Der Zielfokus kann durch die folgenden 2 Varianten umgesetzt werden.

#### Variante 1

In dieser Umsetzungsvariante ist eine Virtualisierung nicht einsetzbar. In diesen Ausnahmefällen wird Hardware funktionsgebunden eingesetzt, d.h. Beispielsweise ein Server als AR und AR-MMI und ein separater Server für AS und AS-MMI aber die Zugriffe können von generellen Clients ausgeführt werden (nicht funktionsbezogen):

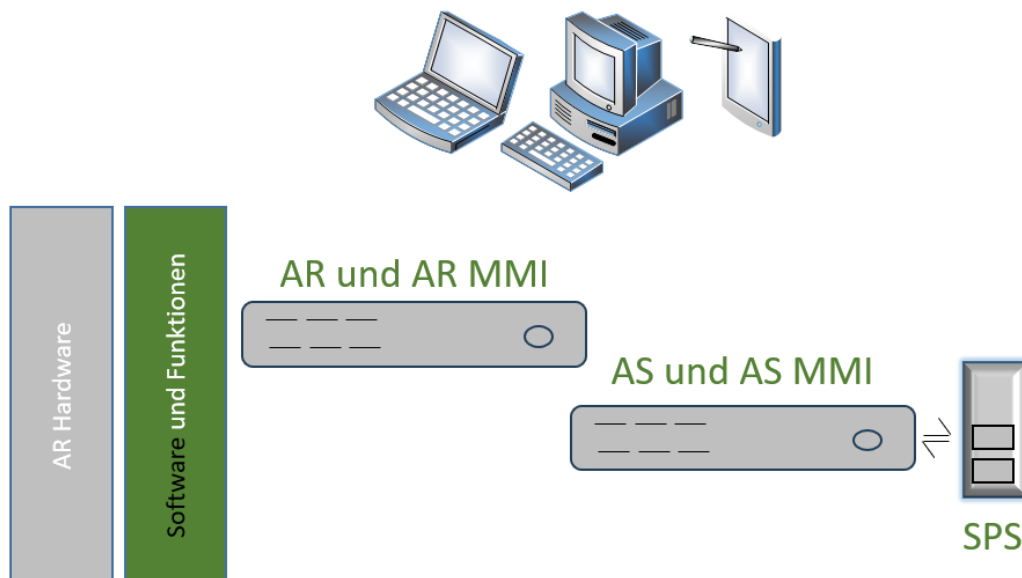


Abbildung 20: Variante 1 Darstellung für nicht virtualisierten AR (in Ausnahmefällen)



## Variante 2

In dieser Umsetzungsvariante werden AR und AR-MMI getrennt realisiert. Ebenfalls sind die AS-MMI Zugriffe nur via herstellerspezifischer (oder zertifizierter) Produkte möglich.

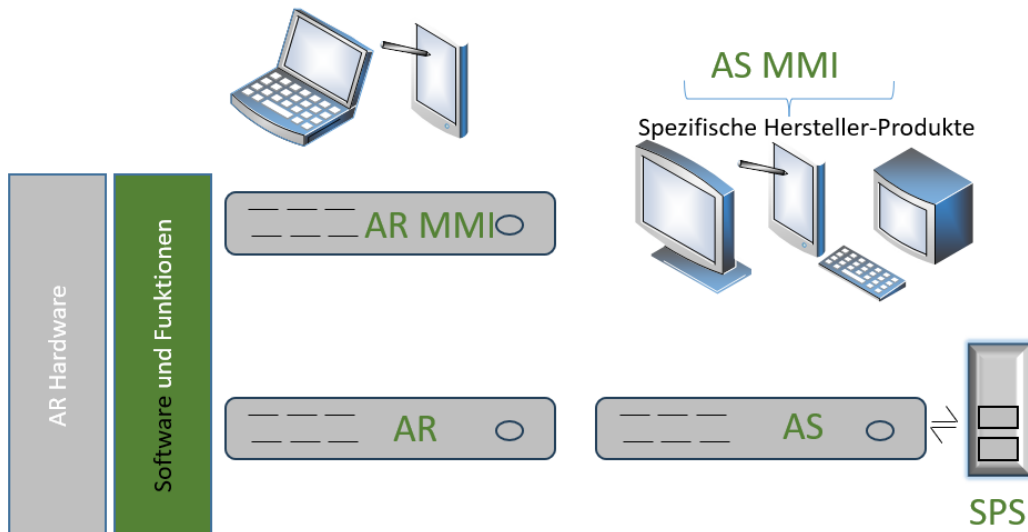


Abbildung 21: Variante 2 Zugriffselemente sind herstellerspezifisch und funktionsgebunden.

### 4.3.4 UeLS-CH (BL) im OT-Technikraum

Die UeLS-CH (BL) werden in OT-Technikräumen installiert. Diese OT-Technikräume sind georedundant auszulegen. Dies bedeutet, zwei Standorte pro GE gemäss Richtlinie 13009.

Die beiden Standorte können je nach Konzept Aktiv-Passiv, Aktiv-Aktiv oder Sonderformen davon betrieben werden. Als Grundsatz gilt: Fällt ein OT-Technikraum aus, muss der zweite vollumfänglich und möglichst unterbruchfrei übernehmen.

Für den Einsatz in diesem Bereich sind sowohl klassische Server und Storage Infrastrukturen als auch VSAN-Infrastrukturen zugelassen.

Hyperconverged Infrastructure (HCI) mit integrierten Netzwerkschwitches sind nicht zugelassen, da es der Vorgabe der Netzwerkausrüstung widerspricht. Falls zukünftig HCI-Varianten ohne integrierte Netzwerkschwitches auf dem Markt erhältlich sind, kann deren Einsatz beim CAB OT Security beantragt werden.

## 4.4 Aufbau des AR (einzelner Rechner als Beispiel)

Der Abschnittsrechner (AR) besteht aus:

- einem AR HOST (Gesamtheit des Rechners);
- mindestens einer virtuellen Maschine AR (VM AR);
- Optional zusätzliche virtuelle Maschinen vom Typ «Applikation» (VM Management).

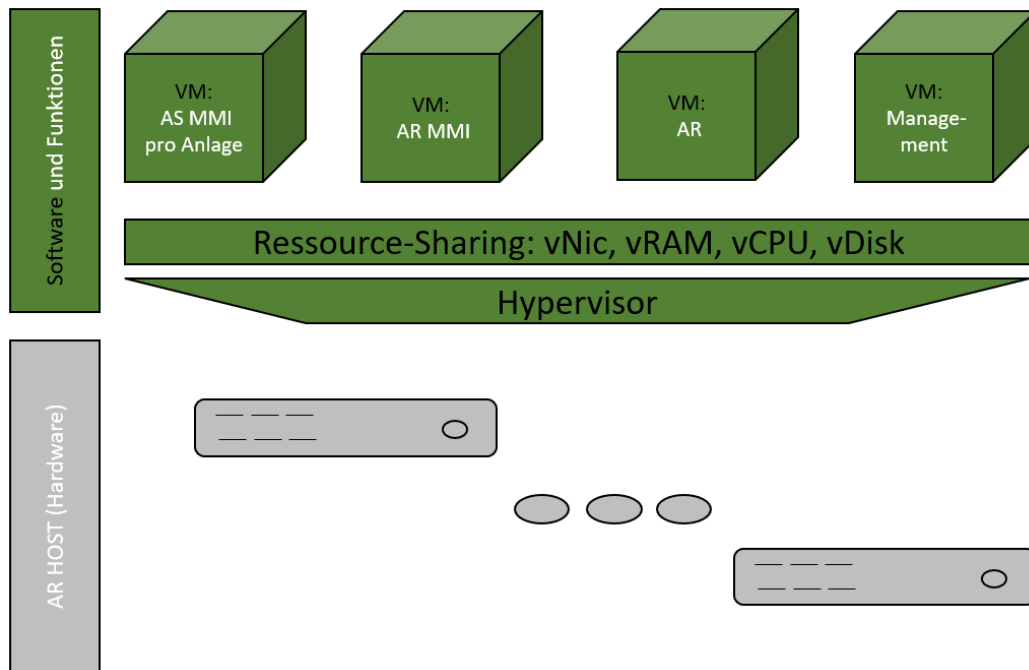


Abbildung 22: Grundaufbau eines AR Host: Trennung der Funktionen der VMs Variante 1

Auf einer VM AR sind das Betriebssystem, die Applikationssoftware und die dafür nötigen Hilfsmittel wie OPC UA Server/Client, Kommunikationstreiber etc., die Systemsoftware für Backup/Restore und weitere Hilfsmittel (z.B. externer SNMP Agent) installiert. Alle anderen Hilfsmittel für die Verwaltung, Konfiguration oder Programmierung der angeschlossenen VMs werden auf einer anderen VM oder mehreren installiert.

Auf einer VM sind das Betriebssystem und weitere optionale Software, wie z.B. die Automatisierungssoftware zur Projektierung, die Programmierungssoftware der Steuerungssysteme (AS), die Systemsoftware für Backup/Restore, die Visualisierung / Bedienung des AS, ein externer Simple Network Management Protocol (SNMP) Agent, etc. installiert. In Absprache mit den jeweiligen Herstellern lassen sich mehrere unterschiedliche Automatisierungssoftwares, Visualisierungen / Bedienungen etc. installieren. Ist dies nicht möglich, so ist eine weitere VM AP einzusetzen (Container wird nicht unterstützt).

Kombinationen, welche eine Anlage betreffen sind zugelassen, d.h. VM AR und AR MMI. Ebenfalls sind auch AS MMI auf derselben VM zugelassen, (Vgl. Abbildung 23).

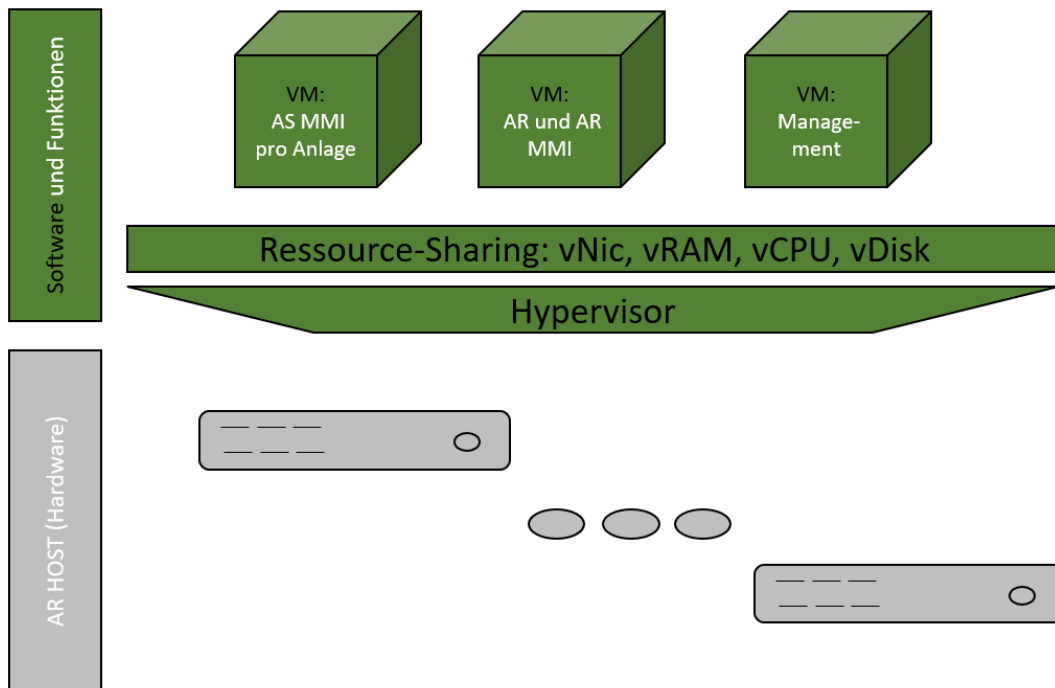


Abbildung 23: Grundaufbau eines AR Host: Trennung der Funktionen der VMs Variante 2

#### 4.4.1 WEB-Browser Kompatibilität für GUI-MMI

Die WEB-Browser Kompatibilität für GUI-MMI ist nach der ASTRA Dokumentation 83050 umzusetzen. Ausnahmen bilden herstellerspezifische standardisierte technische GUIs wie das NMS-GUI.

### 4.5 Aufbau der AS

Eine Anlagensteuerung (AS) ist pro Tunnelobjekt und Anlage einzusetzen (vgl. Kapitel 3.6.2).

#### 4.5.1 Sicherheitskritische AS (inkl. LS)

Die Anlagen BMT, Lüftung und das Portalrot gelten als sicherheitskritisch.

Die generellen Anforderungen an die AS, welche mit SPS umgesetzt werden, ist nachfolgend festgehalten.

#### 4.5.2 Anforderungen an AS (SPS)

Die eingesetzten Komponenten müssen spezifische Kriterien erfüllen. Die nachfolgenden Anforderungen sind zwingend einzuhalten.

- Betriebssystem oder Firmware:
  - muss fester Bestandteil der Hardware und in einem nichtflüchtigen Speicher gespeichert sein (persistent);
  - muss embedded sein und von einem SPS-Hersteller stammen;
  - muss ein zeitliches Verhalten garantieren (Echtzeit, Zykluszeit, Verarbeitungszeit)
  - Der Zugriff zum Betriebssystem zum Zwecke von Updates/Upgrades muss über gesonderte Programme erfolgen und bedarf dem definierten Schutz (mindestens Benutzer, Passwort und später IAM BSA). Der Zugriff kann über das Netzwerk erfolgen (Managementschnittstelle);
  - Das Betriebssystem darf nicht im Betrieb verändert werden (Neustart führt automatisch zum letzten lauffähigen Betriebssystem).
- Hardware:

- muss auf einer genormten Schiene montierbar sein oder in einem 19"-Geräteschrank integriert werden können;
- der Aufbau ist modular und kann ohne Hilfsmittel von aussen erweitert/verändert werden (z.B. Einschubkarte in Personal Computer Gehäuse ist nicht modular);
- ist lüfterlos;
- benötigt für den Betrieb keine rotierenden Teile, wie z.B. Harddisk. Die Auslagerung von nicht betriebswichtigen Daten auf rotierende Teile, wie z.B. Harddisk ist erlaubt;
- muss folgende Zulassungen und Normen erfüllen:
  - CE (Konformitätskennzeichen);
  - SN EN 61000-6-4 (EMV-Verträglichkeit);
  - SN EN 61131-2 (Anforderung für Steuerungshardware);
  - SN EN 60068 (Umgebungseinflüsse);
  - IEC 62443 (Cyber-Security);
- muss eine Betriebstemperatur im Bereich - 20 °C bis + 50 °C ohne Betauung erfüllen;
- darf keine Pufferbatterien enthalten.
- Software:
  - ist gemäss SN EN 61131 aufgebaut;
  - wird gemäss SN EN 61131 programmiert (abschliessend):
    - Funktionsbaustein (FBS);
    - Strukturierter Text (ST);
    - Kontaktplan (KoP, nur mit ausreichender Begründung);
    - Anweisungsliste (AWL, nur mit ausreichender Begründung).
- Daten/Informationen:
  - Nach einem Ausfall oder einem Neustart der Steuerung wird pro Gewerk der vordefinierte «sichere Zustand» angewendet.

Steuerungen, welche auf einem nicht eingebetteten (non-embedded) Betriebssystem mit fest einstellbarer Zykluszeit realisiert sind, werden nicht akzeptiert. Ein gängiges Beispiel hierfür ist eine «SoftSPS», wobei der Begriff «SoftSPS» in der Literatur unterschiedlich beschrieben wird. Im ASTRA wird die «SoftSPS» als eigenständiges Programm in einem nicht-realtime-fähigen Betriebssystem angenommen, z.B. in Form eines «normalen» Personal Computer als Programm, welches verschiedene Eingänge und Ausgänge bedient.

Als Programmiersprache wird «Strukturierter Text» bevorzugt (Portierbarkeit). Die Software muss zudem ausreichend dokumentiert werden (Header, Autor, Version, Kommentare). Es wird ein Namenskonzept für die einzelnen Elemente (z.B. Variablen) verwendet.

### 4.5.3 SPS

Mit dem Einsatz von Speicherprogrammierbare Steuerungen (SPS) wird die einfache Programmierung, die rasche Inbetriebnahme als auch der geringe Wartungsaufwand und die längere Nutzungsdauer erreicht. In Einzelfällen kann es sinnvoll sein, moderne SPS-Redundanzeinheiten zu prüfen. Im Regelfall ist die AS nicht redundant ausgelegt (siehe Kapitel 4.2.3).

Aktuell ist die SPS in Hardwareausführung die bevorzugte funktionale Komponente als AS.

### 4.5.4 Virtuelle SPS

Virtuelle SPS stellen einen zusätzlichen Bedarf an Softwarepflege (OS) und Malwareschutz dar. Aus diesem Grund ist der Einsatz nicht erlaubt.

### 4.5.5 IPC

Industriecomputer (IPC) auf dieser Ebene stellen einen zusätzlichen Bedarf an Softwarepflege dar, explizit das Operating System (OS) und der Malwareschutz. Aus diesem Grund wird deren Einsatz nicht empfohlen.

#### 4.5.6 MMI (GUI)

Die Bedienung der SPS kann auch mit einem dedizierten Monitor, Bedienpanel oder im AR mittels AS-MMI sichergestellt werden.

### 4.6 Aufbau der LS

Die Lokalsteuerungen (LS) sind immer röhrengetrennt aufzubauen (vgl. Kapitel 3.6.2).

#### 4.6.1 Anforderungen an LS

Die generellen Anforderungen an die LS, welche mit einer SPS umgesetzt wird, ist im Kapitel 4.5.2 festgehalten.

### 4.7 Lizenzen

Die Lizenzen müssen auf den Eigentümer (ASTRA) oder auf den Betreiber ausgestellt werden. Alle Lizenzen sowohl in papier- oder elektronischer Form sind an die von der Zentrale/Filiale oder GE vorgesehene Personen oder Gruppenmailbox zu liefern.

#### 4.7.1 Lizenzen ohne Hardwarebindung

Die Lizenzen dürfen nicht Hardwaregebunden sein, sondern müssen übertragbar sein.

Kann der Hersteller dies nicht erfüllen, muss er auf eigene Kosten die Lizenz für das Ersatzmaterial bereitstellen. Bei SPS für mindestens 10 Jahre ab Erwerb der Hardware

### 4.8 Verfügbarkeit der Elemente

Bei der Projektierung sämtlicher Architektur-Ebenen und Anlagen muss eine der im Kapitel 4.1 beschriebenen Rechnertechnologien gewählt werden. Die zu erreichende Verfügbarkeit für die gewählte Rechnertechnologie richtet sich nach den Bedürfnissen der Verfügbarkeit des Objektes (Tunnel, offene Strecke) sowie nach den Möglichkeiten der Betriebsorganisation.

#### 4.8.1 Servicezeit

Die **Servicezeit** definiert die Zeit, in welcher die Service-Erbringung vereinbart bzw. die Anlage in Funktion ist. Der Service bzw. die Anlage wird proaktiv oder reaktiv überwacht. Während der Servicezeit wird bei einem Service-Ausfall (in der Tabelle unten als Serviceunterbruch definiert) bzw. einer Anlagenstörung innerhalb der vertraglich vereinbarten Reaktionszeit ein Ticket eröffnet und unmittelbar mit der Wiederherstellung des Service bzw. der Anlage begonnen.

Die Servicezeit für sämtliche Anlagen und Services der BSA ist immer 7x24h. Es werden keine alternativen Servicezeiten definiert!

*Tabelle 5: Service Level Servicezeit*

| Service Level    | Wert             | Messmethode / Bemerkungen   |
|------------------|------------------|---|
| Servicezeit 7x24 | 7x24h (365 Tage) | <ul style="list-style-type: none"> <li>Montag – Sonntag 00:00 – 24:00 Uhr, inkl. regionale und nationale Feiertage</li> <li>keine „planned downtime“, d.h. keine periodischen Wartungsfenster mit Serviceunterbruch, nur geplante und angekündigte Wartungen</li> <li>Wartungen und Changes mit Serviceunterbruch nur nach gegenseitiger Vereinbarung</li> <li>Arbeiten mit Serviceunterbruch sind in einem speziellen Verfahren mit Einbezug der Nutzer zu bewilligen (min. 15 Arbeitstage Vorlaufzeit)</li> </ul> |

### 4.8.2 Supportzeit

Die Supportzeit ist die Zeit, während der ein Benutzer Supportleistungen (Hilfestellung bei der Nutzung eines Service) für einen Service bzw. eine Anlage erhält. Die Supportzeit kann von der Servicezeit abweichen.

Administrative Leistungen sind nicht Teil der Supportleistungen.

*Tabelle 6: Service Level Supportzeiten*

| Service Level    | Minimal-Wert | Messmethode / Bemerkungen  |
|------------------|--------------|--|
| Supportzeit 5x9  | 5x9h         | <ul style="list-style-type: none"> <li>Montag – Freitag 08:00 – 17:00 Uhr, ohne regionale und nationale Feiertage</li> </ul> |
| Supportzeit 7x24 | 7x24h        | <ul style="list-style-type: none"> <li>7 x 24 Stunden, inkl. Feiertage</li> </ul>  |

### 4.8.3 Verfügbarkeit

Die Verfügbarkeit beschreibt, wie die geforderte und vereinbarte Funktionalität zu einem bestimmten Zeitpunkt oder während einer definierten Periode zu erfüllen ist. Die Verfügbarkeit wird ausschliesslich über die **Downtime** festgelegt. Auf eine alternative Angabe über eine rechnerische prozentuale Verfügbarkeit (z.B. 99.99%) wird verzichtet.

Dabei bedeutet **Downtime** die Summe aller Service Ausfallzeiten in Stunden und Minuten innerhalb der definierten Messperiode, bei der ein Service oder eine Anlage während der vereinbarten Servicezeit nicht verfügbar und damit die minimale Funktionalität nicht gewährleistet ist. Die Service Ausfallzeit beginnt mit dem Auftreten einer Störung, d.h. Erkennung im Monitoring oder Meldung durch Nutzer und endet mit der Wiederherstellung des Service bzw. Behebung der Störung. Für Service mit reaktivem Monitoring beginnt die Service Ausfallzeit mit der Meldung des Benutzers (Ticketerstellung).

*Tabelle 7: Service Level gemessen in Downtime*

| Service Level        | Wert               | Messmethode / Bemerkungen   |
|----------------------|--------------------|---|
| Downtime 2h          | <= 2h pro Jahr     | <ul style="list-style-type: none"> <li>Nur zu erreichen mittels redundanter Systeme</li> <li>Gemessen pro Jahr und redundantem System</li> <li>Max. 1 Totalausfall pro Jahr zugelassen</li> <li>Bei Teilausfällen wird i.d.R. auf das redundante System umgeschaltet, d.h. man hat einen Redundanzverlust und keine Downtime</li> <li>Beheben Redundanzverlust &lt;24h</li> </ul> |
| Downtime 8h          | <= 8h pro Jahr     | <ul style="list-style-type: none"> <li>Gemessen pro Jahr und System</li> <li>Max. 1 Ausfall pro Jahr zugelassen</li> </ul>  |
| Downtime 12h         | <= 12h pro Quartal | <ul style="list-style-type: none"> <li>Gemessen pro Quartal und System</li> <li>Max. 1 Ausfall pro Quartal zugelassen</li> </ul>  |
| Downtime Best Effort | Keine Vorgabe      | <ul style="list-style-type: none"> <li>Ziel ist es, einen Ausfall innerhalb 24h zu beheben</li> </ul>   |

Ein Redundanzverlust gilt nicht als Serviceausfall, muss jedoch innerhalb 24h nach Bekanntwerden behoben werden (Eröffnung eines Tickets).

Die folgende Tabelle gibt praxisgerechte Werte, die als Basis für die Wahl der Rechner-technologie dienen, sowie für die Bestimmung der Anforderungen an die Technik und an den Betrieb der BSA helfen sollen. Diese Werte können für die Service Level Agreement (SLA) herangezogen werden.

