Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral des routes OFROU

DIRECTIVE

ARCHITECTURE DES SYSTÈMES DE GESTION ET DE COMMANDE DES ÉQUIPEMENTS D'EXPLOITATION ET DE SÉCURITÉ

Édition 2026 V2.11
ASTRA 13031

Impressum

Auteurs
Geringer Jolanda OFROU DS-DTI
Crausaz Bernard OFROU DS-UARS
Gähwiler Daniel CSI Consulting AG, Zurich
Indergand Stefan GEXI

Groupe d'accompagnement
Pfammatter Mario OFROU DS-UARS
Claude Stéphane OFROU DS-DTI
Paolo Maltese OFROU N-VIM
Demont Olivier OFROU I-FU
Kundert Renato OFROU I-FU
Berger Markus OFROU I-FU
Wyss Martin OFROU I-B
Bregy Valentin OFROU I-F2

Langue du texte original
Allemand

Éditeur
Office fédéral des routes OFROU
Division Réseaux routiers N
Standards et sécurité de l'infrastructure SSI
3003 Berne

Diffusion
Le document est téléchargeable gratuitement sur le site www.ofrou.admin.ch.

© ASTRA 2026
Reproduction à usage non commercial autorisée avec indication de la source.

Avant-propos

Les équipements d'exploitation et de sécurité (EES) sont essentiels à la sécurité des tunnels et des sections à ciel ouvert du réseau des routes nationales suisses. Les EES et leurs systèmes OT (Operational Technology) garantissent une exploitation sécurisée et une surveillance sans interruption.

Les EES interviennent également dans la gestion du trafic, en contribuant à garantir un trafic aussi régulier et fluide que possible.

La présente directive définit une structure uniforme des systèmes de gestion des EES à l'échelle de la Suisse. Elle constitue une base solide et modulaire qui permet à l'OFROU de poursuivre le développement des EES, mais aussi de déployer de nouvelles solutions, notamment en matière de gestion du trafic ou de mise en réseau des véhicules avec l'infrastructure.

Office fédéral des routes

Jürg Röthlisberger
Directeur

Table des matières

Impressum **2**
Avant-propos **3**
Liste des figures **9**
Liste des tableaux **11**

1 Introduction **12**
1.1 But de la directive 12
1.2 Domaine d'application 12
1.3 Destinataires 12
1.4 Entrée en vigueur et modifications 12

2 Principes relatifs à l'architecture **13**
2.1 Vision des systèmes de gestion et de commande 13
2.2 Environnement de production, d'intégration, de test et de formation 13
2.3 Structure de base de l'architecture système 15
2.3.1 Réseau IP EES (réseau de communication) 15
2.3.2 Niveau gestion 16
2.3.3 Services de base / services centraux 16
2.3.4 Niveau national de gestion du trafic 16
2.3.5 Région de gestion du trafic 16
2.3.6 Niveau de gestion régional 17
2.3.7 Section EES / Section IP 17
2.3.8 Systèmes de la Confédération, systèmes tiers et installations spéciales 20
2.4 Périmètre d'influence 21

3 Architecture SA-CH **22**
3.1 Niveau gestion 22
3.1.1 Niveau applications 22
3.1.2 Niveau services métier 23
3.1.3 EES Datawarehouse (DWH) 24
3.2 Niveau services de base / services centraux 24
3.2.1 Gestion OT 25
3.2.2 Services OT 27
3.3 Niveau de gestion du trafic suisse 28
3.4 Régions de gestion du trafic 29
3.4.1 Gestion de réseau par tronçon ou à l'échelle nationale 30
3.4.2 Exemple d'une gestion de trafic par tronçon 30
3.4.3 Éléments d'architecture spécifiques à la gestion du trafic basés sur les tronçons 32
3.5 Niveau de gestion régional UT 33
3.5.1 Système d'information routière (VIS) 33
3.5.2 Acquisition régionale des données de trafic (rVDE) 33
3.5.3 UeLS-CH 33
3.5.4 Installation de surveillance et d'alarmes météo (GFS) 33
3.5.5 Système vidéo 33
3.5.6 Postes de travail des opérateurs 34
3.5.7 Outils techniques d'exploitation 34
3.5.8 Téléphone de secours (NT) 34
3.5.9 Autres systèmes 34
3.5.10 Services de sous-domaines / IAM EES 34
3.5.11 DD(I) 34
3.5.12 Accès à distance (systèmes de secours OT) 34
3.6 Section EES 34
3.6.1 Serveur de gestion section (AR) 34
3.6.2 Commande d'installation et commande locale 35
3.6.3 Capteurs et actionneurs 36
3.7 Systèmes de la Confédération 36