Tabelle 8: Standardverfügbarkeit gemessen in Downtime

| System / Anlage  | SLA                    | Verfügbarkeit  | Technologie / Architektur  |
|--|------------------------|--|--|
| Management-<br>ebene<br>inklusive FA   | <b>Downtime<br/>2h</b> | <= 2h pro Jahr, max. 1<br>Ausfall pro Jahr zuge-<br>lassen, beheben Re-<br>dundanzverlust <24h | <ul style="list-style-type: none"> <li>HA-Cluster (mindestens 3 Rechner)</li> <li>Zusätzliche Applikationsredun-<br/>danz über zwei georedundante<br/>Standorte</li> </ul>   |
| IP-Netz BSA<br>Backbone An-<br>schluss GE (Rou-<br>ter und BB-FW)                | <b>Downtime<br/>2h</b> | <= 2h pro Jahr, max. 1<br>Ausfall pro Jahr zuge-<br>lassen, beheben Re-<br>dundanzverlust <24h | <ul style="list-style-type: none"> <li>Georedundanter Anschluss an<br/>den Backbone IP-Netz BSA</li> </ul>   |
| IP-Netz BSA Er-<br>schliessungsgringe<br>inkl. netznahe<br>Dienste (Nukleus)     | <b>Downtime<br/>2h</b> | <= 2h pro Jahr, max. 1<br>Ausfall pro Jahr zuge-<br>lassen, beheben Re-<br>dundanzverlust <24h | <ul style="list-style-type: none"> <li>Pro Abschnitt zwei Erschlies-<br/>sungsringrouter an zwei ge-<br/>trennten Zentralen oder Tech-<br/>nikräumen</li> <li>Georedundante Wegführung<br/>der Erschliessungsringe</li> <li>Netznahe Dienste georedu-<br/>dant aufgebaut in den beiden<br/>OTTR</li> </ul> |
| rVL, VL,<br>andere überregio-<br>nale Elemente<br>(temporär, Über-<br>gangszeit) | <b>Downtime<br/>8h</b> | <= 8h pro Jahr, max. 1<br>Ausfall pro Jahr zuge-<br>lassen                                     | <ul style="list-style-type: none"> <li>SPS oder 2-Rechner Hardware,<br/>Failover-Cluster</li> </ul>  |
| UeLS-CH  | <b>Downtime<br/>2h</b> | <= 2h pro Jahr, max. 1<br>Ausfall pro Jahr zuge-<br>lassen, beheben Re-<br>dundanzverlust <24h | <ul style="list-style-type: none"> <li>HA-Cluster (mindestens 3<br/>Rechner pro Standort)</li> <li>Zusätzliche Applikationsredun-<br/>danz über zwei OT-Technik-<br/>räume</li> </ul>  |
| Abschnittsrechner<br>(Host)  | <b>Downtime<br/>2h</b> | <= 2h pro Jahr, max. 1<br>Ausfall pro Jahr zuge-<br>lassen, beheben Re-<br>dundanzverlust <24h | <ul style="list-style-type: none"> <li>HA-Cluster (mindestens 2<br/>Rechner pro Standort)</li> <li>Zusätzliche Applikationsredun-<br/>danz über zwei technische Zent-<br/>ralen</li> </ul>   |
| Anlagesteuerung<br>(Nicht sicher-<br>heitskritische Sys-<br>teme)                | <b>Downtime<br/>8h</b> | <= 8h pro Jahr, max. 1<br>Ausfall pro Jahr zuge-<br>lassen                                     | <ul style="list-style-type: none"> <li>SPS</li> </ul>  |
| Anlagesteuerung<br>(Sicherheitskriti-<br>sche Systeme)                           | <b>Downtime<br/>2h</b> | <= 2h pro Jahr, max. 1<br>Ausfall pro Jahr zuge-<br>lassen, beheben Re-<br>dundanzverlust <24h | <ul style="list-style-type: none"> <li>SPS redundant</li> </ul>  |
| Lokalsteuerung<br>(Nicht sicher-<br>heitskritische Sys-<br>teme)                 | <b>Downtime<br/>8h</b> | <= 8h pro Jahr, max. 1<br>Ausfall pro Jahr zuge-<br>lassen                                     | <ul style="list-style-type: none"> <li>SPS</li> </ul>  |
| Lokalsteuerung (z.<br>B. sicherheitskriti-<br>sche Systeme)                      | <b>Downtime<br/>2h</b> | <= 2h pro Jahr, max. 1<br>Ausfall pro Jahr zuge-<br>lassen, beheben Re-<br>dundanzverlust <24h | <ul style="list-style-type: none"> <li>SPS redundant (siehe BMT Va-<br/>rianten)</li> </ul>  |

## 4.9 Anlagespezifische Anwendung der Technologien

Auf Stufe des OT-Technikraumes lassen sich Funktionen regional zentralisieren, welche eine regionale und somit flächendeckende Bedeutung haben (GUI/MMI- oder Tools, Fachdienste und Fachapplikationen):

Applikationen und Tools:

- UeLS-CH;
- Sub-Domänendienste;
- (i)AM BSA;
- DD(I);
- Remote Zugang / Wartung;
- Technische Betriebstools (wie NMS usw.);
- Weitere Systeme (wie Ticketingsystem usw.);
- GFS;
- VIS (temporär, Übergangszeit);
- rVDE (temporär, Übergangszeit);
- rVL (temporär, Übergangszeit);
- VR (temporär, Übergangszeit).

Nachfolgende Teilanlagen beziehungsweise deren Teilfunktionen gehören ebenfalls zu dieser Kategorie:

*Tabelle 9: Teilanlagen und deren Teilfunktionen*

| AKS-Bez. | Bezeichnung Anlage / Teilanlage           | Explizite Funktionen                                |
|----------|---|---|
| ZES      | Zentrale Einrichtung - Signalisation      | VL-CH   |
| VMS      | Videoanlage                               | Regionale Funktionen                                |
| FE       | Funksystem (Radio, Einsprechung, Polycom) | Einsprechung  |
| NT       | Notruftelefon                             |   |
| TTZ      | Tür / Tor / Zutrittskontrolle             | Berechtigung elektronischer Schlüsselprogrammierung |

Falls sinnvoll kann das Management – und (ausschliesslich dieses) - weiterer Teil- und Anlagen regional zentralisiert werden. Dies bedarf jedoch einer vorgängigen Bestätigung des Herstellers.

### 4.9.1 Einsatz Verfügbarkeitsfunktionen im OT-Technikraum

Auf dieser Ebene sind die in der Virtualisierungsplattform enthaltenen Funktionen Fault-Tolerance oder High Availability bei den VM (Guest-OS) sowie die Redundanzfunktionen gemäss Kapitel 4.2 zulässig.

Die nachfolgenden MMI- oder Tools der Anlagen/Teilanlagen sind bis auf Stufe AR-Funktion virtualisierbar (nicht aber auf der Stufe AS oder LS).

*Tabelle 10: Übersicht Virtualisierung der Teilanlage*

| AKS-Bez. | Bezeichnung Anlage / Teilanlage    | Explizite Funktionen |
|----------|------------------------------------|----------------------|
| NST      | Notstrom                           |                      |
| ZEB      | Zentrale Einrichtung - Beleuchtung |                      |
| DB       | Durchfahrtsbeleuchtung             |                      |



Tabelle 10: Übersicht Virtualisierung der Teilanlage

| AKS-Bez.  | Bezeichnung Anlage / Teilanlage                    | Explizite Funktionen  |
|-----------|--|---|
| BN        | Brandnotbeleuchtung                                |   |
| FWB       | Fluchtwegbeleuchtung                               |   |
| ZEL       | Zentrale Einrichtung - Lüftung                     |   |
| AL        | Abluft   |   |
| LL        | Längslüftung                                       |   |
| ZL        | Zuluft   |   |
| FWL       | Fluchtwegbelüftung                                 |   |
| ZES       | Zentrale Einrichtung - Signalisation               | Tunnel AS   |
| VM        | VM-System  |   |
| LSA       | Lichtsignalanlage                                  |   |
| SER       | Sicherheitseinrichtung                             |   |
| BMT       | Brandmeldeanlage Tunnel                            |   |
| VTV / VMS | Videoanlage  | <ul style="list-style-type: none"> <li>• Ausnahmefälle im Objekt für ED</li> <li>• Bildspeicherung (Ring-speicher)</li> </ul> |
| IPE       | Kommunikationsnetzwerk IP-Netz Erschlies-sungsring |   |
| IPA       | Kommunikationsnetzwerk IP-Netz Access-Bereich      |   |
| LTA       | Leittechnik Abschnitt                              |   |
| FE        | Funksystem (Radio, Einsprechung, Polycom)          | Radio und Polycom   |
| NT        | Notruftelefon                                      | Feuerlöscher/Alarmkästen in Diversanlage und löst Reflex aus  |
| RI        | Hausinstallation                                   |   |
| HLK       | Heizung, Lüftung, Klima                            |   |
| BMG       | Brandmeldeanlage Gebäude                           |   |
| POR       | Pumpwerk   |   |
| LOE       | Löscheinrichtung                                   |   |
| WV        | Wasserversorgung                                   |   |
| SAA       | Strassenabwasserbehandlungsanlage                  |   |

#### 4.9.2 Einsatz Verfügbarkeitsfunktionen AR

Auf dieser Ebene sind die in der Virtualisierungsplattform enthaltenen Funktionen Fault-Tolerance oder High Availability bei den VM (Guest-OS) sowie die Redundanzfunktionen (siehe Kapitel 4.3) zulässig.

#### 4.9.3 Einsatz Verfügbarkeitsfunktionen AS/LS

Es sind für die Einhaltung der geforderten Redundanzen Hot- oder Cold-Standby Systeme bereitzustellen.

## 4.10 Konsolidierung der unterschiedlichen Anlagefunktionen auf der Virtualisierungsplattform

Im OT-Technikraum oder in den technischen Zentralen werden die vorhandenen Ressourcen bestmöglich genutzt und gleichzeitig die Verfügbarkeit erhöht. Dabei ist die entsprechend korrekte Dimensionierung aus dem Anhang V.3 Rechner-Hardware und Datenspeicher-Hardware zu berücksichtigen.

Die nachfolgende Darstellung zeigt die Konsolidierung in einem Objekt:

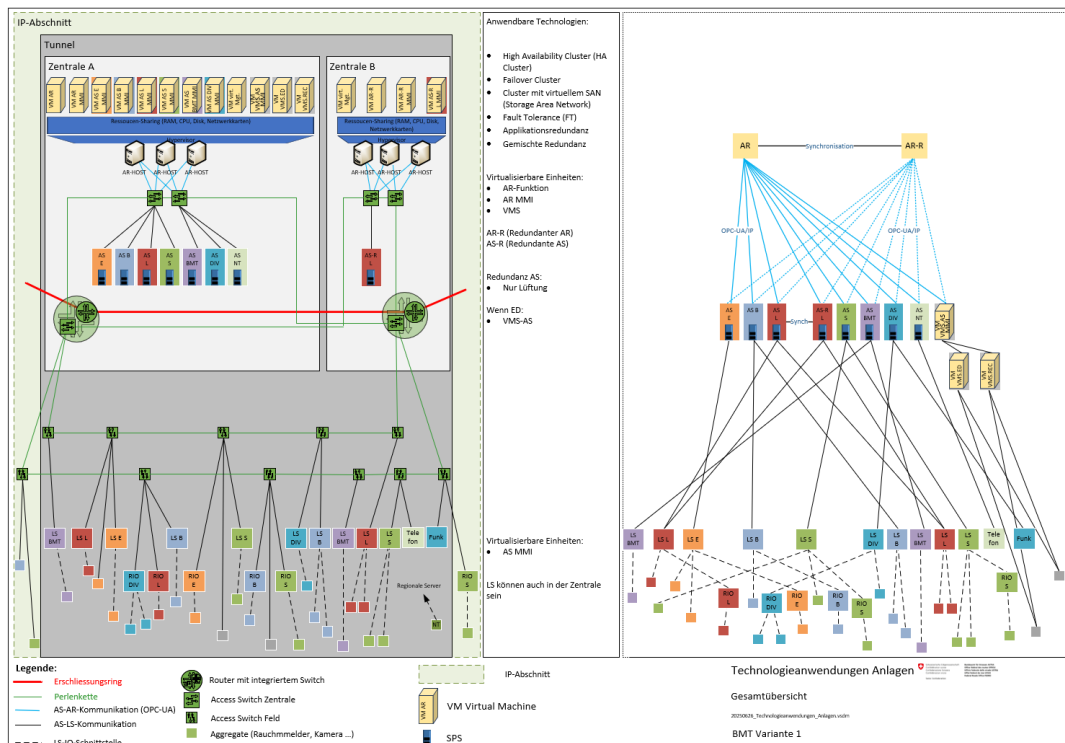


Abbildung 24: Darstellung der Technologieanwendung (einer Röhre)

Die in der Darstellung enthaltenen Farben kennzeichnen die gesamte Anlage (nicht die Unternehmer).

Die Darstellung der Technologieanwendung für eine oder zwei Röhren sind im Anhang V.1 und V.2 verfügbar. Diese beiden Varianten sind ebenfalls anlagenspezifisch dargestellt.

### 4.10.1 OT-Technikraum (zwei Standorte pro GE in einem oder zwei dedizierten IP-Abschnitten)

In diesem Teil ist die höchste Dichte an Konsolidierung (D.h. alle virtuellen Systeme werden auf derselben HOST installiert) gefordert.

### 4.10.2 Technikräume (zwei Standorte innerhalb des IP-Abschnitts)

In den Technikräumen wird gemäss Kapitel 4.9 Anlagenspezifische Anwendung der Technologien konsolidiert. Alles, was gemäss diesem Kapitel virtualisiert werden darf, wird auf derselben Virtualisierungsplattform (siehe Kapitel 4.2.1, besteht aus mehreren Rechner-Hardware-Sets) installiert.

Falls ein Gewerk aus belegbaren Gründen trotz Freigabe zur Virtualisierung getrennte Server nutzen will/muss, wird dies durch die I-FU geprüft/bewilligt werden. Es sind für die Einhaltung der geforderten Redundanzen Hot- oder Cold-Standby Systeme bereitzustellen (falls diese nicht virtualisiert sind, ansonsten gelten die Vorgaben von Kapitel 4.2 und 4.3).

#### 4.10.2.1 Objektgebunden Autonomie

Um eine möglichst hohe Betriebsverfügbarkeit zu erhalten, werden die für den Betrieb sicherheitsrelevanten Anlagen in unterschiedlichen Betriebsszenarien im Kapitel 5.6 aufgeführt. In diesem Kapitel wird beschrieben, wie die Grundsätze für die Betriebsszenarien definiert sind. Der Betrieb muss jederzeit gewährleistet sein, daher gilt es mehrere Rückfallebenen umzusetzen, obwohl in den unterschiedlichen Stufen nicht eine vollumfängliche Funktion zur Verfügung steht.

Betrieb- und sicherheitsrelevante Anlagen müssen inkl. der Fähigkeit zum Management/Steuerung im jeweiligen Objekt zur Verfügung stehen (dies kann unter Umständen eine manuelle Steuerung vor Ort sein). D.h. diese Einheiten können nicht regional zentralisiert werden, da bei einem Ausfall der regionalen Managementebene oder beim Teilausfall des IP-Netz BSA zwischen dem Objekt und den OT-Technikräumen die Betriebsfähigkeit gestört wäre. In einem solchen Fall ist auch die Alarmierung nicht mehr gewährleistet, was eine Bedienung vor Ort im Tunnel erforderlich machen würde und nicht zu bewältigen wäre.

#### 4.10.2.2 Anforderungen Wiederherstellungszeiten

In der ASTRA Dokumentation 86053 sind die Wiederherstellungszeiten definiert, wobei hier vermerkt ist, dass dies der maximale Fall ist und eine kürzere Wiederbereitschaft anzustreben ist. Anhand der Minimalanforderungen bestimmen die Gebietseinheiten die nötige Ersatzteil-Haltung, welche an Lager sein muss.

In Abstimmung zu den jeweiligen Minimalanforderungen der jeweiligen Gewerke ist die Verfügbarkeit der Systemarchitektur entsprechend zu wählen. Bei konsolidierungsfähigen Elementen gemäss 4.9 wird der OTTR oder AR-Host entsprechend der höchsten Anforderung dimensioniert.

#### 4.10.3 Anforderungen Wartung- und Supportgewährleistung (SLA)

Um die definierten Verfügbarkeiten einzuhalten sind Service-Level-Agreements (SLA) inkl. den Rückversicherungsthemen wie Herstellerwartung, Integrationspartnersupportverträge im Rahmen der Zielerreichung durch die verantwortlichen Stellen (je nach Themengebiet: Zentrale, Filiale oder GE) abzuschliessen.

### 4.11 Datenhaltung

Im Normalfall werden die Rohdaten für die gesetzlich definierten Zeiträume gespeichert. Da mit Ausnahme vom IAM BSA (Teil Identity) keine Personendaten verarbeitet werden und auch keine Datenablage in das Geschäftsverwaltungssystem (GEVER) erfolgt, wird der Umgang wie folgt definiert:

Es werden ausschliesslich Rohdaten (strukturiert oder unstrukturiert) langfristig gespeichert. Ausnahme sind bereits auf dem Sensor/Aktor prozessual bearbeitete Daten.

Weiterverarbeitete Rohdaten, welche beispielsweise angereichert oder aggregiert wurden, werden nicht gespeichert, da diese reproduzierbar sind. Ausgenommen hiervon sind die Speicherungen im endgültigen Format der Publikation, dies erfolgt jedoch meistens ausserhalb der OT in der IT-Infrastruktur.

In nachfolgender Tabelle sind die minimalen und/oder maximalen Aufbewahrungszeiträume für «nicht Personendaten» aufgeführt:

Tabelle 11: Life-Cycle von «nicht Personendaten»

| Datenebene  | Rohdaten/Datenbanken  | Logfiles                    |
|---|---|-----------------------------|
| IP-Netz BSA<br>Systeme Bund<br>Drittssysteme  | Keine   | >= 12 Monate<br>< 24 Monate |
| Regionale Managementebene<br>Basisdienste / Zentrale<br>Dienste<br>Managementebene<br>Verkehrsmanagementebene<br>Verkehrsregion | *Tagesbackup: >= 7 Tage<br>*Wochenbackup: >= 4 Wochen<br>*Monatsbackup: >= 3 Monate<br>*Jahresbackup: nach Bedarf<br>Informationen der VM-Anlagen: 10 Jahre | >= 12 Monate<br>< 24 Monate |

\*Je nach Backupsoftware werden unterschiedliche Sicherungstypen und -mechanismen umgesetzt. Diese Tabelle dient der Orientierung und muss gemäss Kapitel 4.12.5 umgesetzt werden.

Auf Managementebene können längere fachapplikationsspezifische Aufbewahrungszeiten definiert sein, welcher der Fachapplikationsanbieter sicherstellen muss.

Im Falle eines Vorfalls werden die betroffenen Daten zusätzlich gemäss Anweisung in einem separaten Speicher kopiert.

Für die BSA Systeme von LS über AS zu AR gelten separate Bestimmungen gemäss den Vorgaben der Gewerke.

#### 4.11.1 Eigentums- und Nutzungsrecht

Die Datenhoheit über jegliche Daten liegt beim Bundesamt für Strassen ASTRA.

Das Bundesamt für Strassen ASTRA hat die uneingeschränkten Nutzungsrechte an allen Daten.

Die Nutzung der Daten durch den Lieferanten muss offengelegt werden. Die Weitergabe der Daten an Dritte ist untersagt.

#### 4.11.2 Software und Anwendungsprogramm

Es gelten für den gesamten Lifecycle von Software und Anwendungsprogrammen die AGB<sup>1</sup> des Bundes.

### 4.12 Nachvollziehbarkeit

Es muss jederzeit möglich sein, Nachforschungen beziehungsweise Audits zu den Systemen und Ereignissen vollziehen zu können. Dazu gehören Bedien-Tätigkeiten und automatisch generierte Meldungen der Anlagen. Details zur Nachvollziehbarkeit finden sich in der ASTRA Richtlinie 13030. Es gibt unterschiedliche Einstufungen der Daten und Informationen. Die Details sind in der ASTRA Dokumentation 83042 enthalten.

#### 4.12.1 Logging

In jedem der Teilnetze (IP-Netz BSA BD, VMZ und aller GEs) muss ein zentrales Logging-System installiert werden. Die nachfolgende Auflistung beschreibt, welche Daten und Informationen gespeichert werden müssen aufgrund der Security und Nachvollziehbarkeit. Innerhalb der BSA (AR bis LS) ist dies auf dieser Ebene zu regeln.

<sup>1</sup> Link zur AGB: AGB des Bundes (admin.ch)

#### 4.12.1.1 Technische Ereignisse

Speicherung sämtlicher technischer Ereignisse wie beispielsweise Systemlogs welche ereignisorientiert erstellt worden sind

#### 4.12.1.2 Logfiles

Die Logfiles dürfen nicht verändert werden können (Schreibgeschützte Speicherung, aber nicht revisionssichere Anforderung).

#### 4.12.2 System Protokollierung

Jedes System muss in seinem Perimeter eine vollständige Protokollierung beinhalten.

#### 4.12.3 Datenhierarchie und -aggregation

In der ASTRA Richtlinie 13032 ist die Datenpyramide ersichtlich. Diese stellt die Informationsverschlinkung von der Feldebene bis zur regionalen Managementebene dar. Nur Daten, welche für die nächsthöhere Ebene relevant sind, werden übermittelt. Es gilt somit das Prinzip der Datenkommunikationsreduktion vom Aggregat bis hin zur Managementebene. Fachspezifische Aggregationen werden in den Fachdiensten oder Fachapplikationen bearbeitet. Ausnahmen bilden einzelne AS, welche diese Funktion direkt übernehmen.

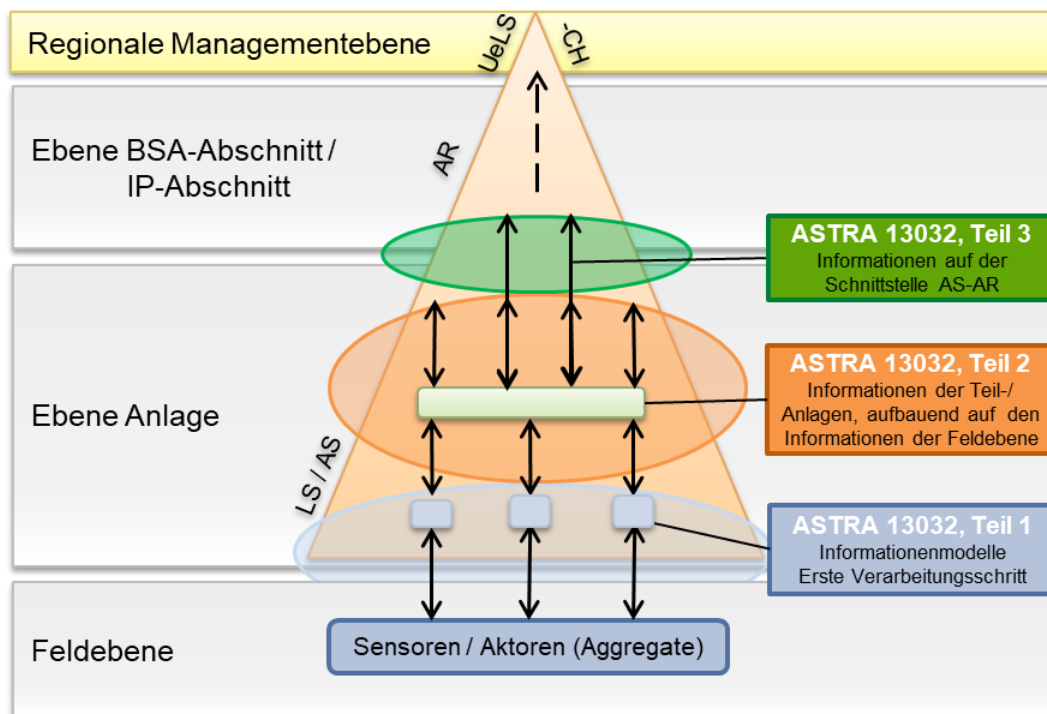


Abbildung 25: Datenpyramide

#### 4.12.4 Archivierung

Unter digitaler Archivierung versteht man das langfristige-, systematische und kontrollierte Aufbewahren von Daten in elektronischer Form. Dabei unterscheidet man zwischen:

- nicht revisionssicherer Archivierung (Langzeitsicherung) und;
- revisionssicherer Archivierung.

Im Bereich der BSA ist in der Regel keine revisionssichere Archivierung notwendig. Falls trotzdem der Fall eintreten sollte, dass man ausgewählte Daten bspw. aufgrund von Rechtsstreitigkeiten revisionssicher ablegen müsste, so wird dies via GEVER vorgenommen. Es werden keine anderen revisionssicheren Archive im Bereich der BSA geführt.

- Langzeitsicherung:

Für die Langzeitsicherung (Archivierung nicht revisionssicher) gelten die Vorgaben aus der Tabelle Kapitel 4.11. Für den Umgang mit Personendaten ist das Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) massgeblich. Nach Ablauf der Archivierungsdauer sind die Daten zu löschen.

#### 4.12.5 Backup und Recovery

Grundsätzlich gelten die Vorgaben aus der ASTRA Richtlinie 13030, GS-7 und GS-8. Zusätzlich einige Bemerkungen:

- Die eingesetzten Produkte für Backup & Recovery müssen eine äusserst umfangreiche Funktionalität für physische als auch virtuelle Sicherungen in unterschiedlichen Umgebungen bewerkstelligen. Es müssen sowohl alte als auch neue Systeme gesichert werden können, die mehr als 3 Generationen auseinanderliegen. Ein Multi-OS-Support und unterschiedlichste Datenbanken müssen gesichert werden;
- Ein klares Backup- und Recovery-Konzept muss durch die GE erstellt werden und nach Prüfung von I-FU/I-B umgesetzt werden. Dabei sind die Minimalanforderungen aus Kapitel 4.11 zu erfüllen;
- Ein zentral beschafftes Produkt steht bei Bedarf zur Verfügung. Ebenfalls können Beispielkonzepte angefragt werden;
- Als Backupmedium gelten: Backup2Disk (Speicherbereich muss von normalen Speicherbereich getrennt sein und offline gesetzt werden können) bspw. ein NAS;
- Nicht zugelassene Speichermedien sind: Externe Festplatten, USB-Laufwerke, DVD usw.

#### 4.13 Zeitsynchronisation

In der ASTRA Dokumentation 83044 «Zeit- und Taktverteilung IP-Netz BSA» ist detailliert beschrieben, wie die Systemzeit aller Komponenten, basierend auf der vereinheitlichten ATOM-Uhr, sichergestellt wird, damit die Datenintegrität zum Thema Zeitstempel jederzeit gewährleistet ist.

#### 4.14 Reporting

Basierend auf den Rohinformationen/-daten werden Weiterverarbeitungen zu unterschiedlichen Zwecken bewerkstelligt. Um Aggregationen oder Informationsanreicherungen (z.B. aus anderen Systemen) umzusetzen, werden unterschiedliche Formen des Reporting eingesetzt. Einige Systeme verfügen selbst über Reportingfunktionen, welche genutzt werden können. Für weiterführende Auswertungen oder falls keine Reportingfunktion vorhanden ist, kann ein solcher Dienst eingeführt werden (Siehe Kapitel 5.5).

Es werden keine Rohdaten oder Daten mit Rückerkennungsmöglichkeit ausserhalb des IP-Netz BSA transportiert (Datenschutz).

#### 4.15 OT Security

##### 4.15.1 Weisungen 73006

Die ASTRA Weisungen 73006 beinhalten das Regelwerk der Steuer- und Leittechnik der BSA (OT-Systeme). Sie enthalten:

- Die Ziele der OT Security Governance (siehe Kap. 4.1);
- Die verschiedenen Grundbausteine, um die strategische, funktionale und operative Ebene zu unterstützen;
- Regeln: Prozesse, Rollen und Organisation;
- Mensch: Mitarbeiterqualifikationen und -ausbildung;
- Technologie: Technische Vorgaben;
- Die Differenzierung zwischen IT und OT auf den Nationalstrassen (siehe Kap. 3.1);
- Die wichtigsten Gremien der OT-Sicherheitsorganisation (siehe Kap. 5.4).

#### 4.15.2 Richtlinie 13030

Die ASTRA Richtlinie 13030 legt Anforderungen und Massnahmen zum Schutz von Elementen der Betriebs- und Sicherheitsausrüstungen (BSA) unter Zuhilfenahme von OT-Mitteln fest, um die Sicherheit in genügendem Masse zu gewährleisten.

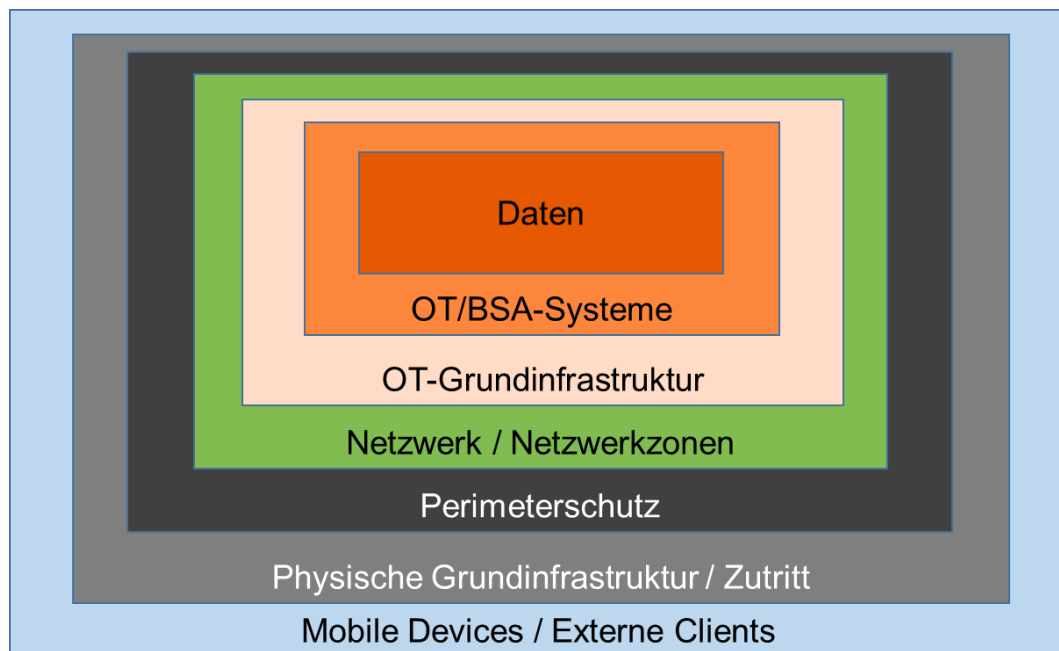


Abbildung 26: Prinzip der mehrschichtigen Security-Anforderungen / Massnahmen – «Defense-in-Depth»-Prinzip

#### 4.15.3 Dokumentation 83042

Die ASTRA Dokumentation 83042 bildet die Grundlage für die Netzwerksicherheit. Dazu legt sie Standards fest und definiert folgende Aspekte:

- sie definiert gemeinsame Begriffe;
- sie definiert das Zonenmodell und regelt die Minimalanforderungen an die Netzwerkzonen und deren Betrieb;
- sie regelt Minimalanforderungen an Netzwerkübergänge zwischen Netzwerkzonen innerhalb einer Gebietseinheit (IP-Netz BSA GE) und zwischen Zonenübergängen zu anderen Gebietseinheiten, der VMZ-CH, den Basisdiensten, den RZ BSA oder externen Netzwerken;
- sie regelt die Minimalanforderungen an Systeme, die an das Netzwerk angeschlossen werden dürfen.

#### 4.15.4 Dokumentation 83056

Die ASTRA Dokumentation 83056 beschreibt die spezifischen Vorgaben des Identitäts- und Accessmanagement inkl. den Zugangsportalen im Wirkungssperimeter der Nationalstrassen-Domäne beschrieben werden.

#### 4.15.5 Fachhandbuch 23001-11880 physische OT Security und Richtlinie 13009

Im Technischen Merkblatt 23001-11880 zur physischen OT Security ist beschrieben, wie die Infrastruktur mit OT-Kommunikationseinrichtungen des ASTRA (OT-Technikräume, Technikräume für den Betrieb der OT-Infrastruktur, die Normschränke, Kabinen, Anschlussdosen und -kästen) geschützt wird.

In diesem «Technischen Merkblatt» (TM) werden die Raumtypen und die Mindestvorgaben zum physischen Schutz der OT-Infrastruktur beschrieben. Diese Vorgaben werden in die Richtlinie 13009 überführt und das TM wird entfernt werden.

## 5 Funktionale Anforderungen

Im folgenden Kapitel werden die funktionalen Anforderungen an die SA-CH beschrieben.

### 5.1 Zugriff

#### 5.1.1 Nutzergruppen

In den Nutzergruppen sind die Nutzer Gebietseinheitsmitarbeiter, Externe Mitarbeiter, Bundesmitarbeiter inkl. ASTRA-Mitarbeiter vorgesehen. Die Anforderungen sind durch das IAM BSA vorgegeben.

#### 5.1.2 Benutzerrollen

Die Benutzerrollen mit ihrem Berechtigungskonzept sind in den ASTRA Weisungen 73002 beschrieben. Es sind sowohl Grob- als auch Feinrollen vorgesehen, welche in der ASTRA Dokumentation 83056 geregelt sind.

### 5.2 Benutzerschnittstellen

#### 5.2.1 Visualisierungsprinzip

Die Visualisierung des **UeLS-CH** mittels MMI hat immer auf dem UeLS-CH Rechner zu erfolgen.

Das MMI für einen BSA-Abschnitt befindet sich auf dem **Abschnittsrechner (AR)**. Somit werden relevanten Anlagenbilder in ihrer Detaildarstellung auf dem AR generiert und gespeichert.

Für die Visualisierung der **Anlagensteuerung (AS)** ist eine der drei Prinzipien zu wählen, die nachfolgend aufgeführt sind. Die Auswahl erfolgt projektspezifisch und richtet sich nach der technischen Machbarkeit sowie den Anforderungen zu Verfügbarkeit und Autonomie aus der vorliegenden Richtlinie:



Tabelle 12: Visualisierungsprinzipien

|                  |  |
|------------------|--|
| <b>Prinzip 1</b> | Hier sind das MMI und der Rechner (SPS) voneinander getrennt. Für die AS wird eine SPS verwendet. Das MMI für die AS ist als VM auf dem AR-Host virtualisiert. Dadurch ist es möglich, gleichzeitig mehrere MMI VMs auf einem Hardware-Set (AR-Host) laufen zu lassen. Jedoch ist bei einem Ausfall des AR-Host ohne Redundanz die Bedienung der AS über das AS MMI nicht mehr gewährleistet. Die Prozesse in der AS laufen in einem solchen Fall jedoch weiter. |
| <b>Prinzip 2</b> | Hier sind das MMI und der Rechner (SPS) voneinander getrennt. Für die AS werden SPS verwendet. Das MMI für die AS ist ein Teil der AR MMI. Bei einem Ausfall des AR-Host ohne Redundanz ist die Bedienung der AS über das AR/AS MMI nicht mehr gewährleistet. Die Prozesse in der AS laufen in einem solchen Fall jedoch weiter.   |
| <b>Prinzip 3</b> | Die AS ist eine SPS (gemäß 4.5.5) oder auf einem separaten Rechner installiert. Das AS MMI und die Prozesse sind nicht auf derselben Hardware. Bei einem Ausfall des AR-Host ohne Redundanz kann die AS und die Bedienung weiter funktionieren.  |

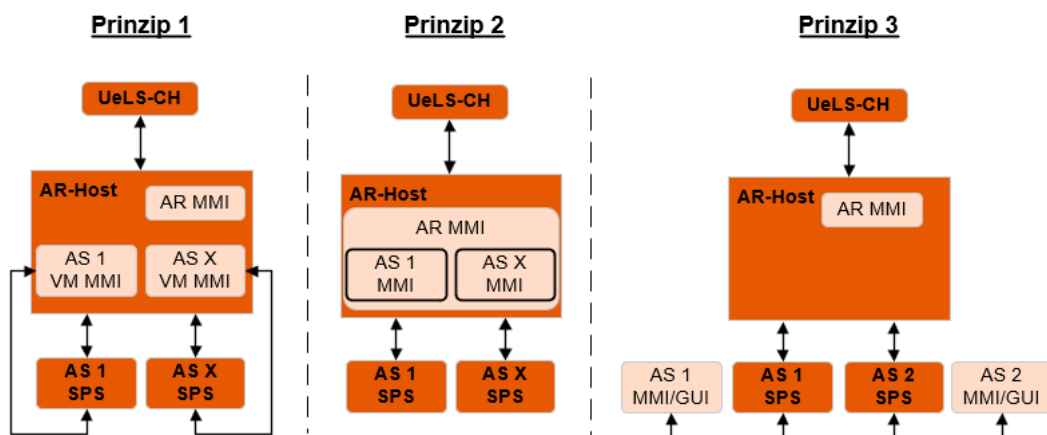


Abbildung 27: Visualisierungsprinzipien

## 5.2.2 Bedienmöglichkeiten

Die nachstehende Tabelle zeigt die zulässigen Bedienmöglichkeiten. Dabei sind die Bedienmöglichkeiten in der UeLS-CH/Betriebsleitreechner (BL) und vor Ort (Technikräume/Technische Zentralen) zu differenzieren. Weiter sind die Voraussetzungen für den Zugriff gemäss ASTRA Richtlinie 13030 zu erfüllen.

*Tabelle 13: Bedienmöglichkeiten*

| Ebene:                                 | Element-gruppe               | Element oder Komponente | UeLS-CH   | Bedienmöglichkeiten: vor Ort   |
|--|------------------------------|-------------------------|---|--|
| <b>Applikationsebene</b>               | Fachapplikationen (FA VM/BM) |                         | Applikationsabhängig                            | n/a  |
| <b>Fachdienstebene</b>                 | Fachdienste                  |                         | Applikationsabhängig                            | n/a  |
| <b>OT-Management</b>                   | OT-Management-Dienste        |                         | Applikationsabhängig                            | n/a  |
| <b>OT-Dienste</b>                      | OT-Dienste                   |                         | Applikationsabhängig                            | n/a  |
| <b>Verkehrsmangementebene (VMZ-CH)</b> | Systeme                      | VMS-B                   | Applikationsabhängig                            | n/a  |
| <b>Verkehrsregionen</b>                |                              | rVL oder VL             | Arbeitsplatz<br>Webzugriff / Client-Applikation | • Operatoren Arbeitsplätze   |
| <b>Regionale Managementebene</b>       | Systeme                      | UeLS-CH und VMS-B       | MMI / GUI (Vgl. 5.2.3)                          | • Webzugriff   |
| <b>BSA-Abschnitt</b>                   | Systeme                      | AR                      | MMI (Weboberfläche)                             | <ul style="list-style-type: none"> <li>• Webzugriff</li> <li>• Netzwerk bekanntes Gerät</li> <li>• Möglichkeit zum Stellen der Betriebs- und Steuerungsart</li> <li>• Notzugang per Jumphost</li> </ul>  |
|  | Systeme                      | AS (SPS)                | MMI (Weboberfläche)                             | <ul style="list-style-type: none"> <li>• Netzwerk bekanntes Gerät</li> <li>• Möglichkeit zum Stellen der Betriebs- und Steuerungsart</li> <li>• Notzugang per Jumphost</li> <li>• Keine Bedienpanels, falls notwendig sind diese im Projekt zu definieren (MP, DP)</li> </ul>            |
|  | Systeme, Aktoren / Sensoren  | LS (SPS)                | Allenfalls MMI (Web-oberfläche)                 | <ul style="list-style-type: none"> <li>• Netzwerk bekanntes Gerät</li> <li>• Möglichkeit zum Stellen der Betriebs- und Steuerungsart</li> <li>• Allenfalls Notzugang per Jumphost</li> <li>• Keine Bedienpanels, falls notwendig sind diese im Projekt zu definieren (MP, DP)</li> </ul> |

### 5.2.3 Benutzeroberflächen

Die Benutzeroberflächen der Fachapplikationen sind gemäss den Styleguides des ASTRA Dokumentationen 83050 bis 83052 sowie der ASTRA Weisung 73002 zu gestalten. Diese werden MMI genannt.

Bei Standardkomponenten und Standard-Tools, wie z.B. NMS, die mehrheitlich von den Administratoren und nicht von den Operatoren genutzt werden, kann von dem Style Guide abgewichen werden. Diese werden GUI genannt.

Die Umsetzung bzw. Anwendung von MMI und GUI ist im Anhang I.2 ersichtlich.

## 5.3 Steuerung

### 5.3.1 Betriebsarten

Die Betriebsarten regeln die Bedienhandlungen der Benutzer und den Datenaustausch zwischen den verschiedenen Ebenen der Systemarchitektur der regionalen Managementebene, Region, Abschnitt, Anlage und Feldebene.

Hinsichtlich der Bedienung, welche über das MMI erfolgt, wird die Betriebsart gewählt. Das Ändern der Betriebsart kann nur im entsprechenden MMI durchgeführt werden (Bsp: Lokal AS = Änderung im AS-MMI). Wie der Zugriff auf das entsprechende MMI erfolgt (z. Bsp: per Browser), spielt für die Betriebsart keine Rolle.

Hinweis: Die grundsätzlichen Benutzerberechtigungen sind nicht in den Betriebsarten, sondern in der Benutzerverwaltung, bzw. Führung geregelt. Nur berechtigte Benutzer können die Betriebsarten ändern.

Es werden die folgenden Betriebsarten für BSA-Anlagen unterschieden:

*Tabelle 14: Betriebsarten*

|                |   |
|----------------|---|
| <b>Fern</b>    | In der Betriebsart „Fern“ werden aktuelle Betriebsdaten an die nächsthöhere Ebene gemeldet und alle Befehle von der nächsthöheren Ebene entgegengenommen.   |
| <b>Lokal</b>   | In der Betriebsart „Lokal“ werden aktuelle Betriebsdaten an die nächsthöhere Ebene gemeldet, aber keine Bedienbefehle von Benutzern der nächsthöheren Ebene entgegengenommen. Befehle und Vorgaben des Steuerungsprozesses der nächsthöheren Ebene werden jedoch übernommen. Alle Reflexe werden abgesetzt oder empfangen und die entsprechenden Reaktionen werden ausgelöst. |
| <b>Wartung</b> | In der Betriebsart „Wartung“ werden keine Betriebsdaten an die nächsthöhere Ebene gemeldet und keine Befehle der nächsthöheren Ebene entgegengenommen. Alle Komponenten in der Betriebsart «Wartung» sind vom Anlagenprozess isoliert. Es werden keine Reflexe abgesetzt oder empfangen. Die entsprechenden Reaktionen werden nicht ausgelöst.                                |

Die nachstehende Tabelle legt fest, welche Betriebsarten auf welcher Ebene realisiert werden müssen und welche ebenenspezifischen Anforderungen sind.

| <i>Tabelle 15: Betriebsarten ebenenspezifisch</i> |   |       |         |
|---|---|-------|---------|
| Systeme & Aggregate                               | Betriebsarten   |       |         |
|   | Fern  | Lokal | Wartung |
| <b>UeLS-CH</b>                                    | Die Betriebsarten regeln im BSA-Umfeld die Beziehungen zur jeweils nächsthöheren Ebene. Die UeLS-CH stellen in der BSA-Systemarchitektur die oberste Hierarchiestufe dar. Daher existiert im Sinne der Betriebsarten keine nächsthöhere Ebene und die UeLS-CH kennen daher keine Betriebsarten, gemäss der Definition.  |       |         |
| <b>AR</b>   | ✓   | ✓     |         |
|   | Für den AR macht die Betriebsart «Wartung» funktionell keinen Sinn. Sie existiert daher nicht. Die funktionelle Umsetzung der Betriebsarten «Fern» und «Lokal» ist gemäss Tabelle 13 definiert.   |       |         |
| <b>AS / LS</b>                                    | ✓   | ✓     | ✓       |
|   | Für die AS / LS können alle drei Betriebsarten Sinn machen. Die Funktionelle Umsetzung der Betriebsarten ist gemäss Tabelle 13 definiert.<br>Verriegelungen dienen zum Schutz von Personen, Sachen und Umwelt. Diese sind projektspezifisch zu realisieren.   |       |         |
| <b>Feld (Aktoren, Sensoren)</b>                   | Es werden keine Betriebsarten unterschieden.<br>Bedienbare Aktoren und Sensoren können per Noteingriffsmöglichkeit bedient werden. Diese Möglichkeit erlaubt die direkte manuelle Kontrolle von Einzelaktoren oder Aktorengruppen vor Ort. Die Steuerung der betroffenen Komponenten ab AS respektive LS wird ausser Kraft gesetzt.<br>Verriegelungen dienen zum Schutz von Personen, Sachgütern und Umwelt. Diese sind projektspezifisch zu realisieren. |       |         |

Sämtliche, von «Fern» abweichenden Betriebsarten und Noteingriffe müssen auf allen darüberliegenden Ebenen visualisiert werden.

Die ASTRA Richtlinien 15010 «Betriebszustände – Verkehrssteuerung» und 15019 «Verkehrstechnische Regelungslogik - Funktionale Minimalanforderungen für Planung und Betrieb der Regelung von Verkehrsmanagement-Systemen zur Verflüssigung des Verkehrs» beschreiben die Betriebsarten der Verkehrsmanagement-Anlagen (VM-Anlagen). Die Betriebsarten der BSA-Anlagen entsprechen gemäss der nachfolgenden Tabelle den Betriebsarten der VM-Anlagen:

| <i>Tabelle 16: BSA-Anlagen &amp; VM-Anlagen</i> |  |
|---|--|
| BSA-Anlagen<br>(Richtlinie 13031)               | VM-Anlagen<br>(Richtlinie 15010 und 15019)     |
| Fern  | Normalbetrieb                                  |
| Lokal   | Lokal-Betrieb                                  |
| Wartung   | -  |
| -   | Simulationsbetrieb                             |
| -   | Autark-Betrieb                                 |
| -   | Signalbild Dunkel<br>(entspricht Blindbetrieb) |

### 5.3.2 Steuerungsarten

Die Steuerungsarten beeinflussen den Zustand der Aggregate einer BSA.

Es sind folgende Steuerungsarten in Bezug auf die Aggregate und Funktionen zu unterscheiden:

- Automatik (gesteuert durch die Prozesslogik der Anlage);
- manuell (gesteuert/bedient durch einen Benutzer).

Es gibt optional folgende Steuerungsart in Bezug auf die Ebene der Anlagen und nicht Aggregate:

- Programme (Optional, gesteuert durch einen definierten Ablauf; diese zählen zur Steuerungsart automatisch).

Die Steuerungsarten schliessen sich gegenseitig aus. Jedes Aggregat kann sich zu einem bestimmten Zeitpunkt nur in einer Steuerungsart befinden. Die Steuerungsarten «Programme» (optional) und «manuell» haben gegenüber der Steuerungsart «Automatik» grundsätzlich immer die höhere Priorität.

*Tabelle 17: Steuerungsarten*

|                            |  |
|----------------------------|--|
| <b>Automatik</b>           | In der Steuerungsart «Automatik» folgt der Anlagen-Prozess den Informationen, die er von seinen angekoppelten Sensoren, oder von, auf anderen BSA laufenden, Prozessen erhält. Er steuert die Aktoren der Anlage basierend auf diesen Vorgaben. Diese Steuerungsart beeinflusst alle Aggregate der Anlage und stellt den Normalfall dar.   |
| <b>Manuell</b>             | In der Steuerungsart «Manuell» folgt der Anlagen-Prozess den Vorgaben einer manuellen Steuerung durch die Benutzer, unabhängig von den gelieferten Werten einer Steuergrösse. Er steuert die Aktoren basierend anhand der manuellen Vorgabe. Diese Steuerungsart beeinflusst <u>einzelne</u> Aggregate oder Teilanlagen. Nicht beeinflusste Aggregate wechseln ihre Steuerungsart nicht. Automatik wird durch die Benutzer geschaltet.<br><br>Bei manueller Steuerung muss die jeweils übergeordnete Steuerung prüfen, ob die Schaltungen zulässig sind. Unzulässige Schaltungen dürfen ohne entsprechende Hinweise und andere geeignete Massnahmen nicht ausgeführt werden. |
| <b>Programm (Optional)</b> | In der Steuerungsart «Programm» folgt der Anlagen-Prozess einem vorgegebenen Ablauf, unabhängig von den gelieferten Werten einer Steuergrösse. Die Aktoren werden anhand des im Programm definierten Ablaufs gesteuert. Diese Steuerungsart kann die gesamte Anlage beeinflussen oder bestimmte Teilanlagen und steuert somit <u>alle</u> Aggregate der Anlage oder der beeinflussten Teilanlagen. Nicht beeinflusste Aggregate wechseln ihre Steuerungsart nicht. Programme können durch Benutzer geschaltet werden, oder werden automatisch ausgelöst (Reflexe, Zeitfunktionen, etc.)  |

Sämtliche, von «Automatik» abweichenden Steuerungsarten müssen auf allen Ebenen visualisiert werden.

### 5.3.3 Funktionen

Die nachfolgenden Funktionen stehen in allen Betriebsarten zur Verfügung.

#### 5.3.3.1 Testfunktionen

Für Test- und Inbetriebnahmen bei Neuanlagen, bei Ersatz oder bei zu wiederholenden Tests im Rahmen des betrieblichen Unterhalts (z.B. IGT vergleiche ASTRA Richtlinie 13028) werden unterschiedliche Testfunktionen zur Verfügung gestellt.

Folgende Testfunktionen sind vorzusehen:

- **Forcieren:**  
Diese Funktion ermöglicht das Forcieren (auch Simulation genannt) von Werten (Messwerte usw.) und damit den Test der Steuerungsfunktionen. Der BSA-Prozess berücksichtigt in diesem Zustand den eingegebenen Ersatzwert für die Steuerung der Anlage. Der Originalwert der Sensorik wird nicht berücksichtigt.
- **Anlagentest:**  
Meldungen werden an spezifische Testbenutzer und nicht an die Operatoren weitergeleitet. Dies wird durch spezifische Benutzergruppen geregelt.
- **Reflexauslösung:**  
Sämtliche Reflexe können quell- und senken-seitig einzeln ausgelöst werden.
- **Blind- und Dunkelbetrieb:**  
Für Tests der Signalisationsanlagen können Dunkelschaltungen oder Blindbetrieb vorgesehen werden, um den Verkehr nicht unnötig zu beeinflussen und keine unsicheren Zustände zu erzeugen.

Sämtliche Testfunktionen müssen auf allen Ebenen visualisiert werden.

#### 5.3.3.2 Unterdrückungsfunktionen

Es existieren verschiedene Unterdrückungsfunktionen für unterschiedliche Anwendungsfälle. Je nach Funktion bezieht sich die Unterdrückung auf den AR, die AS, LS oder die Aggregate. Die Unterdrückung ist permanent. Weil auch sicherheitsrelevante Meldungen beeinflusst werden können, ist die Unterdrückung mit der nötigen Vorsicht anzuwenden.

- **Meldungsunterdrückung:**  
Sämtliche Alarm- und Störungsmeldungen können unterdrückt werden, um den Betrieb trotz technischer Störungen aufrecht zu erhalten.
- **Reflexunterdrückung:**  
Sämtliche Reflexe können quell- und senken-seitig unterdrückt werden.
- **Inaktivschaltung:**  
Diese Funktion ermöglicht es Sensoren inaktiv zu schalten. Die Steuerung berücksichtigt den betroffenen Sensor nicht.

Eine Datenpunkt-Unterdrückung muss visualisiert werden und in der Alarm-/Meldeliste aufgeführt werden.

Für das Verkehrsmanagement (Anlage Signalisation), ist die Unterdrückung als Passivierung aufgeführt. Siehe ASTRA Richtlinie 15019 für mehr Details.

#### 5.3.3.3 Verriegelung

Verriegelungen zur Verhinderung von unzulässigen Zuständen, Handlungen oder Aktionen (z.B. bei der Lüftung, Signalisation, Energieversorgung) können durch Hardware oder Software realisiert werden und sind fach-/ projektspezifisch zu bestimmen.

## 5.4 Monitoring

Der OT-Management Dienst «Service Monitoring» überwacht sämtliche Systeme der Management- und Basisdienstebene. Die Anlagen, welche über das UeLS-CH gemanagt werden, überwachen sich selbst. Die Überwachung verläuft von top down. Das UeLS-CH erhält alle Störungsmeldungen.

## 5.5 Reporting

Mittels Reporting wird die Sichtbarkeit von relevanten Daten und Informationen ermöglicht, was die Grundlagen für Führungs- und Entscheidungsprozesse gewährleistet. Es wird in unterschiedlichen Bereichen und Themengebieten ein Reporting implementiert werden. Diese Vorgaben werden nach Erstellung den Verantwortlichen mitgeteilt.