3.8 Systèmes tiers ... 36
3.9 Installations spéciales ... 36

4 Exigences de performance ... 37
4.1 Utilisation de la virtualisation ... 37
4.1.1 Local technique OT ... 37
4.1.2 Locaux techniques/centrales techniques ... 37
4.2 Systèmes d'exploitation et redondances ... 38
4.2.1 Systèmes d'exploitation et plateforme de virtualisation ... 38
4.2.2 AR redondants ... 38
4.2.3 AS en version redondante ... 39
4.3 Application de virtualisation ... 39
4.3.1 Autonomie et niveaux de repli ... 39
4.3.2 Virtualisation des systèmes de gestion et de commande ... 40
4.3.3 Schéma de la virtualisation de l'AR (objectif) ... 40
4.3.4 UeLS-CH (BL) dans le local technique OT ... 42
4.4 Structure de l'AR (exemple d'un serveur unique) ... 43
4.4.1 Compatibilité des navigateurs web pour les GUI-MMI ... 44
4.5 Structure de l'AS ... 44
4.5.1 AS critiques pour la sécurité (y c. LS) ... 44
4.5.2 Exigences relatives aux AS (API) ... 44
4.5.3 API ... 45
4.5.4 API virtuels ... 46
4.5.5 IPC ... 46
4.5.6 MMI (GUI) ... 46
4.6 Structure de la LS ... 46
4.6.1 Exigences relatives aux LS ... 46
4.7 Licences ... 46
4.7.1 Licences sans lien avec le matériel ... 46
4.8 Disponibilité des éléments ... 46
4.8.1 Heures de service ... 46
4.8.2 Heures d'assistance ... 47
4.8.3 Disponibilité ... 47
4.9 Application des technologies spécifiques aux installations ... 49
4.9.1 Utilisation des fonctions de disponibilité dans le local technique OT ... 50
4.9.2 Utilisation des fonctions de disponibilité AR ... 51
4.9.3 Utilisation des fonctions de disponibilité AS/LS ... 51
4.10 Consolidation des différentes fonctions de l'installation sur la plateforme de virtualisation ... 51
4.10.1 Local technique OT (deux sites par UT dans une ou deux sections IP dédiées) ... 52
4.10.2 Locaux techniques (deux sites à l'intérieur de la section IP) ... 52
4.10.3 Exigences relatives à la garantie de maintenance et d'assistance (SLA) ... 53
4.11 Conservation des données ... 53
4.11.1 Droit de propriété et d'utilisation ... 54
4.11.2 Logiciels et programmes d'application ... 54
4.12 Traçabilité ... 54
4.12.1 Journalisation ... 54
4.12.2 Journalisation du système ... 54
4.12.3 Hiérarchie et agrégation des données ... 54
4.12.4 Archivage ... 55
4.12.5 Sauvegarde et restauration ... 55
4.13 Synchronisation horaire ... 56
4.14 Reporting ... 56
4.15 OT Security ... 56
4.15.1 Instructions 73006 ... 56
4.15.2 Directive 13030 ... 56
4.15.3 Documentation 83042 ... 57
4.15.4 Documentation 83056 ... 57
4.15.5 Manuel technique 23001-11880 Sécurité physique des systèmes OT et directive 13009 57