Die Aggregierung der Informationen erfolgt gemäss dem Prinzip der Datenpyramide. D.h. beispielsweise werden das Reporting der Regionalen Managementebene in der Basisdienstebene aggregiert und zur Weiterverarbeitung bereitgestellt.

Das Schlüsselreporting im Bereich der Security wird bis ins ASTRA ISMS (Information Security Management System) aggregiert werden.

Die wichtigsten Eckwerte (Kennzahlen), welche unterstützt werden sind:

- Bereitstellung einer einheitlichen Basis pro Themengebiet;
- Bereitstellung der Grundlagen zur Entscheidungsfindung;
- Stakeholderorientierte Präsentation von Daten und Informationen;
- Verbesserung der Transparenz;
- Schaffung der Vergleichbarkeit;
- Unterstützung der operativen und strategischen Führung;
- Entwicklungstrends frühzeitig erkennen;
- Überprüfung der Einhaltung der Vorgaben.

## 5.6 Rückfallebene

Dies bedeutet, dass bei Ausfall einer Ebene der SA-CH Architektur der Betrieb, durch die darunterliegende Ebene weiterhin sichergestellt werden kann, d.h. die darunterliegende Ebene bildet die Rückfallebene der darüberliegenden Ebene.

Diese Struktur ermöglicht die Autonomie der einzelnen Ebenen. Jede Ebene bildet funktional und technisch eine eigenständige Einheit und ist in ihren fundamentalen Funktionen nicht von der darüber liegenden Ebene abhängig.

Dieser Grundsatz funktioniert bis auf Stufe 2 (AR). Die nachfolgende Darstellung erläutert diese Stufen:

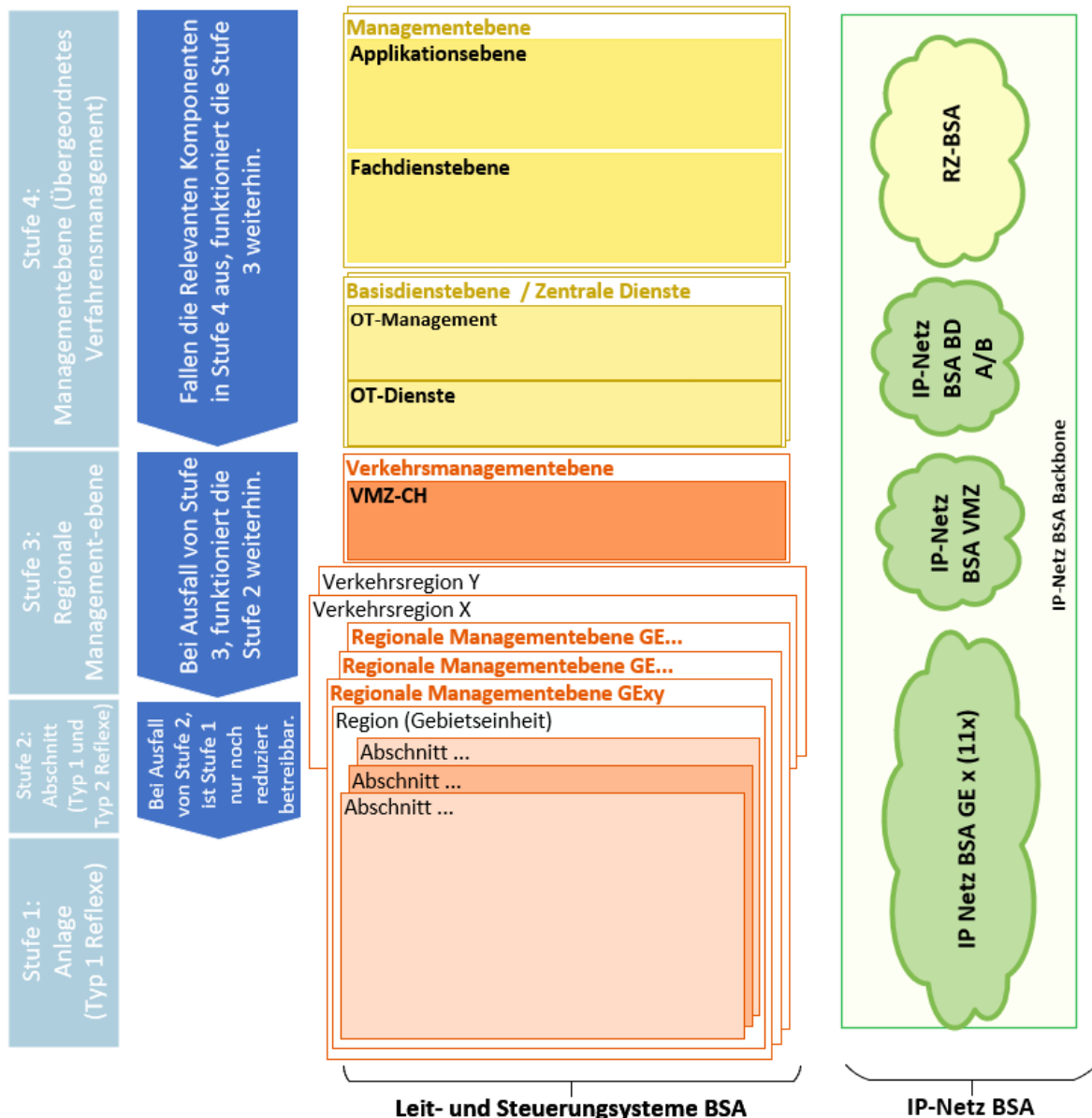


Abbildung 28: Rückfallebenen SA-CH

### Stufe 4

Erstreckt sich von der Managementebene bis zur Ebene der Basisdienste/Zentrale Dienste. Fallen die relevanten Komponenten in Stufe 4 aus, funktioniert die Stufe 3 weiterhin. Die Bedienung kann in allenfalls reduzierter Form auf Stufe 3 weiterhin erfolgen.



**Stufe 3**

Diese beinhaltet sowohl die Regionale Managementebene als auch die Verkehrsmanagementebene. Bei Ausfall von Stufe 3, funktioniert die Stufe 2 weiterhin. Die Bedienung kann in allenfalls reduzierter Form auf Stufe 2 weiterhin erfolgen.

**Stufe 2**

Abschnitt (Typ 1 und Typ 2 Reflexe) / AR: Bei Ausfall von Stufe 2 ist Stufe 1 nur noch reduziert betreibbar, da die Reflexe Typ 2 nicht mehr funktionieren. Die Bedienung kann in reduzierter Form auf Stufe 1 weiterhin erfolgen.

**Stufe 1**

AS, LS, Sensoren (Typ 1 Reflexe). Bei Ausfall von Stufe 1 ist kein Betrieb mehr möglich.

## 5.7 Betriebsrelevante WEB-Links

Die Sammlung der WEB-Links auf allen MMI und GUI sind gesondert zu speichern und für ein allfälliges Disaster Recovery bereit zu halten. Dazu kann mittels diesen WEB-Links bei Ausfall des UeLS-CH direkt auf die AR oder AS/LS zugegriffen werden.

## 5.8 Autonomie

Im Kapitel 4.3.1 wurde die Thematik der objektgebundenen Autonomie aufgenommen. Dies bezeichnet die betriebliche Autonomiefähigkeit im Abschnitt. Die nachfolgenden Übersichten stellen die möglichen Betriebsszenarien mit Berücksichtigung der sicherheitskritischen Anlagen dar. Die Thematik der Energieautonomie oder der spezifischen Anlageautonomie wird hier nicht berücksichtigt.

### 5.8.1 Anlagefunktion in Bezug auf das Betriebsszenario

Nachfolgend wird definiert, welche Teilanlagen minimal für einen sicheren Betrieb funktionieren müssen. Die Abhängigkeiten zur abschnittsinternen und externen Kommunikation sind im Kapitel 5.8.7 ersichtlich.

*Tabelle 18: Teilanlagen für minimalen sicheren Betrieb*

| AKS-Bez. | Bezeichnung Anlage / Teilanlage      | Bemerkung |
|----------|--------------------------------------|-----------|
| ZEE      | Zentrale Einrichtung - Energie       |           |
| HS       | Hochspannung (Energiezuführung)      |           |
| NS       | Niederspannung (Energieverteilung)   |           |
| NST      | Notstrom                             |           |
| ZEB      | Zentrale Einrichtung - Beleuchtung   |           |
| DB       | Durchfahrtsbeleuchtung               |           |
| BN       | Brandnotbeleuchtung                  |           |
| FWB      | Fluchtwegbeleuchtung                 |           |
| ZEL      | Zentrale Einrichtung - Lüftung       |           |
| AL       | Abluft                               |           |
| LL       | Längslüftung                         |           |
| ZL       | Zuluft                               |           |
| FWL      | Fluchtwegbelüftung                   |           |
| ZES      | Zentrale Einrichtung - Signalisation |           |
| VM       | VM-System                            |           |
| LSA      | Lichtsignalanlage                    |           |

Tabelle 18: Teilanlagen für minimalen sicheren Betrieb

| AKS-Bez. | Bezeichnung Anlage / Teilanlage                         | Bemerkung            |
|----------|---|----------------------|
| SER      | Sicherheitseinrichtung                                  |                      |
| BMT      | Brandmeldeanlage Tunnel                                 |                      |
| VTV      | Videoanlage   | ED oder Bildspeicher |
| DI       | Zentrale Einrichtung - Diversanlage                     | Türöffnung           |
| IPE      | Kommunikationsnetzwerk<br>IP-Netz<br>Erschliessungsring |                      |
| IPA      | Kommunikationsnetzwerk<br>IP-Netz<br>Access-Bereich     |                      |
| LTA      | Leittechnik Abschnitt                                   |                      |
| FE       | Funksystem (Radio, Einsprechung, Polycom)               |                      |
| NT       | Notruftelefon   |                      |
| HI       | Hausinstallation  |                      |
| HLK      | Heizung, Lüftung, Klima                                 |                      |
| BMG      | Brandmeldeanlage Gebäude                                |                      |
| POR      | Pumpwerk  |                      |
| LOE      | Löscheinrichtung  |                      |
| TTZ      | Tür / Tor / Zutrittskontrolle                           |                      |
| WV       | Wasserversorgung  |                      |
| SAA      | Strassenabwasserbehandlungsanlage                       |                      |

### 5.8.2 Betriebsszenarien in Bezug auf die Abschnittsautonomie

Es gelten folgende Betriebsszenarien:

- Normalbetrieb (alle Betriebsarten und Bedienmöglichkeiten in Funktion);
- Eingeschränkter Betrieb (alle automatischen Funktionen (Reflexe) sind möglich, aber keine Bedienmöglichkeit oder Kommunikation mit dem UeLS-CH);
- Notbetrieb mit vordefinierten Rückfallwerten;
- Kein Betrieb.

In den folgenden Erläuterungen werden sowohl die auslösende Ursache als auch die verfügbaren Funktionen, als Grundsatz dargestellt.

### 5.8.3 Normalbetrieb

Kein Auslöser.

#### Grundsatz:

- Kommunikation intern und extern in Funktion inkl. Zugriffe;
- Alle Reflexe in Funktion.

### 5.8.4 Eingeschränkter Betrieb

Auslöser: Kommunikation ausserhalb des Abschnitts komplett unterbrochen.

#### Grundsatz:

- Kommunikation intern in Funktion inkl. interne Zugriffe;
- Alle Reflexe in Funktion (Netzwerkverbindungen AS-AR-AS);
- Steuerung: Relevant für Abschnitts-Autonomie (eigenständiger automatischer Weiterbetrieb MIT/OHNE Eingriff eines Operators (vor Ort im Abschnitt));
- Ohne Alarmierung ausserhalb des Abschnitts.

### 5.8.5 Notbetrieb

Auslöser: Kommunikation innerhalb des Abschnitts **teilweise** unterbrochen.

**Grundsatz:**

- Kommunikation intern teilweise ausgefallen;
- Relevant für Abschnitts-Autonomie (eigenständiger automatischer Weiterbetrieb MIT/OHNE Eingriff eines Operators);
- Nur teilweise Alarmierung ausserhalb des Abschnitts. Teilweise Rückfall in Grundzustands-Konfiguration oder Vorprogrammierte Werte;
- Dieses Betriebsszenario wird zeitlich begrenzt und muss bewilligt sein. Wie weit ein sicherer Betrieb gewährleistet werden kann, ist im Grundsatz über den ELG (Einsatzleiter GE) und den ELA (Einsatzleiter ASTRA) abzuklären.

### 5.8.6 Kein Betrieb

Auslöser: Kommunikation innerhalb des Abschnitts komplett unterbrochen.

**Grundsatz:**

- Keine Reflexe in Funktion;
- Keine Bedienung ab UeLS-CH und keine Meldungen an UeLS-CH möglich;
- Tunnelsperrung durch automatische Notfunktion der einzelnen AS.

### 5.8.7 Übersicht Betriebsszenarien

Die nachfolgende Tabelle zeigt eine Übersicht der Betriebsszenarien in Abhängigkeit zu Grundsatz und Zustand.

Tabelle 19: Übersicht der Betriebsszenarien

|               |            | Grundsätze und Zustand                        | Normal Betrieb | Eingeschränkter Betrieb | Notbetrieb   | Kein Betrieb   | Rückfall-ebene (Vgl. 5.6) |
|---------------|------------|---|----------------|-------------------------|--------------|----------------|---------------------------|
| Themenbereich | Auslösend  | IP-Netz BSA ausserhalb des Abschnitts         | Volle Funktion | Keine Funktion          | Teilausfälle | Volle Funktion | Stufen 2-4                |
|               |            | IP-Netz BSA innerhalb eines Abschnitts        | Volle Funktion | Volle Funktion          | Teilausfälle | Keine Funktion | Stufen 1-2                |
|               | Auswirkung | Kommunikation AR zu UeLS/BL(Z)                | Volle Funktion | Keine Funktion          | Teilausfälle | Keine Funktion | Stufen 2-3                |
|               |            | Bedienung über UeLS/BL(Z)                     | Volle Funktion | Keine Funktion          | Teilausfälle | Keine Funktion | Stufe 3                   |
|               |            | Kommunikation innerhalb des Abschnitts        | Volle Funktion | Volle Funktion          | Teilausfälle | Keine Funktion | Stufen 1-2                |
|               |            | Zugriff auf AR, AS, LS                        | Volle Funktion | Volle Funktion          | Teilausfälle | Keine Funktion | Stufe 1                   |
|               |            | Funktion AR inkl. Redundanz (im IP-Abschnitt) | Volle Funktion | Volle Funktion          | Teilausfälle | Keine Funktion | Stufe 1                   |
|               |            | Eingriff auf AR innerhalb eines Abschnitts    | Volle Funktion | Volle Funktion          | Teilausfälle | Keine Funktion | Stufe 1                   |
|               |            | Reflex-Aktivität                              | Volle Funktion | Volle Funktion          | Teilausfälle | Keine Funktion | Stufe 1                   |
|               |            | Auswirkung auf Tunnelbetrieb                  | Volle Funktion | Volle Funktion          | Teilausfälle | Keine Funktion | Stufe 1                   |

### 5.8.8 Anwendbarkeit

Nachfolgend ist im Grundsatz ersichtlich, welche Betriebsszenarien in welcher Tunnelkategorie anwendbar sind:

*Tabelle 20: Übersicht zur Anwendbarkeit in Abhängigkeit der Tunnelkategorie*

|                 | Tunnellänge<br>(GV und RV*) | Lüftung               | Normal<br>Betrieb | Eingeschränkter<br>Betrieb | Notbetrieb    |
|-----------------|-----------------------------|-----------------------|-------------------|----------------------------|---------------|
| Tunnelkategorie | < 300 m                     | keine                 | Erlaubt           | Erlaubt                    | Erlaubt       |
|                 | < 600 m                     | keine                 | Erlaubt           | Erlaubt                    | Erlaubt       |
|                 | < 1000 m                    | Ja (ohne Abluft)      | Erlaubt           | Erlaubt                    | Nicht erlaubt |
|                 | < 3000 m                    | Ja (evtl. mit Abluft) | Erlaubt           | Erlaubt                    |               |
|                 | > 3000 m                    | Ja (Spezialtunnel)    | Erlaubt           | Erlaubt                    |               |

\* GV=Gegenverkehr, RV = Richtungsverkehr

## 5.9 IP-Netz BSA

Das IP-Netz BSA übernimmt die Kommunikation auf allen Ebenen der Systemarchitektur. Das Kommunikationsnetz verbindet die Managementebene mit den Basisdiensten, der Verkehrsmanagementebene und den Regionalen Managementebenen und stellt insbesondere auch die Kommunikation innerhalb der Anlagen und der Anlagen untereinander sicher. Das IP-Netz BSA unterstützt die Übertragung von Daten, Video und Sprache sowohl nativ mit einer IPv6-Adressierung als auch mit einer IPv4-Adressierung für Legacy-Systeme oder Systeme, die noch nicht IPv4-fähig sind.

Die gesamte Kommunikation der BSA erfolgt über das IP-Netz BSA. Es werden keine separaten Netze verwendet. Ausnahmen können lediglich für abgelegene oder autarke Anlagen zugelassen werden, welche nicht mit IP-Netz BSA erschlossen sind.

Weitere Informationen zur Topologie oder zur Technologie sind in der ASTRA Richtlinie 13040 zu finden.

## 5.10 Kommunikationsgrundsätze

### 5.10.1 Grundsätze und Anforderungen

Das IP-Netz BSA ist ein IPv6 Netz, das auch IPv4 transportieren kann (Dualstack). Es gelten folgende Anforderungen:

- Sämtliche Netzwerkkomponenten (Erschliessungsringrouter, Switches) werden ausschliesslich über IPv6 administriert;
- Sämtliche Netzwerkkomponenten (Erschliessungsringrouter, Switches) können sowohl IPv4 als auch IPv6 transportieren (Dualstack);
- Das Network Management System (NMS) ist ebenfalls als IPv6 Instanz aufgesetzt;
- Netzwerknähe Dienste wie NTP, DNS und DHCP sind sowohl als IPv4 als auch als IPv6 Instanzen aufzusetzen;
- Netzwerkausrüstung und die zentrale Infrastruktur greifen über IPv6 auf Services wie RADIUS, LDAP und AD zu;
- Die Grundinfrastruktur (Server & Storage) für die zentralen Dienste in den OT-Technikräumen sind als IPv6 Instanzen aufzusetzen und zu administrieren;
- Ebenso sind die Firewalls oder Firewall-Clusters als IPv6 Instanzen zu realisieren;
- Das UeLS-CH CH und die Abschnittsrechner (AR) in den GE sind über IPv6 erreichbar, ebenso die Operatoren-Arbeitsplätze/Bedienarbeitsplätze;

- Sämtliche Anlagen/Teilanlagen, welche über die IP-Abschnitte hinweg operieren (wie bspw. das Videomanagementsystem inkl. der Kameras) und neu aufgesetzt bzw. erneuert werden, sind als IPv6 Instanzen zu realisieren und sind ausschliesslich über IPv6 erreichbar;
- Die übrigen Anlagen/Teilanlagen sind nach Möglichkeit bei Erneuerungen oder beim Neubau als IPv6 Instanzen zu realisieren. Bestehende Anlagen müssen nicht auf IPv6 migriert werden.

Primäres Ziel ist es, eine IPv6-Grundinfrastruktur in den GEs aufzubauen und vor allem die Erreichbarkeit in die Gebietseinheiten hinein oder hinaus nativ via IPv6 sicherzustellen (nicht über NAT64/46).

### 5.10.2 Protokolle

Der Datenaustausch zwischen der Managementebene, der Regionalen Managementebene und den Abschnittrechnern erfolgt immer über IP-basierte Protokolle. Standardmässig kommt dabei das Kommunikationsprotokoll OPC UA zum Einsatz. Für die Anlagen des Videomanagements werden standardisierte Streaming-Protokolle wie RTSP eingesetzt.

Innerhalb eines IP-Abschnitts kann die Kommunikation IP- als auch Ethernet-basierend erfolgen. Bei Bedarf können die Aktoren und Sensoren auch über serielle Protokolle angesprochen werden. Sollten Anlagen- und Lokalsteuerungen oder auch einzelne Aktoren wie Kameras IP-abschnittsübergreifend angesprochen werden, so sind immer IP-basierende Protokolle wie bspw. OPC UA oder RTSP (Real-Time Streaming Protocol) einzusetzen.

Den Einsatz von Protokollen ist im Leitfaden «IP-Netz BSA Leitfaden Migration Anlagenetze» im Detail beschrieben.

## 5.11 Datenmodell und Datenpunkte

Die vorliegende ASTRA Richtlinie 13031 beschreibt, wie die Elemente miteinander und mit der (Regionalen) Management-Ebene kommunizieren. Die Datenpunkt Modellierung und deren Prozesse sind in der ASTRA Richtlinie 13033 «Anwendung des Datenpunktmodells SA\_CH» beschrieben.

Die ASTRA Richtlinie 13032 (Teil 1 bis 6) beschreibt den Austausch von Informationen innerhalb und zwischen den Ebenen (Teil 1-3), die Reflexe (Teil 4), das Alarm-Management, (Teil 5) sowie die Anforderungen für die graphische Darstellung (Teil 6). Die Richtlinie 13034 regelt den Einsatz von OPC UA.

## 5.12 Datenaustausch

Dieses Kapitel beschreibt sowohl den Datenaustausch auf dem UeLS-CH und dem AR als auch der AS zu den angrenzenden Systemen.

### 5.12.1 UeLS-CH

#### **Datenaustausch mit weiteren Systemen (0):**

UeLS-CH stellt weiteren Applikationen und deren Benutzern selektierte Alarmer zur Verfügung.

#### **Datenaustausch mit ELS (0):**

Die UeLS-CH stellt dem Einsatz-Leitsystem (ELS) / und deren Benutzern die selektierten Alarmer/Ereignisse zur Verfügung.

#### **Datenaustausch mit den AR (1):**

Diese Schnittstelle dient dem UeLS-CH zur Steuerung und Überwachung der BSA-Abschnitte.

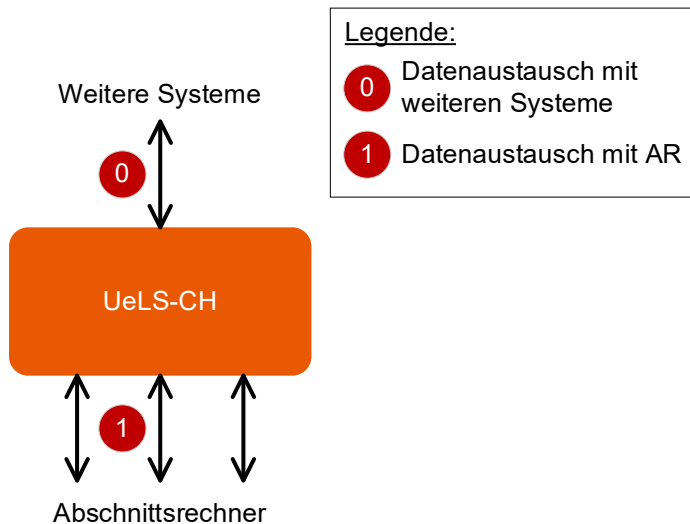


Abbildung 29: UeLS-CH-Datenaustausch

### 5.12.2 Abschnittsrechner

#### Datenaustausch mit Regionaler Management-Ebene (UeLS-CH) / Benutzer (1):

Der AR stellt der Regionalen Management-Ebene (UeLS-CH) / und deren Benutzern selektierte Datenpunkte zur Verfügung.

#### Datenaustausch mit den AS (2):

Diese Schnittstelle dient dem AR zur Steuerung und Überwachung der Anlagen.

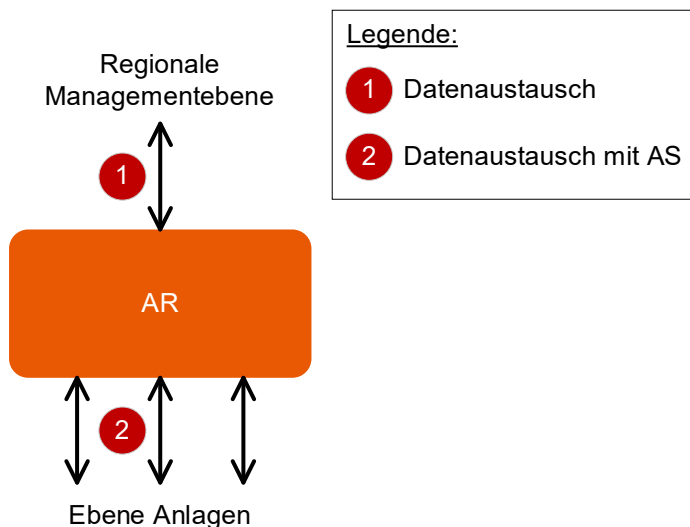


Abbildung 30: AR-Datenaustausch

### 5.12.3 Anlagen- / Lokalsteuerung

#### Datenaustausch zwischen AR und Benutzer (2):

Die AS sendet Meldungen, Messwerte und Quellreflexe an den AR und erhält Befehle und Senkenreflexe vom AR.

#### Kommunikation Typ 1 (3):

Die Kommunikation zwischen AS und AS geschieht hauptsächlich via AR. Für die Reflexe Typ 1 ist eine direkte zusätzliche Verbindung zwischen den AS vorgesehen (vgl. Kap 5.13).

**Datenaustausch innerhalb der Anlage (4), (5), (6):**

Die AS tauscht Daten und Steuerbefehle mit den LS, ihren Remote IOs und Sensoren und Aktoren aus.

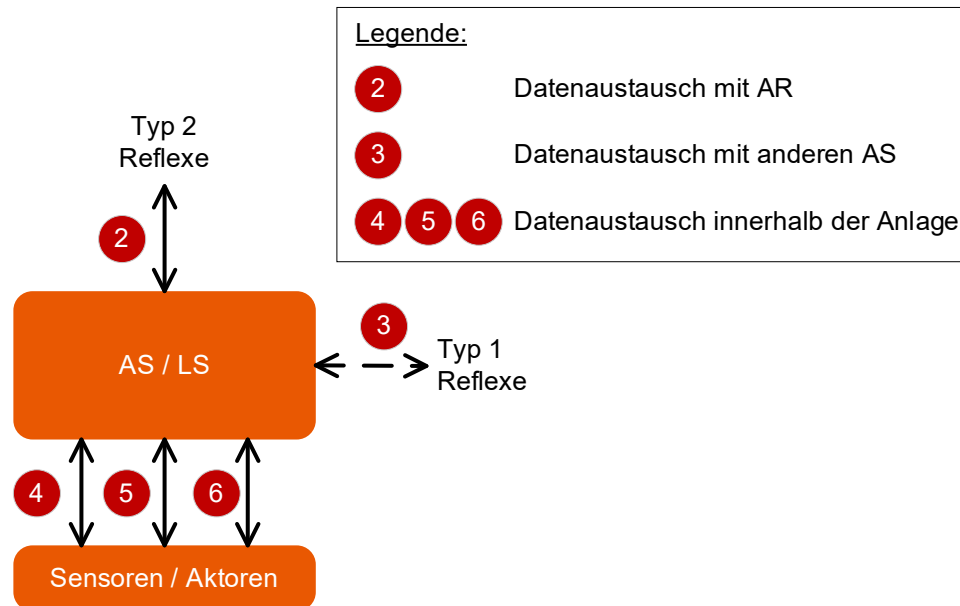


Abbildung 31: AS/LS – Datenaustausch

## 5.13 Reflexe

In diesem Dokument werden nur die Arten von Reflexen und die Art ihrer Weiterleitung genannt. Die Verwendung der Reflexe ist in der ASTRA Richtlinie 13032 (Teil 4) beschrieben.

### 5.13.1 Art der Reflexe

Grundsätzlich müssen die Reflexe von einer Quelle bis zu einer Senke gelangen. Die Weiterleitung von Reflexen kann auf drei Arten erfolgen:

- Mit der **automatischen Weiterleitung** fließen die Reflexe ohne Unterbruch von der Quelle bis zur Senke;
- Mit der **halbautomatischen Weiterleitung** werden die Reflexe ohne eine Bestätigung des AR (durch den Operator) nicht weitergeleitet oder die Reflexe werden vom AR weitergeleitet in dem Fall, wenn ein Timeout für die Annahme oder Ablehnung des Reflexes innerhalb eines bestimmten Zeitraums eingestellt ist (z.B. Brand kann der Fall sein);
- Unter **manueller Weiterleitung** versteht man die manuelle Erzeugung von Reflexen. Dies kann der Fall sein, wenn die automatischen Reflexe nicht funktionieren oder wenn bei einem Test das korrekte Verhalten der Anlage geprüft wird.

Die Reflex Bedienung durch einen Operator ist auf dem AR vorgesehen.

Grundsätzlich ist immer projektspezifisch zu prüfen, welche Anbindung in Anbetracht der Abhängigkeiten zu den weiteren Anlagen die sicherste Variante ist.

### 5.13.2 Reflex Typen

Aufgrund des erwarteten Sicherheitsbedürfnisses auf den Nationalstrassen werden die Reflexe in zwei Typen eingeteilt. Sie unterscheiden sich in den Anforderungen an die Verfügbarkeit, die Reflexübertragung und den daraus resultierenden technischen Lösungen:

Der Reflex-Typ 1 (sicherheitskritischer Reflex) kommt zum Einsatz, wenn der Reflex höchste Priorität hat und auch bei einem Ausfall einer Kommunikationsverbindung mit einem / oder eines darüber liegenden Elementes wie dem AR funktionieren muss.

Der Reflex-Typ 2 (nicht sicherheitskritischer Reflex) kommt zum Einsatz, wenn eine gefährliche Situation ein sofortiges Handeln erfordert.

Die Liste der Reflex Typ 1 wird in der ASTRA Richtlinie 13032 (Teil 4) definiert.

### 5.13.3 Zielarchitektur

Durch die Verfügbarkeitserhöhung der AR, können Typ 1 Reflexe in der Architektur der Typ 2 Reflexe umgesetzt werden, jedoch nur, wenn der Nachweis für die verlangte Verfügbarkeit erbracht ist.

#### 5.13.3.1 Sicherheitskritischer Reflex (Typ 1)

Der Typ 1 kommt zum Einsatz, wenn der Reflex höchste Priorität hat. Somit muss dieser ebenfalls bei einem Ausfall einer Kommunikationsverbindung oder eines Elements auf der Stufe AS oder AR übertragen werden. Dabei werden Einzelausfälle betrachtet. Eine höhere Verfügbarkeit muss für die Übertragung dieses Reflex-Typs gewährleistet werden (Netz, Switches, redundant Steuerungen, etc.). Die Reflexe werden direkt an jede relevante AS und/oder LS weitergeleitet. Allenfalls wird der Reflex redundant über das IP-Netz BSA übermittelt. Jede Unterebene muss sich mit der oberen Ebene koordinieren, um den Reflex zu bearbeiten.

Anstelle der Hardwareverbindung kann via IP-Netz BSA eine Direktverbindung eingerichtet.

Die Kopplung von Anlagen über dedizierte Reflex-Verbindungen ist zulässig, d.h. über Schnittstellen, die nur der Reflex-Übertragung zwischen den Anlagen dienen und getrennt sind von den Schnittstellen der AS-LS-Kommunikation und der AS-AR-Kommunikation.

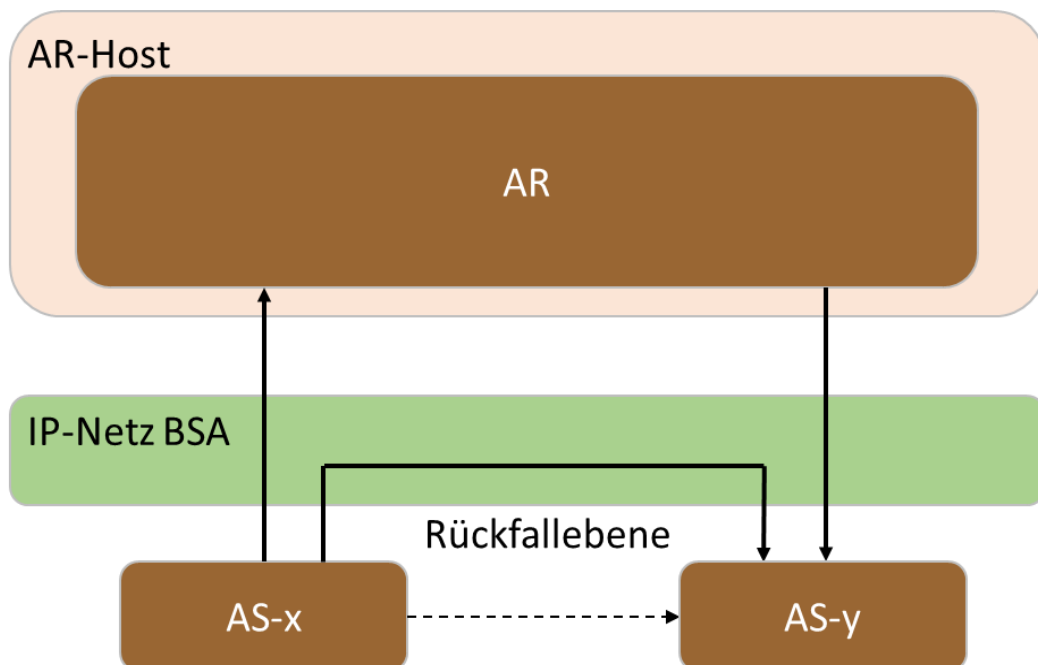


Abbildung 32: Reflex Typ 1

#### 5.13.3.2 Nicht sicherheitskritischer Reflex (Typ 2)

Der Typ 2 wird für alle Reflexe verwendet, die nicht als Typ 1 eingestuft sind. Für diesen Reflex-Typ ist eine Standard-Verfügbarkeit ausreichend. Die Reflexe vom Typ 2 werden über den AR ausgetauscht, ohne parallele Übertragung.



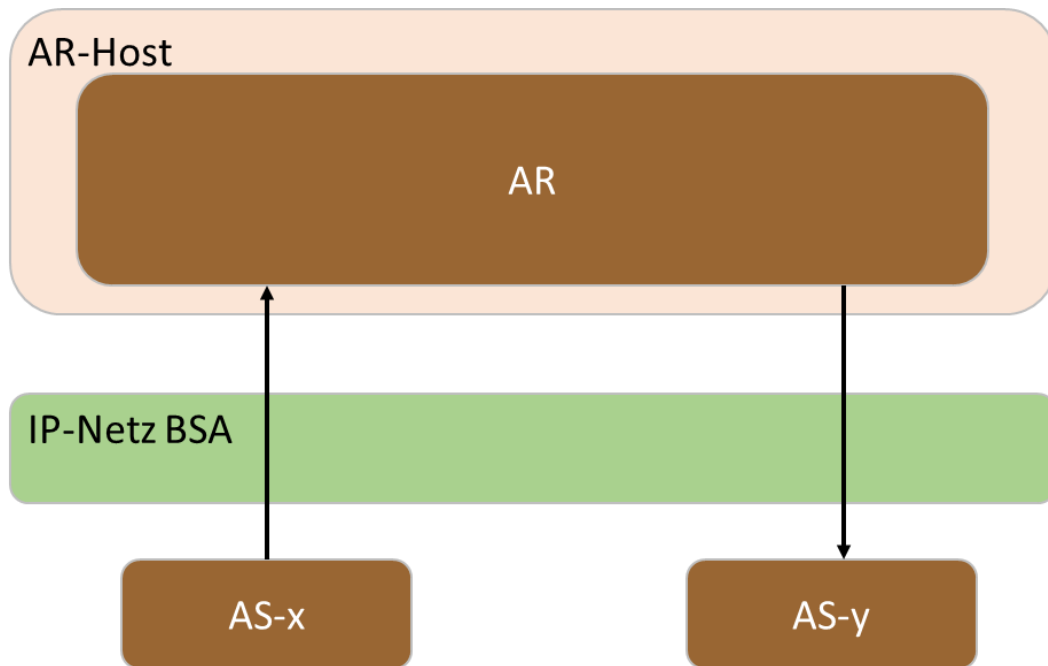


Abbildung 33: Reflex Typ 2

Die Begriffe Standardverfügbarkeit und höhere Verfügbarkeit sind im Kapitel «Verfügbarkeit» definiert.

## 5.14 Zugangsportale OT/BSA und Remote Zugang (OT-Notsysteme)

Gemäss ASTRA Dokumentation 83056 werden diese via den Zugangsportalen OT/BSA gewährleistet.

## 5.15 Anbindung von Umsysteme

Die Umsysteme sind über das IP-Netz BSA an die SA-CH Architektur anzubinden.

## 5.16 Mobile Kommunikation

Die erste Generation von M2M-Integrationen wurde für die kabellose Integration von Verkehrszählern und Verkehrskameras eingesetzt. Diese Integration basiert auf der dedizierten Zuweisung von IP-Adressbereichen des gesamten BIT-Adressbereiches und direkten Koppelung in den IP-Netz BSA Backbone.

Die nächste Generation (ab Januar 2025) wird flächendeckend genutzt werden können (unterschiedliche Anwendungen innerhalb des IP-Netz BSA) und ist dediziert für die BSA definiert.

## 6 Migration

Um die Zielarchitektur zu erreichen, werden bei bestehenden Infrastrukturen Zwischenschritte notwendig sein. In den nachfolgenden Subkapiteln werden die möglichen Zwischenschritte erläutert, welche zur Zielarchitektur führen.

Unter Migration versteht man die Überführung der bestehenden Architektur in die neue, hier beschriebenen, Architektur. Die Migration gilt als abgeschlossen, wenn alle bestehenden Anlagen durch konforme Anlagen ersetzt worden sind. Dieser Prozess dauert dementsprechend mehrere Jahre. (Ziel SA-CH: bis 2029)

In den Nachfolgenden Subkapiteln werden die wichtigsten Punkte hinsichtlich der Migration aufgezeigt.

Im Grundsatz gelten für die Projektumsetzungen die Richtlinien, welche zum Zeitpunkt der Bewilligung des MP/DP gültig waren. Da die Projektlaufzeiten sehr lange sind und teilweise durch Einsparungen längere Projektstopps erfolgt sind, muss bei der Ausschreibung des Realisierungspflichtenheft (RPH) noch einmal auf die aktuellen Weisungen, Richtlinien und Dokumentation überprüft werden. Differenzen sind mit der Fachunterstützung und SA-CH zu besprechen. Der Projektleiter muss die Ausnahmen begründen und es muss eine schriftliche Bewilligung vorliegen.

Mittels der Konformitätsprüfungen wird in den unterschiedlichen SIA-Phasen der Erreichungsgrad der Vorgaben ermittelt. Allenfalls werden Nachprüfungstermine definiert, um grössere Abweichungen auszugleichen (Übergangsfristen).

Alle Projekte müssen die Netzwerkzonen und die Security gemäss den Vorgaben erfüllen. Abweichungen können nicht zugelassen werden, da die Kommunikation bei Nichteinhaltung nicht funktioniert.

### 6.1 Organisatorische Anpassungen Geschäfts- und Betriebsorganisation BSA-OT

In der Weiterentwicklung der Geschäfts- und Betriebsorganisation BSA-OT werden sowohl die bestehenden Aufgaben der BSA und OT geklärt als auch neue Aufgaben aufgeführt. Es werden Verantwortung und Kompetenzen aufgenommen und dargestellt. Diese Anpassungen werden in Etappen umgesetzt. und fliessen anschliessend in die Vereinbarungen ein.

### 6.2 Generelles zum Migrationskonzept

Das Migrationskonzept muss sämtliche benötigten Etappen inkl. Risikobewertung enthalten. Dazu müssen das Testprozedere und die Konformitätsprüfung vorliegen.

Da jedes Projekt eine unterschiedliche Ausprägung aufweist, kann keine generelle Migrationsarchitektur erstellt werden.

### 6.3 Kommunikation und Leittechnik

Im «Leitfaden Migration Anlagennetze» sind die Zwischenschritte detailliert aufgelistet. Die Implementierung von Kommunikationsstandards muss gemäss den Definitionen erfolgen (keine abgewandelten Integrationen). Die Projektleiter IP-Netz BSA der Filialen und der Fachsupport IP-Netz BSA der Zentrale steht zur Unterstützung zur Verfügung.

### 6.3.1 Leittechnik (UeLS-CH und Systemintegration)

In diesem Kapitel sind die empfohlenen Umsetzungsvarianten am Beispiel der Leittechnik (UeLS-CH und Systemintegration) beschrieben. Diese Richtlinie beschreibt den Soll-Zustand der Systemarchitektur. Die Abbildung 34 zeigt eine Übersicht der Migrationsarchitektur in Bezug auf die Leittechnik.

Die Umsetzung ist vom projektspezifischen IST-Zustand der vorhandenen Systeme und Projektdefinitionen abhängig. In der SIA-Phase 31 (MK) werden die Varianten aufgezeigt und diskutiert (vgl. ASTRA Dokumentation 83055).

In der Abbildung 34 ist zur Verständlichkeit jedes relevante Element nur einmal dargestellt. Die Notation „1...x“ weist auf die Vielzahl hin. Weiter sind der Abbildung sind zwei Umsetzungsvarianten dargestellt.

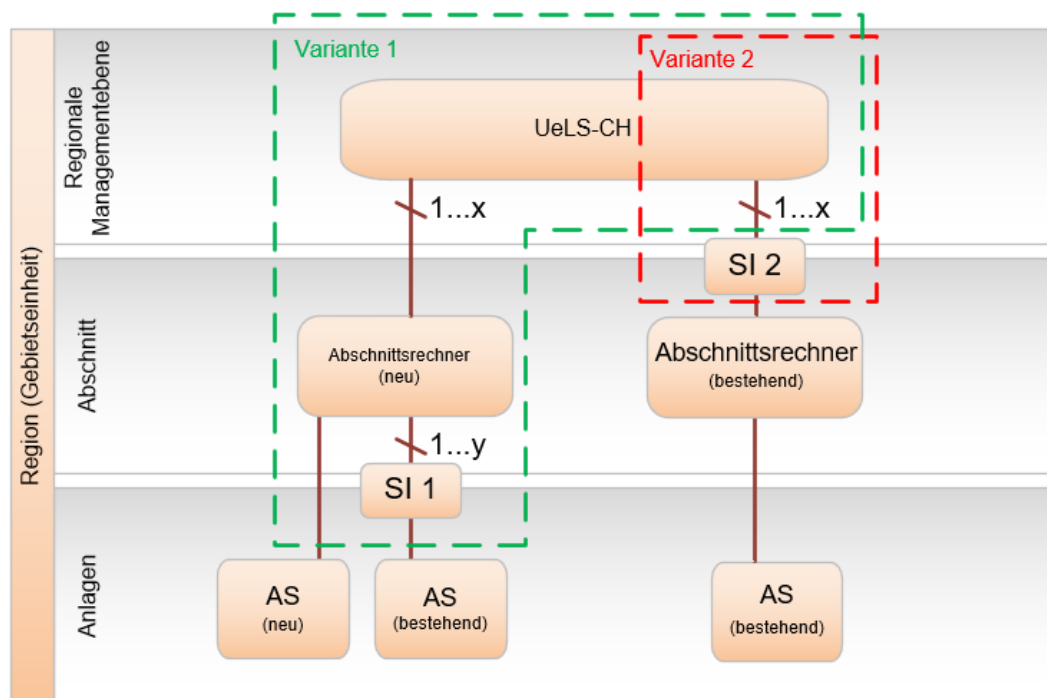


Abbildung 34: Umsetzungsvarianten Leittechnik (UeLS-CH und Systemintegration) wobei neu = SA-CH-konform und bestehend = nicht SA-CH-konform

\*neu = SA-CH-konform / \*bestehend = nicht SA-CH-konform

Grundsätzlich ergeben sich für die Migration, gemäss Abbildung 34 die folgenden Varianten:

#### Variante 1

Werden bestehende, nicht SA-CH-konforme Anlagensteuerungen (AS) in neue, SA-CH-konforme Abschnittsrechner (AR) integriert, so werden diese AS mit Hilfe von Serviceintegratoren (SI 1) mit den jeweiligen AR verbunden. Die SI gewährleisten die Funktion der Schnittstelle AR <> AS gemäss den Vorgaben SA-CH.

#### Variante 2

Werden bestehende, nicht SA-CH-konforme AR mit bestehenden AS in ein UeLS-CH integriert, so werden diese AR mit Hilfe von Serviceintegratoren (SI 2) mit dem UeLS-CH verbunden. Die SI gewährleisten die Funktion der Schnittstelle UeLS-CH <> AR gemäss den Vorgaben SA-CH.

Diese Varianten ermöglichen eine etappierte Migration der Abschnittsrechner und Anlagensteuerungen.

## 6.4 Verkehrsmanagementsysteme

Alle nachfolgend aufgeführten Systeme sind temporäre Übergangslösungen und werden später rückgebaut.

### 6.4.1 Vehicle-by-Vehicle System (VBV)

Das VBV wird mittelfristig in Etappen durch den Fachdienst Betriebs- und Verkehrsdatenerfassung (FD BVDE) abgelöst werden. Das VBV verarbeitet die Daten der Verkehrszähler und beliefert Umsysteme in unterschiedlichen Formaten mit diesen Informationen.

#### 6.4.1.1 Zählstellencontroller (ZSC)

Die ZSC sind in Abstimmung mit der IP-Netz BSA Migration abzubauen.

### 6.4.2 Verkehrsinformationssystem (VIS)

Die Migration der VIS wird von den ASTRA-Filialen geplant. Es ist darauf zu achten, die Ausfallzeiten während der Migration möglichst gering zu halten und mit der VMZ-CH vorgängig zusammen zu planen. Optimalerweise erfolgt dabei auch eine Überprüfung der vorhandenen Bedienungen mit der VMZ-CH und wenn erforderlich der gleichzeitige Ersatz der aktuellen VIS-Systeme. Zukünftig werden die WTA und WWW in die sich in Umsetzung befindliche FA VL-CH angebunden und sind somit schweizweit zentral steuerbar.

### 6.4.3 Regionale Verkehrslenkung (rVL)

Die bestehenden rVL werden zukünftig, nach der Übergangsphase, entweder durch VR<sub>RM</sub> VM-CH oder VL-CH abgelöst werden und entfallen somit.

Es ist darauf zu achten, die Ausfallzeiten während der Migration möglichst gering zu halten und mit der VMZ-CH vorgängig zusammen zu planen. Optimalerweise erfolgt dabei auch eine Überprüfung der vorhandenen Bedienungen mit der VMZ-CH.

### 6.4.4 Regionale Verkehrsdatenerfassung (rVDE)

Die bestehenden rVDE werden zukünftig, nach der Übergangsphase, entweder durch den direkten Infotransit der Verkehrszähler an VR<sub>RM</sub> VM-CH oder VL-CH angeschlossen werden und entfallen somit.

Es ist darauf zu achten, die Ausfallzeiten während der Migration möglichst gering zu halten und mit der VMZ-CH vorgängig zusammen zu planen. Optimalerweise erfolgt dabei auch eine Überprüfung der vorhandenen Bedienungen mit der VMZ-CH.

### 6.4.5 Regionale Verkehrsrechner (VR)

Die VR (Zwischenlösung IVM und RM VM) werden nach der Übergangsphase durch die FA VL-CH abgelöst.

# Anhänge

|            |   |           |
|------------|---|-----------|
| <b>I</b>   | <b>Begrifflichkeiten .....</b>                          | <b>79</b> |
| I.1        | Verfügbarkeit (Availability) .....                      | 79        |
| I.2        | Hochverfügbarkeit (High Availability) .....             | 79        |
| I.3        | Fehlertoleranz (Fault Tolerance) .....                  | 79        |
| I.4        | Redundanz (Redundance) .....                            | 79        |
| I.5        | Hot-Standby .....                                       | 79        |
| I.6        | Cold-Standby .....                                      | 80        |
| I.7        | Daten- und Systemsicherung (Backup) .....               | 80        |
| I.8        | Disaster-Recovery .....                                 | 80        |
| <b>II</b>  | <b>Redundanzen .....</b>                                | <b>81</b> |
| II.1       | Applikationsredundanz .....                             | 81        |
| II.2       | Weitere Erhöhung der Redundanz .....                    | 82        |
| II.3       | High Availability Cluster (HA Cluster) .....            | 82        |
| II.4       | Failover Cluster .....                                  | 82        |
| II.5       | Cluster mit virtuellem SAN (Storage Area Network) ..... | 83        |
| II.6       | Fault Tolerance (FT) .....                              | 83        |
| II.6.1     | AR Redundanzvergleich .....                             | 84        |
| <b>III</b> | <b>Grundlagen Virtualisierung .....</b>                 | <b>85</b> |
| III.1      | Virtualisierungsplattform .....                         | 85        |
| <b>IV</b>  | <b>Systemarchitektur Schweiz (SA-CH) .....</b>          | <b>87</b> |
| IV.1       | Architektur SA-CH .....                                 | 87        |
| IV.2       | Architektur SA-CH GUI/MMI-Umsetzung .....               | 88        |
| <b>V</b>   | <b>Technologieanwendungen .....</b>                     | <b>89</b> |
| V.1        | Technologieanwendungen einer Röhre .....                | 89        |
| V.2        | Technologieanwendungen zwei Röhren .....                | 91        |
| V.3        | Berechnungsbeispiel für Hardwareressourcen .....        | 93        |
| V.3.1      | HOST-Hardware (Server) .....                            | 93        |
| V.3.2      | Datenspeicher Hardware (Storage) .....                  | 95        |



# I Begrifflichkeiten

Nachfolgend werden die Grundbegriffe und deren Definition beschrieben.

## I.1 Verfügbarkeit (Availability)

Die Verfügbarkeit eines technischen Systems ist das Mass, dass das System bestimmte Anforderungen innerhalb eines Zeitrahmens erfüllt. Fehler, Ausfälle, Unterbrüche, Abschaltungen und viele andere Ursachen im System selbst oder in den Umsystemen können eine Nichtverfügbarkeit («downtime») verursachen.

Für BSA sind die Anforderungen oft durch ihre Funktionstüchtigkeit implizit bestimmt, d.h. solange eine Anlage funktioniert, ist sie verfügbar. Bei komplexen Systemen legt z.B. ein SLA (Service Level Agreement) die Anforderungen fest, damit das System als verfügbar gilt.

Die Geschäftsprozesse und somit die Systeme sollen möglichst unterbruchfrei bereitgestellt werden, um die Geschäftsziele zu erreichen. Somit muss die Verfügbarkeit auf die benötigte Betriebszeit ausgerichtet sein. Daraus folgt, dass der Zeitrahmen, in welchem das System die Anforderungen erfüllen muss, bei BSA 7x24 ist.

## I.2 Hochverfügbarkeit (High Availability)

Hochverfügbarkeit ist die Systemeigenschaft, eine hohe Verfügbarkeit aufzuweisen. Typische Werte der Verfügbarkeit betragen bei einem hochverfügbaren System 99.99% («four-9s») oder 99.999% («five-9s»), was im 7x24-Betrieb einer Nichtverfügbarkeit von 52 Minuten resp. 5.2 Minuten pro Jahr entspricht. Diese hohen Verfügbarkeitswerte lassen sich bei komplexen Systemen nur durch ein fehlertolerantes Design mit entsprechenden Redundanzen erreichen.