5 Exigences fonctionnelles 58
5.1 Accès 58
5.1.1 Groupes d'utilisateurs 58
5.1.2 Rôles des utilisateurs 58
5.2 Interfaces utilisateurs 58
5.2.1 Principe de visualisation 58
5.2.2 Possibilités de commande 60
5.2.3 Interfaces utilisateur 61
5.3 Commande 61
5.3.1 Modes d'exploitation 61
5.3.2 Modes de commande 63
5.3.3 Fonctions 64
5.4 Monitoring 64
5.5 Reporting 65
5.6 Niveau de repli 65
5.7 Liens WEB utiles pour l'exploitation 67
5.8 Autonomie 67
5.8.1 Fonction de l'installation selon le scénario d'exploitation 67
5.8.2 Scénarios d'exploitation relatifs à l'autonomie de la section 68
5.8.3 Exploitation normale 68
5.8.4 Exploitation limitée 68
5.8.5 Exploitation d'urgence 68
5.8.6 Pas d'exploitation 69
5.8.7 Vue d'ensemble des scénarios d'exploitation 69
5.8.8 Champ d'application 70
5.9 Réseau IP EES 70
5.10 Principes de communication 70
5.10.1 Principes et exigences 70
5.10.2 Protocoles 71
5.11 Modèle de données et points de données 71
5.12 Échange de données 71
5.12.1 UeLS-CH 71
5.12.2 Serveur de gestion section 72
5.12.3 Commande d'installation / commande locale 72
5.13 Interdomaines 73
5.13.1 Modes de transmission des interdomaines 73
5.13.2 Types d'interdomaines 73
5.13.3 Architecture cible 74
5.14 Portails d'accès OT/EES et accès à distance (systèmes de secours OT) 75
5.15 Connexion des systèmes périphériques 75
5.16 Communication mobile 75

6 Migration 76
6.1 Adaptations organisationnelles de la structure et de la structure d'exploitation de l'OT/EES 76
6.2 Informations générales sur le concept de migration 76
6.3 Communication et système de gestion 76
6.3.1 Système de gestion (UeLS-CH intégration du système) 77
6.4 Systèmes de gestion du trafic 78
6.4.1 Système Vehicle-by-Vehicle (VBV) 78
6.4.2 Système d'information sur le trafic (VIS) 78
6.4.3 Gestion régionale du trafic (rVL) 78
6.4.4 Acquisition régionale des données de trafic (rVDE) 78
6.4.5 Calculateur de trafic régional (VR) 78

Annexes 79

Glossaire 99

Bibliographie 105
Liste des modifications 107

Liste des figures

Figure 1 : Structure de base de l'architecture 15
Figure 2 : Vue d'ensemble du réseau IP EES, comprenant les deux sites des services de base A et B et les deux sites à remplacer, RZ EES A et B (ABX) 16
Figure 3 : Étendue spatiale des éléments d'architecture (représentation logique) 17
Figure 4 : Étendue spatiale des éléments spécifiques de l'architecture de gestion du trafic (représentation logique) 19
Figure 5 : Vue d'ensemble des systèmes de la Confédération et des systèmes tiers 20
Figure 6 : Niveau applications 22
Figure 7 : Niveau services métier 23
Figure 8 : Gestion OT 25
Figure 9 : Services OT 27
Figure 10 : Niveau de gestion du trafic suisse 28
Figure 11 : Périmètre d'influence de l'AM VL-CH 30
Figure 12 : Gestion du trafic par tronçon 30
Figure 13 : Exemple d'« installations dédiées » et d'« installations combinées » 32
Figure 14 : Exemple de HV-AD avec « installations dédiées » et « installations combinées » 32
Figure 15 : Niveau de gestion régional des unités territoriales 33
Figure 16 : Local technique OT 37
Figure 17 : Local technique/centrale technique 38
Figure 18 : Schéma de l'objectif de la virtualisation de l'AR - AR, AR MMI et AS MMI sur des VM distinctes 40
Figure 19 : Schéma de l'objectif de la virtualisation de l'AR - AR et AR MMI sur une VM commune 41
Figure 20 : Variante 1 - schéma de l'AR non virtualisé (dans des cas exceptionnels) 41
Figure 21 : Variante 2 - les éléments d'accès sont spécifiques au fabricant et liés à leur fonction 42
Figure 22 : Structure de base d'un AR Host : séparation des fonctions des VM - variante 1 43
Figure 23 : Structure de base d'un AR Host : séparation des fonctions des VM - variante 2 44
Figure 24 : Schéma de l'application de la technologie (un tube) 52
Figure 25 : Pyramide des données 55
Figure 26 : Principe des exigences et mesures de sécurité à plusieurs couches – Principe de défense en profondeur « Defense in Depth » 57
Figure 27 : Principes de visualisation 59
Figure 28 : Niveaux de repli SA-CH 66
Figure 29 : Échange de données avec l'UeLS-CH 72
Figure 30 : Échange de données AR 72
Figure 31 : Échange de données AS/LS 73
Figure 32 : Interdomaine de type 1 74
Figure 33 : Interdomaine de type 2 75
Figure 34 : Variantes de mise en œuvre du système de gestion (UeLS-CH et architecture du système), où nouveau = conforme SA-CH et existant = non conforme SA-CH 77