## I.3 Fehlertoleranz (Fault Tolerance)

Fehler im System (z.B. Hardwareausfälle, Kommunikationsverlust) führen dazu, dass das System den Anforderungen nicht genügt und somit nicht mehr als verfügbar gilt. Mittels Fehlertoleranz bleibt trotz eines Fehlers die Erfüllung der Anforderungen weiter gewährleistet. Ziel ist es, katastrophale Ausfälle zu verhindern, die durch einen einzelnen Fehlerpunkt (Single Point of Failure) verursacht werden könnten und der der Weiterbetrieb gewährleistet wird.

Fehlertoleranz fließt in das Systemdesign ein und deckt nur die Fehler ab, die im Design berücksichtigt wurden. Fehlertoleranz ist i.d.R. so designed sein, dass sie mehrere Fehler (z.B. Ausfall einer Spannungsversorgung und Ausfall eines Kommunikationspfades), auch gleichzeitig, abfängt.

## I.4 Redundanz (Redundance)

Mit Redundanz stehen zusätzliche Ressourcen (Hard- oder Software) bereit, die zur Erfüllung der Anforderungen nicht benötigt werden. Im Störfall werden sie aktiviert, um einen Weiterbetrieb zu gewährleisten. In der Regel sind die zusätzlichen Ressourcen Teilsysteme, die mehrfach vorhanden sind. Übliche Bezeichnungen sind «1:1», wenn eine Reserve-Ressource pro Ressource bereitsteht und «1:n», wenn nur eine Reserve-Ressource für n Ressourcen vorgehalten werden.

## I.5 Hot-Standby

Die Reserve-Ressource ist vollständig mit der aktiven Ressource synchronisiert für die sofortige Übernahme des Betriebes. Die Reserve-Ressource erfüllt die Anforderungen sofort, ohne dass sie sich mit angeschlossenen Systemen abgleichen muss («hit-less»).

Typischerweise überwacht ein unabhängiger Monitor die Ressourcen und leitet die Umschaltung («Switch-over») ein. In einfachen Architekturen überwachen sich die Ressourcen gegenseitig und sind selbst für die Umschaltung verantwortlich.

## **I.6 Cold-Standby**

Die Reserve-Ressource ist bis zum Ausfall passiv. Nach ihrem Start muss sie sich zuerst mit den angeschlossenen Systemen abgleichen. In dieser Abgleichperiode erfüllt die Reserve-Ressource die Anforderungen noch nicht und für die Umsysteme ist die Umschaltung sichtbar (nicht «hit-less»). Oft ist ein neuer Verbindungsaufbau notwendig oder Transaktionen müssen von Grund auf neu gestartet werden. Die Betriebsfähigkeit der Reserve-Ressource muss durch einen externen Anstoss erstellt werden, da weder die ausgefallene Ressource noch die passive Reserve-Ressource dazu verlässlich in der Lage ist. Ein manueller Eingriff ist nicht unüblich.

## **I.7 Daten- und Systemsicherung (Backup)**

Sowohl Die Daten- und Systemsicherung erstellt ein Abbild des Systemzustands zu einem definierten Zeitpunkt. Dieses Abbild kann die Daten oder auch die Systeme in den Zustand zu diesem Zeitpunkt zurücksetzen. Dadurch können Fehler in der Bedienung oder in der datenverarbeitenden Applikation rückgängig gemacht werden. Allerdings gehen auch alle übrigen Modifikationen seit der letzten Sicherung verloren und müssen erneut gemacht werden. Eine Systemsicherung erlaubt nebst dieser Rücksetzung auch eine Wiederherstellung auf einer anderen Hardware. Dadurch ist die Systemsicherung auch ein Mechanismus gegen Hardwareausfälle, auch wenn dabei grosser Datenverlust und eine lange Nichtverfügbarkeit in Kauf genommen wird.

Eine Archivierung erlaubt mit ähnlichen Mechanismen, Datensätze und Systemzustände über lange Zeiträume aufzubewahren. Hier steht nicht die Wiederherstellung im Vordergrund. Als Beispiel ist im Nachgang an Vorfälle (z.B. Forensik) so eine Rekonstruktion möglich oder ein lückenloser Audit-Trail ist nachweisbar.

## **I.8 Disaster-Recovery**

Nach einem Komplettausfall wird, gemäss den Prozessen und Wiederanlaufplänen (inkl. genauer System-Rangfolge), der Betriebszustand wieder erreicht.



## II Redundanzen

Die Redundanz hat zum Ziel, die Verfügbarkeit und die Wartbarkeit eines Systems, in diesem Fall die «Leit- und Steuersysteme der Betriebs- und Sicherheitsausrüstungen» auf Nationalstrassen zu erhöhen.

Durch die entsprechende Wahl des Netzwerkes (vgl. ASTRA Richtlinie 13040) und durch die entsprechende Systemarchitektur wird die Gesamtverfügbarkeit erhöht, indem Teile des Ganzen ausfallen können, ohne einen Totalausfall zu riskieren. Wie die Systemarchitektur ist auch die Kommunikationsarchitektur ein wesentliches Element zur Erhöhung der Verfügbarkeit.

Die nachfolgende Auflistung beschränkt sich auf die Verfügbarkeitserhöhung der OTTR-Rechner der AR und der AS.

Grundsätzlich wird die Verfügbarkeit der Kommunikationsmittel, der Applikationen und der Daten durch eine redundante hochverfügbare Umgebung erhöht (Hardware und Software als auch die Verwaltung der Elemente).

Die Redundanz kann auf verschiedenen Ebenen erreicht werden, hängt aber von den unterstützten Möglichkeiten der Hersteller ab und muss entsprechend geprüft werden:

- Software-Redundanz: Applikation, Datenbank, Applikations- Desktop- und/oder Servervirtualisierung mittels Hypervisor (je nach Hersteller unterschiedlich);
- Hypervisor-Zusatzfunktionen: High Availability (durch das Ressourcen-Sharing auf dem Hypervisor kann ein Hardwareausfall nahtlos überbrückt werden), Fault Tolerance (Schattensystem läuft synchron mit), automatisierte Lastverteilung u.a.;
- Hardware-Redundanz: Hardware-Cluster oder Verbund von zwei oder mehr Einheiten mit unterschiedlichen Realisierungsmöglichkeiten: Aktive/Passiv (Hot- oder Cold-Standy), Aktiv/Aktive (Synchron oder Hot-Standby).

### II.1 Applikationsredundanz

Häufig verfügen die eingesetzten Applikationen über eine eigene Redundanzmöglichkeit. In diesem Falle kann diese Redundanzmöglichkeit eingesetzt werden.

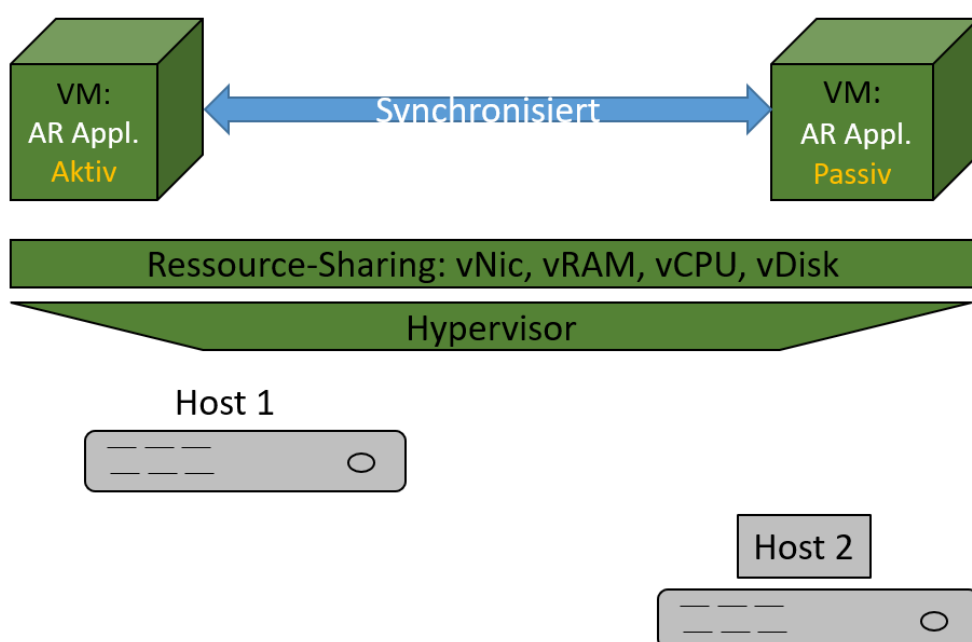


Abbildung II.1: AR-Applikationsredundanz

Die Abbildung II.1 zeigt eine Applikationslösung. Das Prinzip ist hierbei (vereinfacht):

- Beide Hosts (Host 1 und 2) sind aktiv (AR 1-1 und AR 1-2);
- Ein Guests (VM AR-Applikation auf VM AR 1-1) ist aktiv, der andere passiv (AR-Applikation auf VM AR 1-2);
- Die AR-Applikationen auf den Guest synchronisieren die Daten zueinander und überwachen sich gegenseitig;
- Bei einem Ausfall der aktiven Applikation wird «sofort» die passive Applikation aktiv.

Der Vorteil liegt darin, dass eine bewährte, funktionierende Redundanzlösung eingesetzt wird, welche vom Hersteller unterstützt wird. Der Hauptnachteil liegt in der Bedienung. Die Managementebene muss den aktiven AR kennen und entsprechend dem Zugriff steuern. Kommunikationstechnisch ist diese Lösung problemlos, da die Kommunikationslinien doppelt ausgeführt werden können (Bestandteil von OPC UA; Profinet Multi Controller, Multi Device; Modbus TCP Multi Client, Multi Server).

Der Host muss separat überwacht werden und wird unabhängig betrieben (VM AR 1-1 unabhängig zu VM AR 1-2).

## II.2 Weitere Erhöhung der Redundanz

Die Applikationsredundanz lässt unter Nutzung von zusätzlichen inneren Redundanzmechanismen der Virtualisierungsplattformen weiter erhöhen. Es lassen sich die Redundanzmechanismen miteinander verbinden, indem die AR-Applikation resp. der entsprechende Guest (VM) und die gleiche AR-Applikation (VM) als unabhängige Dienste konfiguriert werden. Ein Ausfall des Dienstes auf dem Host bewirkt einen Start des gleichen Dienstes auf einem anderen Host oder eine Verschiebung. Gleichzeitig erkennt aber die AR-Applikation auf dem Host den Ausfall der anderen AR-Applikation auf dem anderen Host und wird dadurch aktiv.

## II.3 High Availability Cluster (HA Cluster)

Mittels High Availability Clustern werden 2 oder mehr Rechner miteinander verbunden, so dass von «Aussen» gesehen nur 1 Rechner sichtbar ist. So dass bei einem Ausfall eines der Systeme ein anderes nahtlos genutzt werden kann, um die Verfügbarkeit des Dienstes oder der Anwendung aufrechtzuerhalten.

Tritt auf einem Rechner des Clusters ein Fehler auf, werden die auf diesem Rechner laufenden Dienste auf einen anderen Rechner migriert (automatisiert oder nach Bedarf manuell). Alle kritischen Elemente (RAM, Netzwerkkarten, CPUs, Disks, PowerSupplies, usw.) sind mindestens doppelt vorhanden. Alle Rechner greifen auf die gleiche Datenbasis zu.

Diese Lösung wird von marktführenden Hypervisor-Anbietern unterstützt (Zusatzmodule für vSphere, Hyper-V Server, etc.) und kann als Redundanzmöglichkeit eingesetzt werden.

Im Gegensatz zur Applikationsredundanz ist der HA-Cluster eine klassische Informatiklösung und keine Applikationslösung. Die HA-Cluster Lösung benötigt einen höheren Hardwareeinsatz (2 Rechner, mehrere Netzwerke pro Rechner) und einen zusätzlichen Konfigurationsaufwand (Bestimmung der Dienste und Ressourcen für die Überwachung). Dafür ist die HA-Lösung nicht herstellerspezifisch in Bezug auf die AR-Applikation, und ist eine gängige und verbreitete Lösung in Informatikumgebungen.

## II.4 Failover Cluster

Mit Hilfe des erweiterten HOST-Operatingssystem lassen sich Hochverfügbarkeitscluster realisieren, auch «Failover-Cluster» genannt. Der Failover-Cluster bietet eine hohe Ausfallsicherheit durch Redundanz.

In einem Failover-Cluster sind die kritischen Komponenten redundant ausgeführt. Fällt eine Komponente in einem Rechner aus, übernimmt die redundante Komponente des anderen Rechners die Funktion. Je nach Konstellation können im Failover-Cluster beide Rechner (Knoten), der primäre und der sekundäre, aktiv sein und eine Lastverteilung durchführen. Es kann allerdings auch nur einer aktiv und der andere passiv sein und im Standby betrieben werden.

Diese Cluster sind von «Aussen» als ein Rechner mit mindestens einer virtuellen Maschine AR sichtbar.

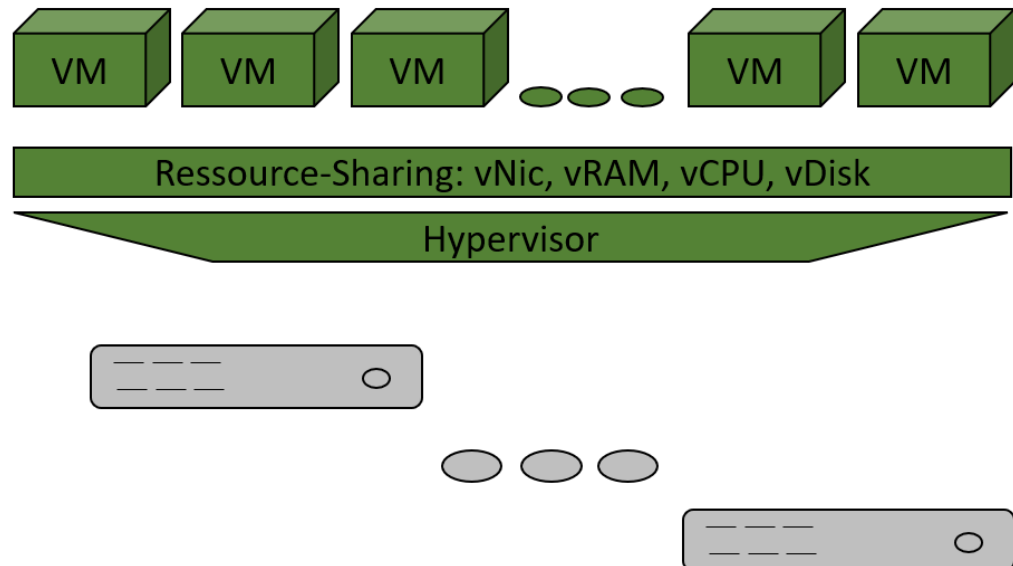


Abbildung II.2: Failover-Cluster

Beim Failover-Cluster werden die virtuellen Maschinen innerhalb des Clusters betrieben, sind also von «Aussen» nur als ein Rechner sichtbar. Die gesamte Redundanz-Verwaltung übernimmt der Failover-Cluster.

## II.5 Cluster mit virtuellem SAN (Storage Area Network)

In dieser Funktion wird der vorhandene Datenspeicher für alle Rechner bereitgestellt und gemeinsam genutzt (VSAN).

Das Prinzip ist hierbei (stark vereinfacht):

- Immer ein Element ist aktiv (z.B. eine Kommunikationsschnittstelle);
- Jeder Knoten überwacht seine spezifischen Dienste und seine spezifische Hardware;
- Die 2 Hosts tauschen meistens über ein spezielles Netzwerk die Zustandsdaten aus;
- Bei Unregelmäßigkeiten übernimmt der jeweils andere Knoten die nötigen Dienste und stellt die nötige Hardware zur Verfügung;
- Die Harddisks im Rechner 1 und im Rechner 2 werden logisch (virtuell) zu «einer Disk» zusammengefasst.

## II.6 Fault Tolerance (FT)

Bei Verwendung von Fault Tolerance werden die Hardware-Ressourcen über zwei Server gespiegelt und sämtliche Befehle redundant auch auf dem Spiegelsystem ausgeführt. Fällt der Master-Server aus, übernimmt der Slave die weitere Verarbeitung der laufenden Anwendungen in Echtzeit.

## II.6.1 AR Redundanzvergleich

Zugelassen sind die Applikationsredundanz, der HA-Cluster und die gemischte Redundanz. Die nachfolgende Tabelle ist nicht abschliessend und liefert nur rudimentäre Entscheidungsgrundlagen.

*Tabelle II.3: AR-Redundanzvergleich*

| Anforderung / Verfügbarkeit        | Applikations-Redundanz | HA-Cluster | Gemischte Redundanz | Bemerkung  |
|------------------------------------|------------------------|------------|---------------------|--|
| Netzwerk Konfiguration             | Tief                   | Normal     | Hoch                |  |
| Netzwerk Betrieb                   | Tief                   | Tief       | Tief                |  |
| Unterhalts-personal                | Tief                   | Tief       | Hoch                | Ausgangslage, Zusammensetzung Personal kann sich mit der Zeit ändern |
| OT Support                         | Tief                   | Hoch       | Hoch                |  |
| Verbreitung OT                     | Sehr tief              | Sehr hoch  | Sehr tief           | Wissen auf dem «Markt»   |
| Kosten Hardware                    | Mittel                 | Hoch       | Hoch                |  |
| Kosten Systemsoftware              | Hoch                   | Hoch       | Sehr Hoch           |  |
| Verfügbarkeit                      | Hoch                   | Sehr hoch  | Sehr Hoch           |  |
| Backup / Restore                   | Normal                 | Tief       | Normal              |  |
| Datenhaltung                       | Normal                 | Normal     | Normal              |  |
| Update Betriebssystem (Sicherheit) | Hoch                   | Tief       | Sehr hoch           |  |
| Ersatzaufwand                      | Hoch                   | Tief       | Sehr Hoch           |  |
| Verfügbarkeit auf dem Markt        | Hoch                   | Sehr Hoch  | Hoch                |  |
| SCADA Wissen                       | Mittel                 | Hoch       | Mittel              | 1)   |

1) Für einen reibungslosen HA-Clusterbetrieb muss der Cluster genau wissen, welche Dienste / Prozesse wie überwacht werden müssen. Oftmals fehlt dieses Wissen bei den Lieferanten, da häufig «fertige» Software entweder eingekauft oder eigene fertige Software eingesetzt wird. Dies ist beim Einsatz spezifisch zu klären

Es wird eine Redundanz gemäss den obigen Kapiteln gefordert. Die Ausprägung wird der Gebietseinheit überlassen und hat auf die Einbindung in die regionale Managementebene wie auch zur Verbindung in die Anlagenebene keine wesentlichen Auswirkungen.

### III Grundlagen Virtualisierung

#### III.1 Virtualisierungsplattform

Mit der Virtualisierung wird die Hardwarebindung neutralisiert. D.h. es wird mittels einer Software-Zwischenschicht (Hypervisor) die Hardware emuliert. Dies ermöglicht die Kompatibilität des virtualisierten Rechners zu den verschiedenen Herstellern von Server-Hardware zu erhöhen und zugleich die Wartung zu vereinfachen. Mit dem virtuellen Verbund über den Hypervisor werden die vorhandenen physischen Ressourcen verwaltet und den Virtuellen Maschinen (VM) zur Verfügung gestellt.

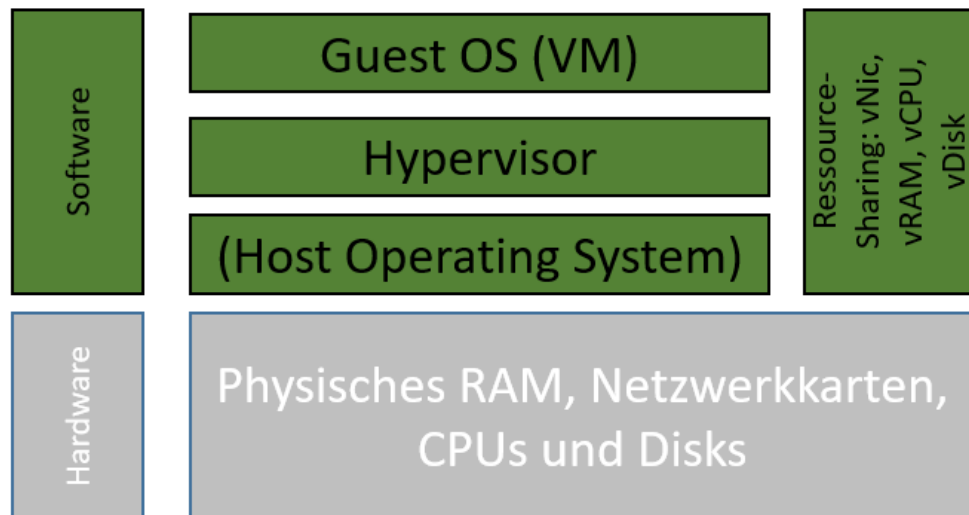


Abbildung III.4: Aufbau Virtualisierungsplattform (Schematisch)

Nachfolgen die wichtigsten Funktionen:

- Effiziente Nutzung aller vorhandenen Ressourcen;
- Server-Herstellerunabhängigkeit;
- Hard- und Software-Wartung wird vereinfacht und kann im laufenden Betrieb erfolgen;
- Backup und Disaster-Recovery kann einfacher realisiert werden (siehe nächstes Kapitel).

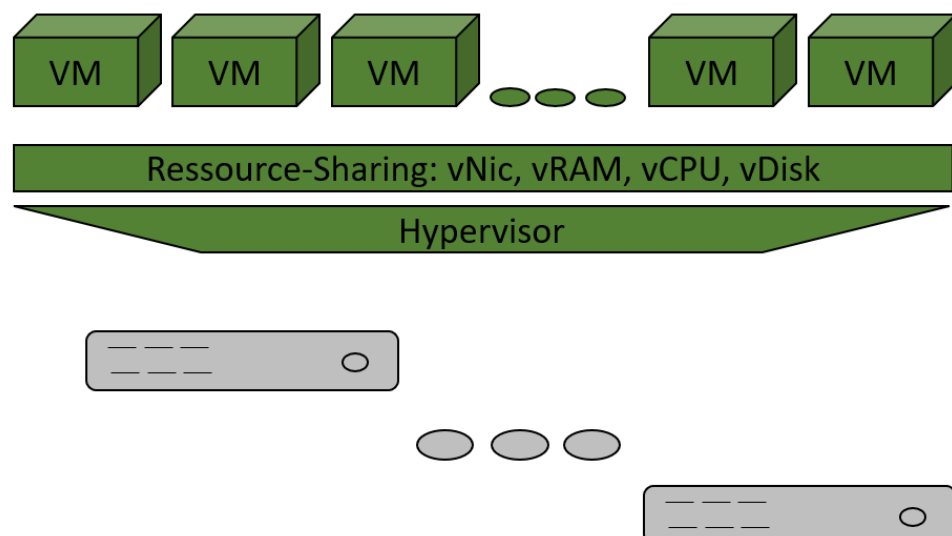


Abbildung III.5: Virtualisierungsplattform schematisch

Jede Virtualisierungsplattform besteht aus mehreren Rechner-Hardware-Sets (gemäss Abbildung III.5), d.h.:

- Virtualisierungsplattform im OT-Technikraum (OTTR) und technische Zentrale: Mindestens je 3 Rechner-Hardware;
- Virtualisierungsplattform im technischen Raum oder kleinen Objekten (beispielsweise Tunnel unter 600 m): Mindestens je 2 Rechner-Hardware.

Es sind zwei Arten der Virtualisierung zugelassen:

- Virtualisierung mittels Hostoperatingsystem und/oder Virtualisierungssoftware getrennt. Beispiel: Microsoft Hyper-V mit Microsoft Windows Server;
- Virtualisierung mittels Host- und/oder Virtualisierungssoftware zusammengefasst. Beispiel: VMware vSphere.

## IV Systemarchitektur Schweiz (SA-CH)

## IV.1 Architektur SA-CH

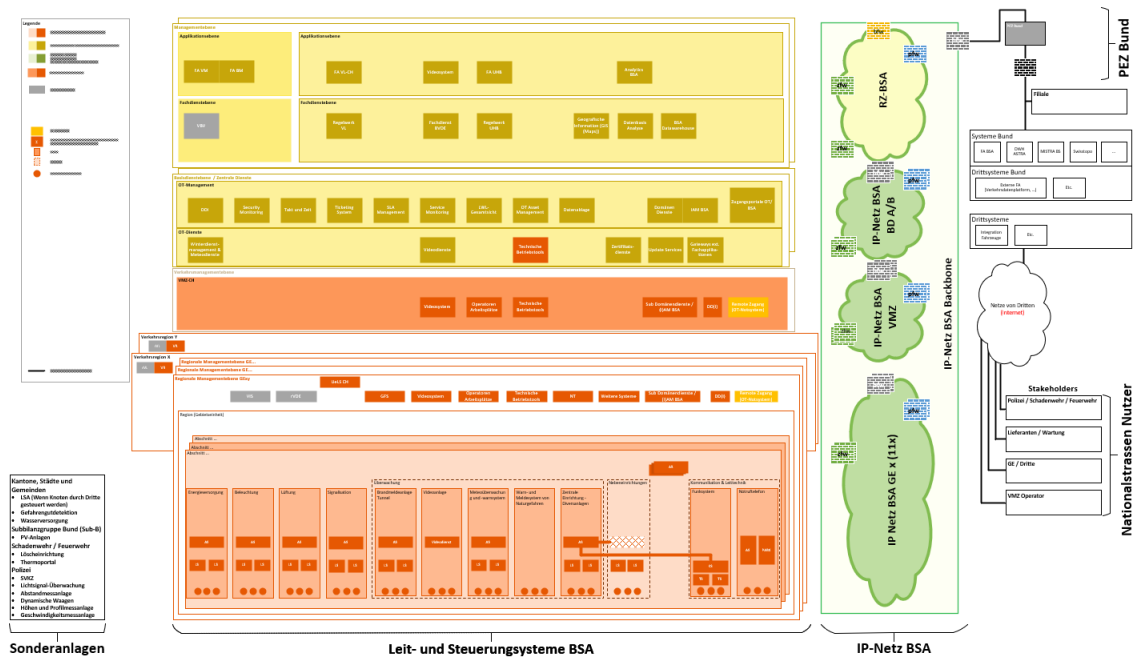




Abbildung IV.6: Architektur SA-CH (Darstellung Abschnitt: Maximale Anzahl an Anlagen im Tunnel)

## IV.2 Architektur SA-CH GUI/MMI-Umsetzung

In der nachfolgenden Übersicht sind sowohl die GUI () als auch MMI () Benutzeroberflächen ersichtlich. Wie im Kapitel 5.2.3 erläutert ist, sind MMI-Umsetzungen gemäss Styleguides ASTRA für alle Fachapplikationen verpflichtend zu berücksichtigen. Standardkomponenten und Standard-Tools, wie z.B. NMS können mit dem Standard-GUI umgesetzt werden.