Liste des tableaux

Tableau 1 : Étendue spéciale de la gestion du trafic 18
Tableau 2 : Périmètres d'influence du point de vue des utilisateurs 21
Tableau 3 : Périmètre d'influence - perspective systémique 21
Tableau 4 : Utilisation de la virtualisation dans les niveaux système de l'architecture 40
Tableau 5 : Niveau de service heures de service 47
Tableau 6 : Heures d'assistance selon le niveau de service 47
Tableau 7 : Niveau de service mesuré en downtime 48
Tableau 8 : Disponibilité standard mesurée en downtime 48
Tableau 9 : Parties d'installation et leurs fonctions partielles 50
Tableau 10 : Vue d'ensemble de la virtualisation de l'installation partielle 50
Tableau 11 : Cycle de vie des « données non personnelles » 53
Tableau 12 : Principes de visualisation 59
Tableau 13 : Possibilités de commande 60
Tableau 14 : Modes d'exploitation 61
Tableau 15 : Modes d'exploitation spécifiques à chaque niveau 62
Tableau 16 : Installations EES et installations de gestion du trafic 62
Tableau 17 : Types de commande 63
Tableau 18 : Parties d'installation nécessaires à une exploitation minimale sécurisée 67
Tableau 19 : Vue d'ensemble des scénarios d'exploitation 69
Tableau 20 : Vue d'ensemble de l'applicabilité selon la catégorie de tunnel 70

1 Introduction

1.1 But de la directive

La présente directive harmonise la structure des systèmes de gestion des équipements d'exploitation et de sécurité (EES) ainsi que leurs systèmes OT sur les routes nationales. Elle définit les prescriptions relatives à leur planification, leur conception et leur réalisation.

Elle décrit également les caractéristiques des systèmes de gestion et de commande ainsi que des interfaces.

La directive porte principalement sur les fonctions, et non sur le matériel. Les interdictions sont explicitement énoncées. Le cadre dans lequel il est possible d'évoluer est pour le reste décrit.

1.2 Domaine d'application

La directive s'applique de manière contraignante à la planification, la conception, la réalisation et l'exploitation des systèmes de gestion et de commande de tous les équipements d'exploitation et de sécurité (EES) ainsi que de leurs systèmes OT sur les routes nationales.

1.3 Destinataires

Cette directive s'adresse à toutes les personnes internes et externes amenées à travailler sur les systèmes OT et les EES, que ce soit dans le cadre de la conception ou de l'exploitation.

Elle est plus particulièrement destinée aux personnes suivantes :

- Chefs de projet de l'OFROU (pour les projets en lien avec les systèmes de gestion et de commande) ;
- Planificateurs et entreprises opérant sur l'OT (Operational Technology) / les EES sur mandat de l'OFROU ;
- Spécialistes et responsables de la gestion du patrimoine EES de l'OFROU ;
- Chefs de projet SA-CH de l'OFROU ;
- Spécialistes OT/EES des unités territoriales ;
- Toutes les autres parties prenantes de l'organisation, notamment l'exploitation de l'OT/EES.

1.4 Entrée en vigueur et modifications

La présente directive entre en vigueur le 28.01.2025. La « Liste des modifications » est disponible à la page 107.

2 Principes relatifs à l'architecture

L'architecture système Suisse décrit les systèmes de gestion et de commande des routes nationales. Elle constitue un modèle illustrant les relations et les propriétés des différents éléments et de leurs fonctions. Les systèmes relevant directement de la Confédération, les systèmes tiers ainsi que les installations spéciales sont également présentés.

Ce chapitre aborde les objectifs de l'architecture système Suisse (SA-CH) ainsi que les exigences générales qui s'y rapportent. Une vue d'ensemble de l'architecture système est par ailleurs proposée. Les niveaux sont présentés en détail au chapitre 3.

2.1 Vision des systèmes de gestion et de commande

L'architecture système vise l'état cible suivant :

- Une architecture homogène, modulaire et extensible ;
- L'autonomie des régions, objets et installations ;
- La normalisation des exigences et interfaces entre les systèmes ;
- Une indépendance vis-à-vis des fabricants ;
- La capacité de l'infrastructure à intégrer de nouvelles technologies ;
- Une efficacité renforcée des prestations.

Les conditions-cadres suivantes doivent être respectées :

- La connectivité à l'échelle nationale est garantie par un réseau technique homogène (réseau IP EES) ;
- Les systèmes de gestion et de commande des EES sont conçus de manière homogène à l'échelle nationale : leur structure, et plus particulièrement leurs interfaces, répond à des prescriptions uniformes ;
- Les systèmes périphériques de tiers (ne relevant pas du champ d'application de l'architecture système) sont reliés par des interfaces standardisées ;
- L'architecture système permet l'intégration de systèmes supplémentaires et l'utilisation de nouvelles technologies ;
- Les services sont fournis de manière centralisée, ou des prescriptions fonctionnelles claires sont définies pour la mise à disposition des services décentralisés ;
- La communication entre les niveaux est assurée conformément aux exigences de l'OT Security et de la Network Security Policy ;
- Les objectifs métier des directives 15003 et 15007 s'appliquent pour les installations de gestion du trafic et le monitorage du trafic.

2.2 Environnement de production, d'intégration, de test et de formation

En cas de besoin, il convient de mettre en place un environnement de production, d'intégration, de test et de formation pour le niveau de gestion régional, les services de base ainsi que pour le niveau de gestion. Cette décision est prise dans le cadre du projet concerné et consignée dans les documents du projet (Hermes : PA, SIA : PI / Pdét).

L'environnement de formation peut être mis à disposition sous forme de simulation. Toutes les fonctionnalités des applications métier doivent être disponibles dans cet environnement. Leur utilisation ne doit pas avoir d'impact sur les installations.

Pour les systèmes uniformes à l'échelle nationale, un environnement de test et un environnement de formation sont suffisants (y compris en cas d'installation sur des sites distincts).

Pour le niveau installation et commande des EES, des tests d'intégration doivent être réalisés dans l'environnement d'intégration et dans l'environnement de production. Conformément à la directive 13028, il s'agit de tests des installations avec toutes les interfaces concernées.

Pour chaque projet, l'entrepreneur (UN) ou l'auteur du projet (PV) doit élaborer les protocoles de test de manière à pouvoir, après la mise en œuvre, tester et vérifier intégralement, en interaction avec les systèmes concernés, les fonctions commandées par le maître d'ouvrage (les exigences de ce dernier doivent être prises en compte).

Le test dans l'environnement d'intégration consiste généralement en :

- un test à l'usine de l'entrepreneur EES (test d'usine intégré, IWT / Factory Integration Test, FIT) au cours de la première phase ;
- un test sur site dans l'environnement réel avec tous les environnements systèmes pertinents au cours de la deuxième phase.