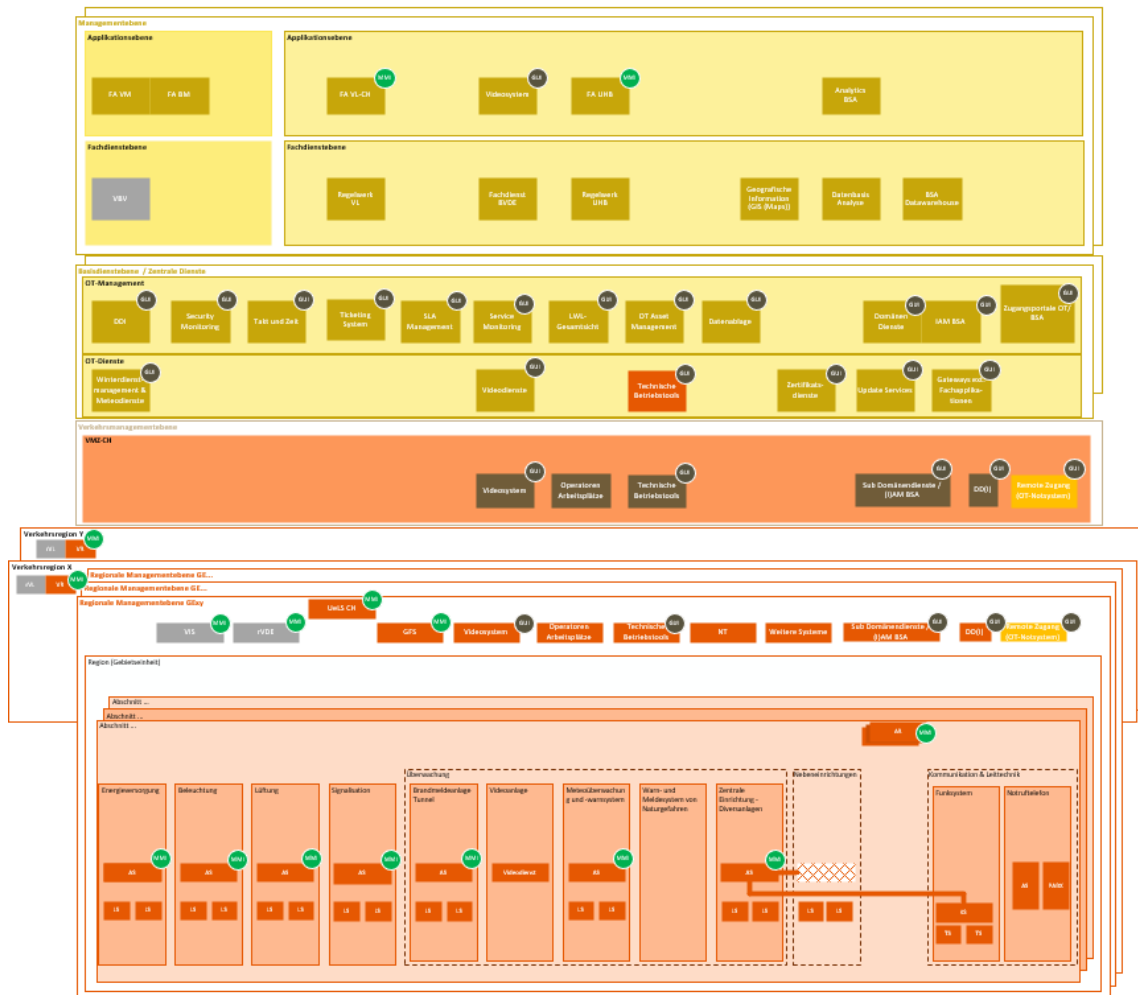


Abbildung IV.7: Architektur SA-CH mit MMI/GUI



## V Technologieanwendungen

### V.1 Technologieanwendungen einer Röhre

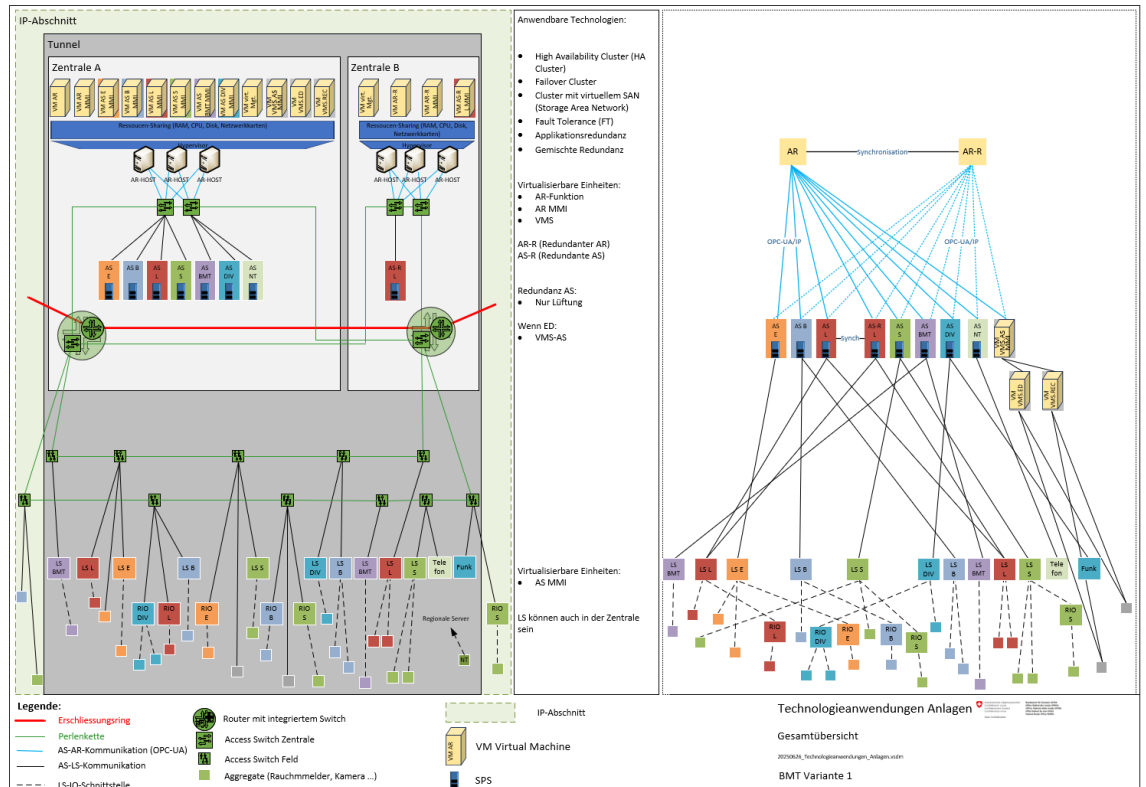


Abbildung V.8: Gesamtübersicht - Technologieanwendungen einer Röhre - Variante 1

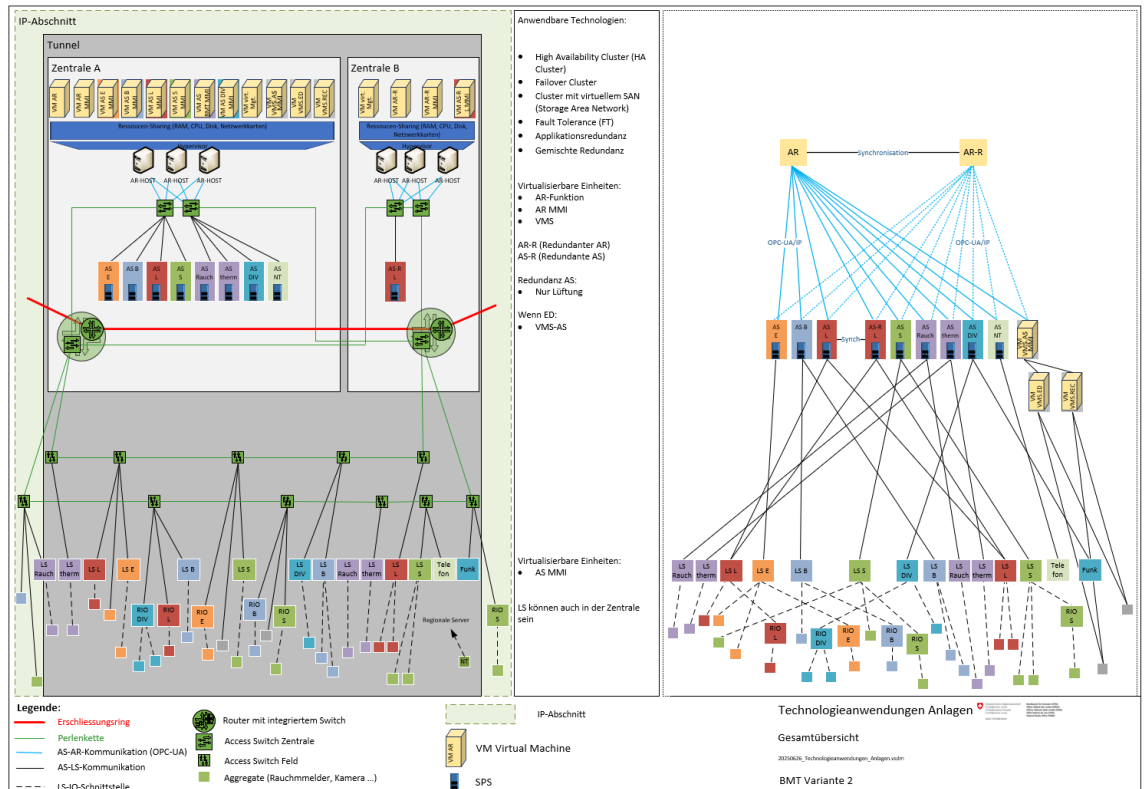


Abbildung V.9: Gesamtübersicht - Technologieanwendungen einer Röhre - Variante 2

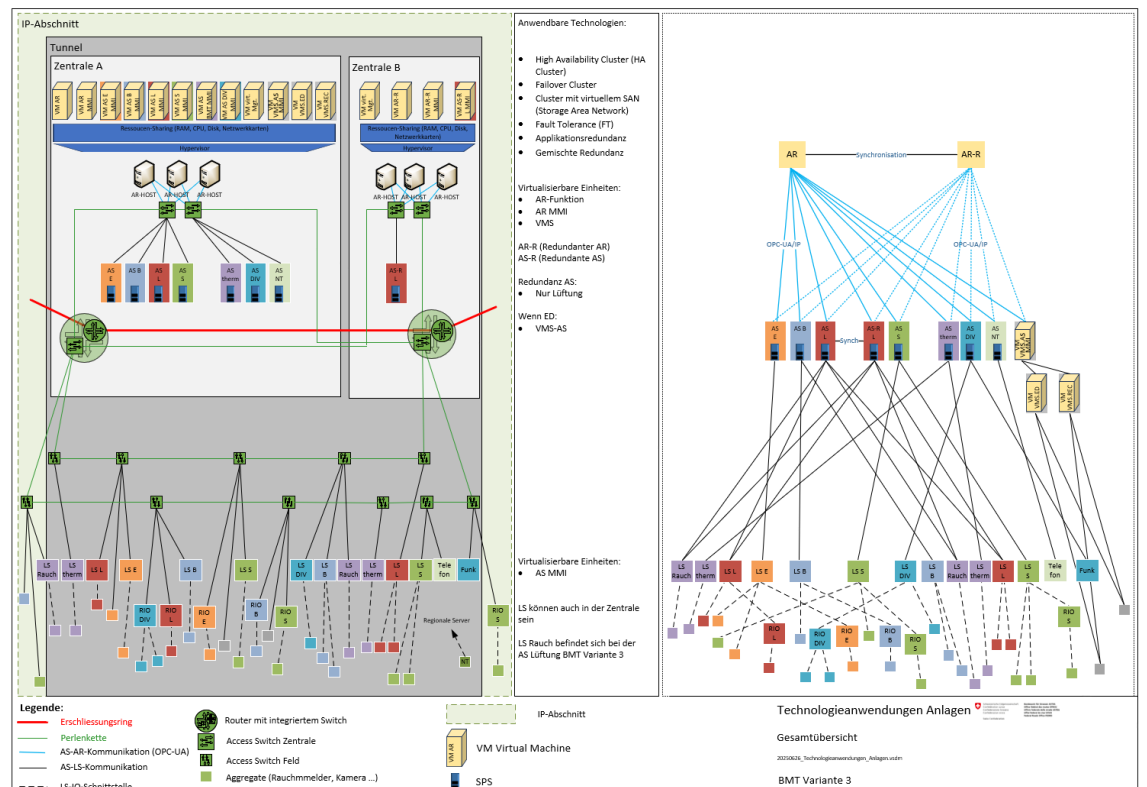


Abbildung V.10: Gesamtübersicht - Technologieanwendungen einer Röhre - Variante 3

## V.2 Technologieanwendungen zwei Röhren

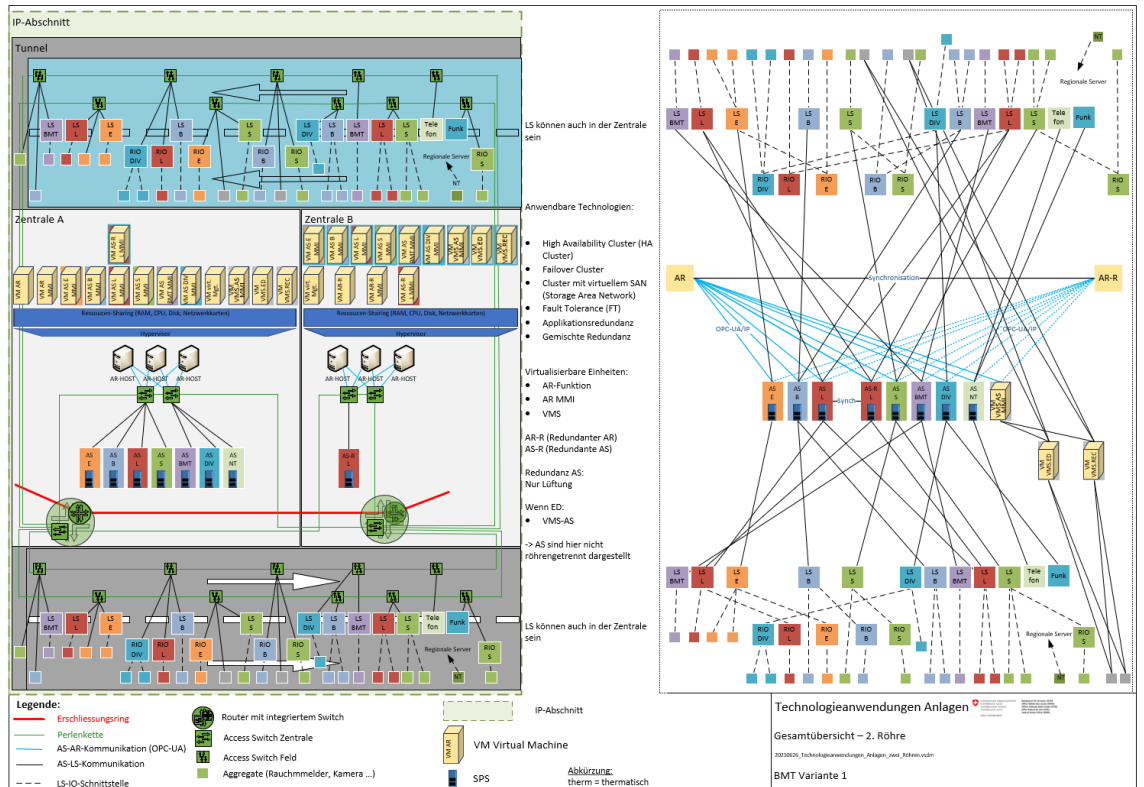


Abbildung V.11: Gesamtübersicht - Technologieanwendungen zwei Röhren - Variante 1

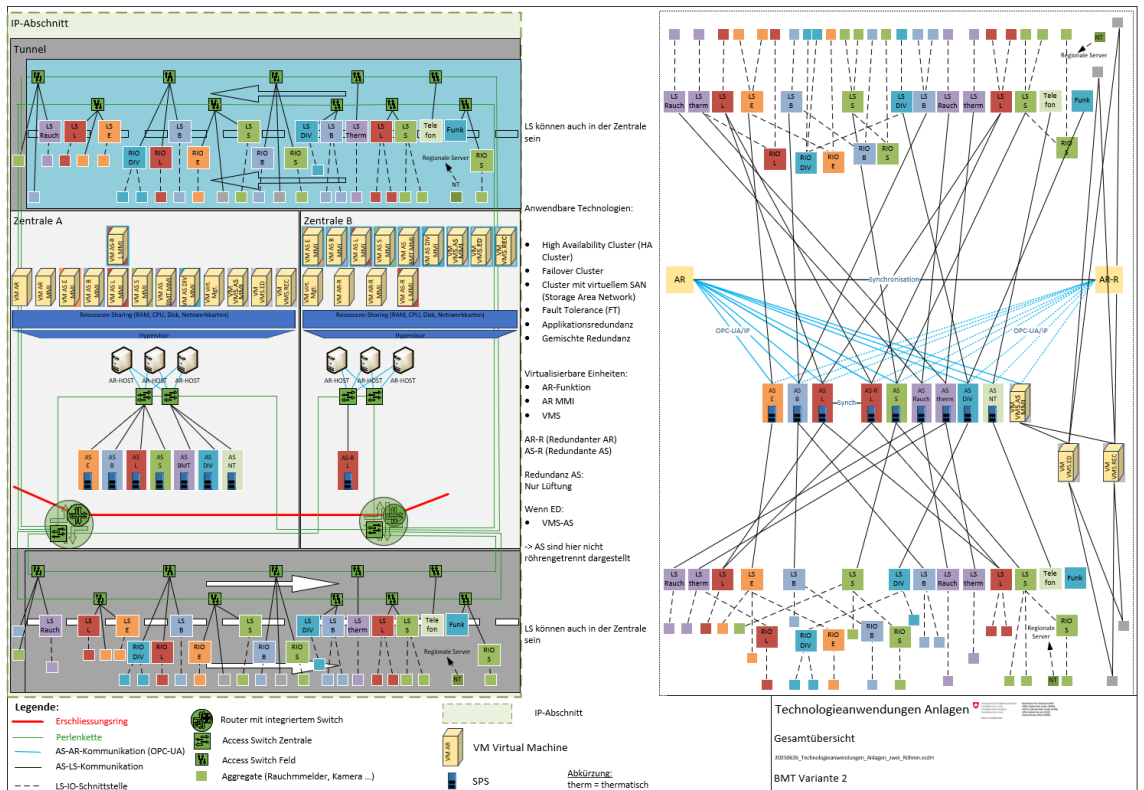


Abbildung V.12: Gesamtübersicht - Technologieanwendungen zwei Röhren - Variante 2

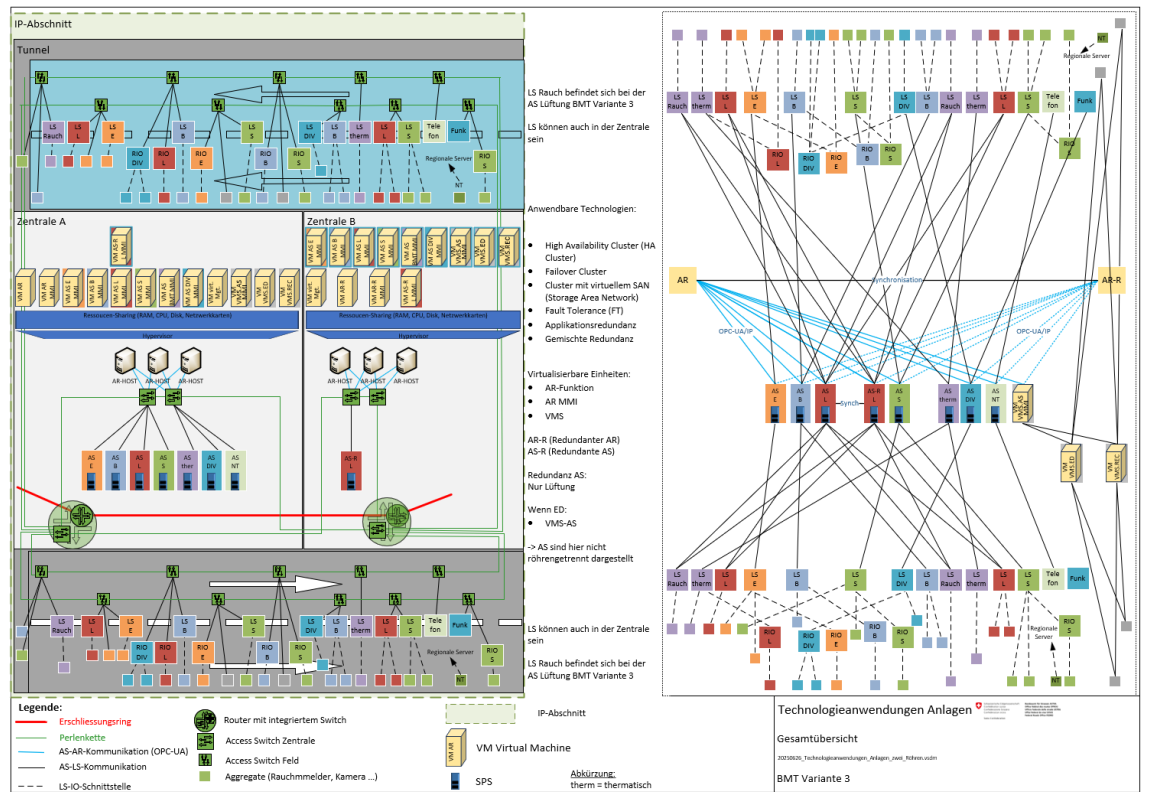


Abbildung V.13: Gesamtübersicht - Technologieanwendungen zwei Röhren - Variante 3

## V.3 Berechnungsbeispiel für Hardwareressourcen

### V.3.1 HOST-Hardware (Server)

Die Dimensionierung der Rechner-Hardware hängt vom effektiven Einsatzzweck ab. Rechner-Hardware ist somit in OT-Technikräumen, Technikräumen/Technischen Zentralen unterschiedlich je nach Anforderung zu wählen. Die wichtigsten sogenannten Hardwareressourcen sind nachfolgend (nicht abschliessend) aufgelistet:

- Prozessoren (Achtung dies hat teilweise Einfluss auf die Softwarelizenzierung);
- Arbeitsspeicher (RAM);
- Harddisks;
- Netzwerkkarten.

Im Grundsatz müssen mindestens jeweils 2 Einheiten vorhanden sein. Je nach Einsatzzweck ein Vielfaches davon.

Die Minimalanforderungen werden seitens Betriebssystemhersteller als auch Applikations- oder Datenbankhersteller bekanntgegeben.

#### Beispiel

Um Anforderungen an die Rechner-Hardware zu definieren, kann grob folgendes angewendet werden:

1. Anforderungen aller VM zusammentragen;
2. 50% Reserve dazurechnen für weitere VMs oder kurzzeitig erhöhte Belastungen vorzusehen;
3. Summe der Anforderung an einer HOST-Hardware;
4. Von den theoretisch verfügbaren Kapazitäten 25% subtrahieren, dies ergibt grob die effektiv nutzbare Ressource.