Ce test intervient après la validation du FAT (voir directive 13028).

Le test dans l'environnement de production correspond à un test dans le système réel (test en temps réel, TTR / Site Integration Test, SIT). Ce test est réalisé après la validation du SAT (voir directive 13028).

2.3 Structure de base de l'architecture système

L'Architecture de système Suisse (SA-CH) est structurée en plusieurs niveaux et techniquement conçue de manière à garantir un fonctionnement continu 24 heures sur 24 et 7 jours sur 7. La Figure 1 ci-dessous présente la structure de base de l'architecture (voir annexe IV.1) :

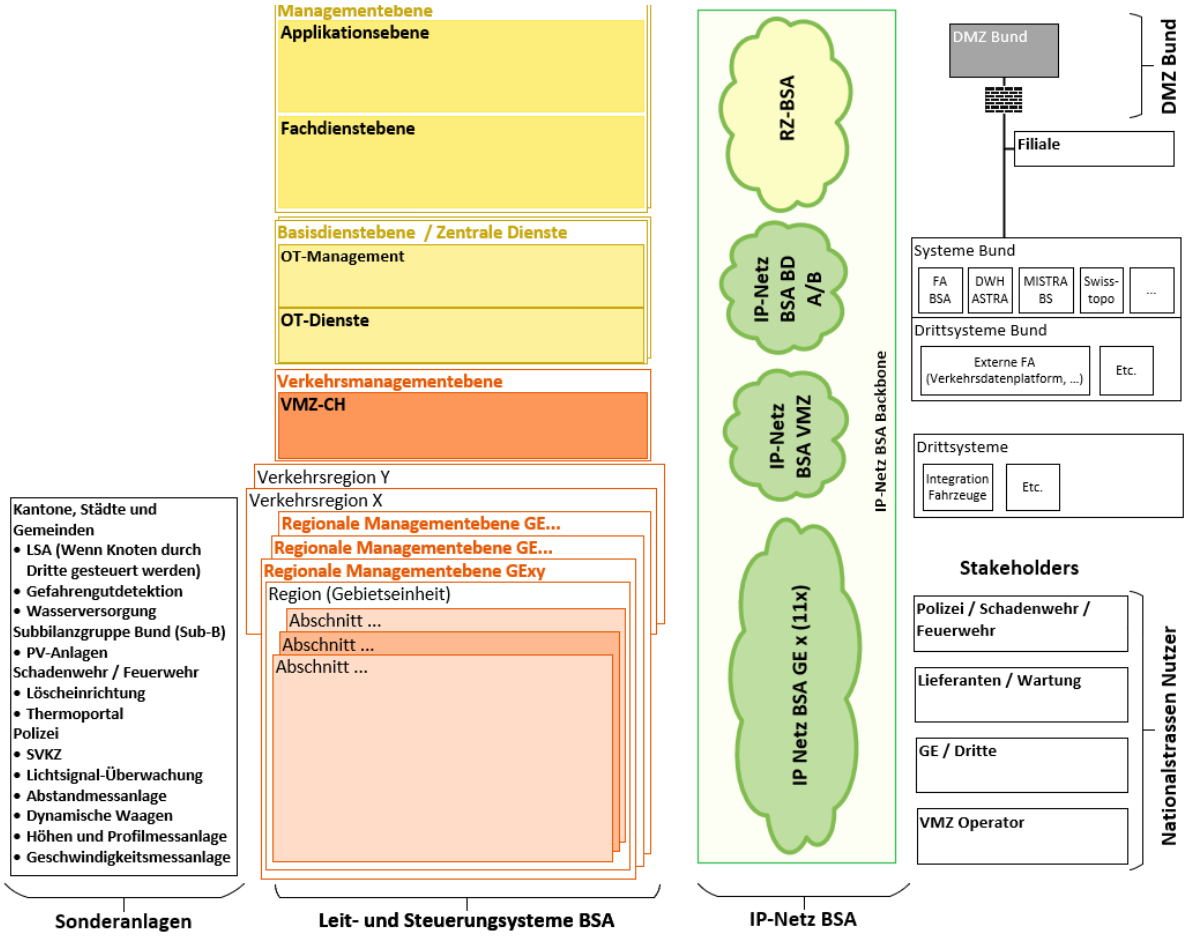


Figure 1 : Structure de base de l'architecture

2.3.1 Réseau IP EES (réseau de communication)

Au cours des prochaines années, l'infrastructure de communication des équipements d'exploitation et de sécurité (EES) des routes nationales sera progressivement mise en conformité avec la directive ASTRA 13040 « Réseau IP EES ». Le réseau IP EES vise à standardiser l'architecture du réseau, les exigences relatives aux équipements réseau ainsi que les services du réseau IP EES, et à les inscrire dans une base moderne et pérenne. Les actuels réseaux IPv4 (ancienne technologie) sont remplacés par des réseaux IPv6 (nouvelle technologie), et les actuels raccordements VDV ont été migrés vers le réseau IP EES Backbone (dorsale de la Confédération).