#### Beispiel RAM

*Tabelle V.14: Beispiel RAM*

| Anforderung                  | RAM [GB]   |   |
|------------------------------|------------|---|
| Betriebssystem HOST          | 24         |   |
| VM 1                         | 24         |   |
| VM 2                         | 48         |   |
| VM 3                         | 48         |   |
| VM 3                         | 96         |   |
| Total                        | 240        |   |
| Reserve 50%                  | 120        |   |
| Total inkl. Reserve          | 360        | Pro HOST-Hardware   |
| Zuzüglich 25%                | 90         | Aufrechnung damit die effektive Nutzbarkeit erreicht wird |
| Total bereinigte Anforderung | <b>450</b> | Pro Rechner-Hardware (Bestellwert)                        |
| Abzüglich 25%                | <b>-90</b> | Subtraktion Systemverlust                                 |
| Total effektive Nutzbarkeit  | <b>360</b> | Effektiver nutzbarer Wert                                 |

**Beispiel mit 2- und 3er HOST-Sets***Tabelle V.15: Beispiel mit 2- und 3er HOST-Sets*

| <b>Berechnung RAM [GB]</b>                           | <b>Total</b> | <b>Total 2er Set</b> | <b>Total 3er Set</b> |
|--|--------------|----------------------|----------------------|
| Betriebssystem HOST                                  | 16           | 32                   | 48                   |
| Betriebssystem Gest (VM 1)                           | 16           | 32                   | 48                   |
| Betriebssystem Gest (VM 2)                           | 16           | 32                   | 48                   |
| Betriebssystem Gest (VM 3)                           | 16           | 32                   | 48                   |
| Applikation (VM 1)                                   | 32           | 64                   | 96                   |
| Applikation (VM 2)                                   | 24           | 48                   | 72                   |
| Datenbank (VM 3)                                     | 64           | 128                  | 192                  |
| <b>Total</b>   | <b>184</b>   | <b>368</b>           | <b>552</b>           |
| Reserve (Ausfall 1 Server-Hardware)                  |              | 368                  | 552                  |
| Reserve (Wartung 1 Server-Hardware)                  |              | 368                  | 552                  |
| <b>Total für Abdeckung Ausfall 1 Server</b>          |              | <b>736</b>           | <b>1104</b>          |
| <b>Total für Abdeckung Wartung 1 Server</b>          |              | <b>736</b>           | <b>1104</b>          |
| <b>Total für Ausfall und Wartung von je 1 Server</b> |              |                      | <b>1656</b>          |

Diese Tabelle berücksichtigt die Tabelle V.164 nicht. Somit muss für den effektiven Be stellwert zusätzlich 25% addiert werden.

### V.3.2 Datenspeicher Hardware (Storage)

Die Dimensionierung der Datenspeicher-Hardware hängt vom effektiven Einsatzzweck ab. Datenspeicher-Hardware ist somit in OT-Räumen, Technikräumen usw. unterschiedlich je nach Anforderung zu wählen. Die wichtigsten sogenannten Berechnungsgrundlagen sind nachfolgend (nicht abschliessend) aufgelistet:

- Harddisks;
- Netzwerkkarten.

Die effektive Nutzbarkeit von Harddisk oder Speichermedien berechnet sich wie folgt (Annäherungsrechnung).

*Tabelle V.17: Effektive Nutzbarkeit von Harddisk oder Speichermedien*

| Beispiel Berechnung Speicher [GB]  | Total pro Harddisk | Total mit 3 Harddisks | Bemerkung                |
|--|--------------------|-----------------------|--------------------------|
| Rohkapazität   | 300                | 900                   |                          |
| Bruttokapazität (ca. 90%) (System eigene Nutzung abgezogen)                                      | 270                | 810                   |                          |
| Kapazitätsgewinnung bei Verwendung von Deduplizierung und Komprimierung sind Herstellerabhängig. |                    |                       |                          |
| Ab Bruttokapazität   | Nutzbar:           |                       |                          |
| Netto bei RAID 0   |                    | 810                   | Keine Fehlertoleranz     |
| Netto bei Raid 1   |                    | 270                   | 2 Disk Fehler auffangbar |
| Netto bei RAID 5   |                    | 540                   | 1 Disk Fehler auffangbar |
| Netto bei RAID 10 als auch RAID 6 und 60   |                    | -                     | Mindestens 4 Disk        |





# Glossar

| Begriff/Abkürzung   | Terme/abréviation       | Bedeutung  |
|---------------------|-------------------------|--|
| (BSA) Abschnitt     | section (EES)           | logischer Abschnitt für BSA, nicht der Streckenabschnitt   |
| (Netzwerk-) Segment | segment (de réseau)     | Segmente gemäss ASTRA 83040 (meist VLAN)   |
| (Netzwerk-)Zone     | zone (de réseau)        | im Sinne der NSP des Bundes Si003 (getrennt durch PEZ)   |
| (Teil-)Anlage       | (partie d')installation | nur im Sinn der AKS-Definitionen gebraucht   |
| Access-Bereich      | niveau accès            | L2-Struktur, die den Zugang (Userport) den Endgeräten bereitstellt   |
| ABX                 | ABX                     | Kurzform für Abraxas   |
| AD                  | AD                      | Active Directory   |
| AI                  | AI                      | Künstliche Intelligenz (engl. Artificial Intelligence)   |
| AKS-CH              | AKS-CH                  | Struktur und Kennzeichnung der Betriebs- und Sicherheitsausrüstungen   |
| AR                  | AR                      | Abschnittsrechner  |
| AS                  | AS                      | Anlagensteuerung   |
| Ausrüstung/Gerät    | équipement              | Jede Art von aktiven Geräten im BSA-Umfeld (auch ohne Verbindung zum IP-Netz BSA)  |
| AWL                 | liste d'instructions    | Anweisungsliste  |
| B                   | B                       | Beleuchtung  |
| Backbone/BB         | backbone/BB             | Vom Bund (L3 durch BIT, Übertragung durch FUB) bereitgestellte nationale Vernetzung aller Teilnetze  |
| BD (Basisdienste)   | BD (services de base)   | Netzwerk-Basisdienste (IPAM-Tool, DNS, Zeitquellen, ...) für das gesamte IP-Netz BSA   |
| BIT/ KdoCy          | OFIT/ cdmt Cyber        | Bundesamt für Informatik und Telekommunikation / Kommando Cyber  |
| BLI                 | BLI                     | Blinker  |
| BLZ                 | BLZ                     | Betriebsleitzentrale   |
| BM                  | BM                      | Baustellenmanagemnt  |
| BMT                 | BMT                     | Brandmeldeanlage Tunnel (BMT)  |
| BSA                 | EES                     | Betriebs- und Sicherheitsausrüstungen  |
| BSA-Abschnitt       | section EES             | Von einem Abschnittsrechner gesteuerter Abschnitt der Nationalstrasse  |
| BSA-Region          | région EES              | Anlagenspezifisch definierte Region, in der es eine regional übergeordnete Steuerung gibt  |
| BVDE                | BVDE                    | Betriebs- und Verkehrsdaten Erhebung   |
| CA                  | CA                      | Zertifizierungsstelle (engl. Certificate Authority)  |
| CAB                 | CAB                     | Change Advisory Board  |
| KAM                 | KAM                     | Kamera   |
| Client/Host         | client/hôte             | allgemeine ICT-Begriffe (keine BSA-spezifische Bedeutung), Verwendung bei der Beschreibung von Protokollen   |
| DDI                 | DDI                     | DNS-, DHCP-, IP-Adress-Management-Tool   |
| DHCP                | DHCP                    | Dynamic Host Configuration Protocol  |
| Dienst              | service                 | Dienst ist ein Obergriff sowohl für Fachdienste wie auch für Basisdienste. Dienste implementieren Zugriffs- und Verarbeitungslogik, verfügen aber nicht über eine Benutzeroberfläche.  |
| DIV                 | DIV                     | Zentrale Einrichtung Diversanlagen   |
| DNS                 | DNS                     | Das Domain Name System (DNS) ist einer der wichtigsten Dienste in vielen IP-basierten Netzwerken. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung. Das DNS funktioniert ähnlich wie eine Telefonauskunft. |

| Begriff/Abkürzung  | Terme/abréviation  | Bedeutung   |
|--|--|---|
| Domäne   | domaine  | Die Domäne ist ein Bereich um Dinge zu ordnen oder zusammen zu fassen. Beim ASTRA wird die Domäne verwendet für:<br>Namensraum: Innerhalb eines Namensraums sind Identitäten eindeutig, d.h. es gibt nicht mehrere Identitäten für die gleiche Ressource.<br>Funktionsdomäne: Zusammenfassung verschiedener Funktionen.<br>Fachdomäne: Zusammenfassung verschiedener Fachdienste.<br>Prozessdomäne: Zusammenfassung verschiedener Prozesse. |
| DWH  | DHW  | Datawarehouse   |
| E  | E  | Energieversorgung   |
| ELZ  | ELZ  | Einsatzleitzentrale (der Polizei).  |
| Endgerät   | équipement terminal  | jede Art von Ausrüstung an einem Userport des IP-Netzes BSA   |
| F/Filiale  | F/filiale  | Filiale (fünf regionale Einheiten des ASTRA)  |
| FA   | application métier   | Fachapplikation   |
| FAT  | FAT  | Factory Acceptance Test   |
| FBS  | bloc fonctionnel   | Funktionsbaustein   |
| FE   | FE   | Funkanlage  |
| Firewall   | firewall/pare-feu  | Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.  |
| FIT  | FIT  | Factory Integration Test  |
| FLS  |  |   |
| FT   | FT   | Fault Tolerance   |
| FUB  | FUB  | Führungsunterstützungsbasis heisst heute Kommando Cyber   |
| G  | G  | Geschwindigkeitssignal  |
| GE   | UT   | Gebietseinheit (11 überkantonale organisatorischen Einheiten, die ihr eigenes IP-Netz BSA GE betreiben)   |
| GFS  | GFS  | Meteoüberwachungs und -warnsystem (auch Glatteisfrühwarnsystem genannt)   |
| GHGW   | GHGW   |   |
| GIS  | GIS  | Geoinformationssystem   |
| GS   | GS   | Gefahrensignal  |
| GUI  | GUI  | Graphical User Interface (hier gleichbedeutend wie MMI jedoch ohne ASTRA-spezifische Anpassungen, d.h. Hersteller-Standard)   |
| HA Cluster   | HA Cluster   | Hight Availability Cluster  |
| HCI  | HCI  | Hyperconverged Infrastructure   |
| IAM BSA  | IAM BSA  | Identity Management System BSA  |
| IKT  | IKT  | Informations- und Kommunikationstechnik   |
| IP   | IP   | Internet Protokoll  |
| IP-Abschnitt   | IP-section   | logischer Abschnitt für die Perlenketten  |
| IPAM   | IPAM   | IP Address Management   |
| IPC  | IPC  | Industriecomputer   |
| IP-Netz BSA<br>GE<br>GE Abschnitt<br>BD<br>VMZ<br>Backbone | réseau IP EES<br>UT<br>UT section<br>BD<br>VMZ<br>Backbone | Ein IP-Netz für die Betriebs- und Sicherheitsausrüstungen der Nationalstrassen mit folgenden Elementen (Teilnetzen):<br>- 11 IP-Netze BSA GE<br>- dem IP-Netz BSA Backbone (Backbone der Bundesverwaltung)<br>- Verbindungen zur VMZ-CH<br>- Verbindungen zu den Rechenzentren BSA<br>- Verbindungen zu den BD (Basisdiensten des IP-Netz BSA)  |
| ISBO   | ISBO   | Informatiksicherheitsbeauftragter der Organisation  |

| Begriff/Abkürzung                          | Terme/abréviation           | Bedeutung  |
|--|-----------------------------|--|
| ISO  | ISO                         | Information Security Officer   |
| KoP  | schéma à contacts           | Kontaktplan  |
| L  | L                           | Lüftung  |
| LDAP                                       | LDAP                        | Lightweight Directory Access Protocol  |
| Leitebene                                  | niveau gestion              | Siehe Prozessleitebene   |
| Leitsystem                                 | système de gestion          | Dient dem Bedienpersonal zur Überwachung und Leitung von Anlagen   |
| Leittechnik                                | système de commande/gestion | Funktionen und Komponenten, die der Überwachung und Leitung von Anlagen dienen.  |
| LS   | LS                          | Lokalsteuerung   |
| LWL  | LWL                         | Lichtwellenleiter  |
| Management-Ebene (auch Mgmt-Ebene oder ME) | niveau management (ou ME)   | zentrale, übergeordnete Leitebene  |
| MDT  | MDT                         | Mittlere Wiederherstellzeit (engl. mean down time)   |
| MMI  | MMI                         | Man Machine Interface (jedoch mit ASTRA-spezifische Anpassungen)   |
| Monitoring                                 | monitoring                  | Überwachung und Visualisierung der technischen Funktionen der Anlagen und Leitsysteme.   |
| MTTR                                       | MTTR                        | Mittlerer Zeitbedarf (engl. mean time to repair)   |
| N  | N                           | Nebeneinrichtung   |
| NCSC -> BACS                               | NCSC -> BACS                | Nationales Zentrum für Cybersicherheit (National Cyber Security Centre)-> Bundesamt für Cybersicherheit  |
| NMS  | NMS                         | Network Management System  |
| NT   | NT                          | Notruftelefonanlage  |
| NTP  | NTP                         | Network Time Protocol  |
| OBNB                                       | OBNB                        | Optische Behördennetz Bund   |
| OPC UA                                     | OPC UA                      | Open Platform Communications Unified Architecture  |
| OPC  | OPC                         | Open Platform Communications   |
| OT   | OT                          | Operational Technology   |
| OTTR                                       | OTTR                        | Operational Technology Technikraum   |
| PEP  | PEP                         | Sicherheitselemente / Policy Enforcement Point   |
| PEZ  | PEZ                         | Vorgelagerte Sicherheitszone, die von aussen den Zugriff unter weniger hohen Auflagen zulässt, als die nachgelagerten inneren Zonen mit höherem Schutzbedarf (aus dem Englischen für Policy Enforcement Zone). Dies entspricht ausserhalb der Bundesverwaltung der DMZ (Demilitarized Zone).   |
| PKI  | PKI                         | Public Key Infrastructure. Es handelt sich um ein System, das die Ausstellung, Verwaltung und Überprüfung von digitalen Zertifikaten ermöglicht, welche für die sichere Kommunikation und Authentifizierung im Internet verwendet werden. PKI wird eingesetzt, um Daten zu verschlüsseln, digitale Signaturen zu erstellen und die Identität von Benutzern, Geräten oder Diensten zu überprüfen. |
| Portalrot                                  | rouge au portail            | Rotlicht am Tunnelleingang (Portal)  |
| Prozessleitebene                           | niveau processus            | Begriff aus der Leittechnik: In dieser Ebene erfolgen die Überwachung und Bedienung aller Anlagesteuerungen und die übergeordnete Steuerung (Tunnelreflexe) innerhalb eines Abschnitts mittels eines Abschnittsrechners.   |
| PUN  | R-BAU                       | Pannestreifenumnutzung   |
| RaDo                                       | RaDo                        | Rampendosierung / Rampenbewirtschaftung  |
| RTSP                                       | RTSP                        | Real-Time Streaming Protocol   |
| rVDE                                       | rVDE                        | regionale Verkehrsdatenerfassung   |
| rVL  | rVL                         | regionale Verkehrslenkung  |

| Begriff/Abkürzung          | Terme/abréviation          | Bedeutung  |
|----------------------------|----------------------------|--|
| RZ(-BSA)                   | RZ(-BSA)                   | Rechenzentrum BSA  |
| S                          | S                          | Signalisation  |
| SA-CH                      | SA-CH                      | Systemarchitektur Schweiz  |
| SAN                        | SAN                        | Storage Area Network   |
| SAP                        | SAP                        | Service Access Point: Im IP-Netz BSA ist dies i.d.R. ein physischer Port eines Switches oder Routers.  |
| SAT                        | SAT                        | Site Acceptance Test – Abnahme beim Endinstallationsplatz, d.h. beim Kunden  |
| Server                     | serveur                    | allgemeine ICT-Begriffe (keine BSA-spezifische Bedeutung), Verwendung bei der Beschreibung von Protokollen   |
| Service                    | service                    | Siehe Dienst   |
| SISTO                      | SISTO                      | Sicherheitsstollen   |
| SIT                        | SIT                        | Site Integration Test  |
| SLA                        | SLA                        | BSA Service Level Agreement  |
| SMS                        | SMS                        | Security Management System   |
| SNMP                       | SNMP                       | Simple Network Management Protocol   |
| SOC                        | SOC                        | Security Operation Center  |
| SPS                        | SPS                        | Speicherprogrammierbare Steuerung  |
| SSO                        | SSO                        | Single Sign On   |
| ST                         | ST                         | Strukturierter Text  |
| U                          | U                          | Überwachungsanlagen  |
| UeLS-CH                    | UeLS-CH                    | Übergeordnetes Leitsystem Schweiz (ehemaliger BL)  |
| UHB                        | UHB                        | Unterhalt und Betrieb  |
| ÜV-LW                      |                            | Überholverbot Lastwagen  |
| VBV                        | VBV                        | Vehicle-By-Vehicle   |
| VDV                        | VDV                        | Verkehrsdatenverbund bezeichnet das Kommunikationsnetzwerk zum Transport der Verkehrsmanagementdaten   |
| VIS                        | VIS                        | Verkehrsinformationssystem   |
| VL                         | VL                         | Verkehrslenkung  |
| VL-CH                      | VL-CH                      | Verkehrslenkung Schweiz  |
| Videosystem                | Système vidéo              | System zur Bearbeitung der Videoinformationen  |
| Videodienst                | Service vidéo              | Dienst zur Bearbeitung der Videoinformationen  |
| VM                         | VM                         | Virtuelle Maschinen  |
| VM AP                      | VM AP                      | Virtuelle Maschinen Applikation  |
| VMS.AS                     | VMS.AS                     | Im VMS.AS werden alle vom AR gesendeten Befehle, einschliesslich Funktionen und Steuerungen, ausgeführt.   |
| VMS.ED                     | VMS.ED                     | Modul zur serverbasierte Bildanalyse und Ereignisermittlung für Videoanlage  |
| VMS.MGT GE                 | VMS.MGT GE                 | Zentrale VMS-Komponente – speichert die Konfiguration des Überwachungssystems, sowie veraltet die Benutzerauthentifizierung, die Benutzerberechtigungen, Regeln etc.               |
| VMS.OPA/ DEC               | VMS.OPA/ DEC               | Sind Clients für den Nutzer des VMS  |
| VMS.REC                    | VMS.REC                    | Der Recording-Server verwaltet Kommunikation, Aufzeichnungen und Zustandsmeldungen der angeschlossenen Geräte (Kameras, Video- und Audio Encoder, I/O-Module und Metadatenquellen) |
| VMS.MGT RZ/ARC/OPA         | VMS.MGT RZ/ARC/OPA         | Teil des Videosystems VIDEO-CH für die Archivierung von ereignisbezogenen Bildsequenzen  |
| VMS.MOS/MGT BD/AN/TCA/TCN/ | VMS.MOS/MGT BD/AN/TCA/TCN/ | Teil des Videosystems VIDEO-CH für die Archivierung von ereignisbezogenen Bildsequenzen  |

| Begriff/Abkürzung | Terme/abréviation | Bedeutung   |
|-------------------|-------------------|---|
| VMS-M/TNN/TDSG    | VMS-M/TNN/TDSG    | Teil des Videosystems VIDEO-CH für die Archivierung von ereignisbezogenen Bildsequenzen |
| VMZ-CH            | VMZ-CH            | Verkehrsmanagementzentrale Schweiz  |
| VR                | VR                | Verkehrsrechner sowohl RM VM als auch Zwischenlösung IVM                                |
| VSAN              | VSAN              | virtuelle Storage Area Network  |
| WTA               | WTA               | Wechseltextanzeige  |
| WWW               | WWW               | Wechselwegweisung   |
| ZSC               | ZSC               | Zählstellencontroller   |



# Literaturverzeichnis

## Weisungen, Richtlinien und Dokumentationen des ASTRA

- [1] Bundesamt für Strassen ASTRA, „**Steuerung der Betriebs- und Sicherheitsausrüstungen: Rollen, Aufgaben und Anforderungen für Benutzeroberflächen**“, Weisung ASTRA 73002, [www.astra.admin.ch](http://www.astra.admin.ch).
- [2] Bundesamt für Strassen ASTRA, „**OT-Security Governance**“, Weisung ASTRA 73006, [www.astra.admin.ch](http://www.astra.admin.ch).
- [3] Bundesamt für Strassen ASTRA, „**Videoanlagen**“, Richtlinie ASTRA 13005, [www.astra.admin.ch](http://www.astra.admin.ch).
- [4] Bundesamt für Strassen ASTRA, „**Technische Zentralen BSA**“, Richtlinie ASTRA 13009, [www.astra.admin.ch](http://www.astra.admin.ch).
- [5] Bundesamt für Strassen ASTRA, „**Kontrollen und Tests der BSA**“, Richtlinie ASTRA 13028, [www.astra.admin.ch](http://www.astra.admin.ch).
- [6] Bundesamt für Strassen ASTRA, „**OT Security**“, Richtlinie ASTRA 13030, [www.astra.admin.ch](http://www.astra.admin.ch).
- [7] Bundesamt für Strassen ASTRA, „**Engineering der BSA-Daten**“, Richtlinie ASTRA 13032, [www.astra.admin.ch](http://www.astra.admin.ch).
- [8] Bundesamt für Strassen ASTRA, „**OPC-UA Definition**“, Richtlinie ASTRA 13034, [www.astra.admin.ch](http://www.astra.admin.ch).
- [9] Bundesamt für Strassen ASTRA, „**IP-Netz BSA**“, Richtlinie ASTRA 13040, [www.astra.admin.ch](http://www.astra.admin.ch).
- [10] Bundesamt für Strassen ASTRA, „**Verkehrsmanagement auf Nationalstrassen (Kopfrichtlinie VM-NS)**“, Richtlinie 15003, [www.astra.admin.ch](http://www.astra.admin.ch).
- [11] Bundesamt für Strassen ASTRA, „**Verkehrstechnische Regelungslogik - Funktionale Minimalanforderungen für Planung und Betrieb der Regelung von Verkehrsmanagement-Systemen zur Verflüssigung des Verkehrs**“, Richtlinie ASTRA 15019, [www.astra.admin.ch](http://www.astra.admin.ch).
- [12] Bundesamt für Strassen ASTRA, „**Network Security Policy IP-Netz BSA (NSP IP-Netz BSA)**“, Dokumentation ASTRA 83042, [www.astra.admin.ch](http://www.astra.admin.ch).
- [13] Bundesamt für Strassen ASTRA, „**Zeit- und Taktverteilung IP-Netz BSA**“, Dokumentation ASTRA 83044, [www.astra.admin.ch](http://www.astra.admin.ch).
- [14] Bundesamt für Strassen ASTRA, „**Style Guide BSA – Teil 0: Allgemeine Grundlagen**“, Dokumentation ASTRA 83050, [www.astra.admin.ch](http://www.astra.admin.ch).
- [15] Bundesamt für Strassen ASTRA, „**Style Guide BSA - Teil 2: Ebene Streckensysteme**“, Dokumentation ASTRA 83052, [www.astra.admin.ch](http://www.astra.admin.ch).
- [16] Bundesamt für Strassen ASTRA, „**Style Guide BSA - Teil 3: Symbolbibliothek**“, Dokumentation ASTRA 83053, [www.astra.admin.ch](http://www.astra.admin.ch).
- [17] Bundesamt für Strassen ASTRA, „**Übergeordnetes Leitsystem (UeLS-CH) - Grundanforderungen**“, Dokumentation ASTRA 83054, [www.astra.admin.ch](http://www.astra.admin.ch).
- [18] Bundesamt für Strassen ASTRA, „**Übergeordnetes Leitsystem (UeLS-CH) - Leitfaden zu ASTRA 83054 für Planung, Aus-schreibung, Realisierung und BSA-Integration**“, Dokumentation ASTRA 83055, [www.astra.admin.ch](http://www.astra.admin.ch).
- [19] Bundesamt für Strassen ASTRA, „**IAM BSA**“, Dokumentation ASTRA 83056, [www.astra.admin.ch](http://www.astra.admin.ch).
- [20] Bundesamt für Strassen ASTRA, „**Minimale Anforderungen an den Betrieb- Strecke und Tunnel**“, Dokumentation ASTRA 86053, [www.astra.admin.ch](http://www.astra.admin.ch).
- [21] Bundesamt für Strassen ASTRA, „**Notruftelefon**“, Technisches Merkblatt ASTRA 23001-11650, [www.astra.admin.ch](http://www.astra.admin.ch).





## Auflistung der Änderungen

| Ausgabe | Version | Datum      | Änderungen  |
|---------|---------|------------|---|
| 2025    | 2.10    | 16.12.2025 | <ul style="list-style-type: none"> <li>• Vertiefung der Verkehrsmanagementanlagen.</li> <li>• Diverse formelle Anpassungen, kleine Textkorrekturen.</li> <li>• Literaturverzeichnis bereinigt.</li> </ul>   |
| 2024    | 2.00    | 28.01.2025 | <ul style="list-style-type: none"> <li>• Inkrafttreten Ausgabe 2025 V2.00, komplette neue Fassung.</li> </ul>   |
| 2016    | 1.70    | 01.11.2017 | <ul style="list-style-type: none"> <li>• Publikation der französischen Version.</li> <li>• Bereinigung zusammen mit der Übersetzung ins F.</li> </ul>   |
| 2016    | 1.60    | 01.01.2016 | <ul style="list-style-type: none"> <li>• Inkrafttreten Ausgabe 2016.</li> <li>• Gesamtes Dokument: Infrastrukturnetz BSA (ISN) durch BSA-Kommunikationsnetz ersetzt.</li> <li>• Gesamtes Dokument: Die Anforderungsnummerierung (Rx) entfernt.</li> <li>• Kapitel 2.5 Migration eingefügt.</li> <li>• Legende zu Abbildung 2.3 eingefügt.</li> <li>• Abbildungen 3.1 und 5.1 vereinfacht.</li> <li>• Kapitel 7 bereinigt.</li> <li>• Literaturverzeichnis bereinigt.</li> <li>• Diverse formelle Anpassungen, Textkorrekturen.</li> </ul> |
| 2015    | 1.50    | 01.10.2015 | <ul style="list-style-type: none"> <li>• Datenpunkt Fachkatalog Anhang II entfernt</li> </ul>   |
| 2015    | 1.40    | 01.06.2015 | <ul style="list-style-type: none"> <li>• Datenpunkt Fachkatalog Anhang II eingefügt</li> <li>• Diverse Korrekturen vorgenommen</li> </ul>   |
| 2015    | 1.10    | 01.01.2015 | <ul style="list-style-type: none"> <li>• Inkrafttreten Ausgabe 2015</li> </ul>  |