Ces nouveautés requièrent des services de base et des outils centraux garantissant l'exploitation sûre (sécurité IT/OT et disponibilité) et efficace du réseau IP EES. La gestion de l'exploitation du réseau IP EES UT reste sous la responsabilité des unités territoriales, tandis que celle réseau IP EES Backbone incombe à l'OFIT/cmdt Cyber.

L'exploitation des nouveaux services de base et outils centraux implique de nouvelles tâches, qui sont décrites ci-après.

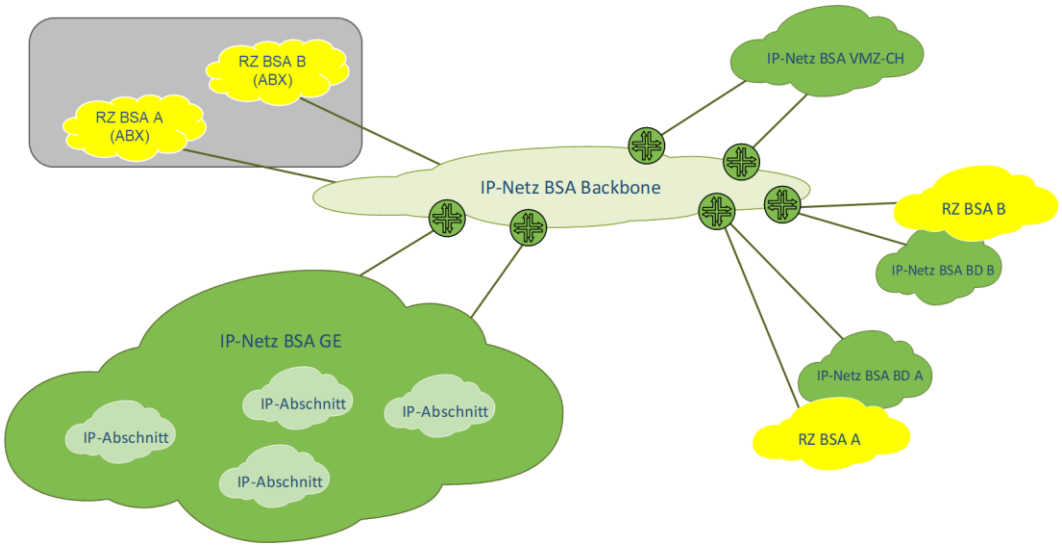


Figure 2 : Vue d'ensemble du réseau IP EES, comprenant les deux sites des services de base A et B et les deux sites à remplacer, RZ EES A et B (ABX)

2.3.2 Niveau gestion

Le niveau gestion regroupe les services métier supérieurs et les applications métier destinés à l'exploitation opérationnelle de niveau supérieur. On distingue le niveau des services métier et le niveau applications.

2.3.2.1 Niveau applications

Ce niveau est principalement utilisé pour les applications métier de la gestion du trafic et pour la mise à disposition d'informations destinées à être transmises aux systèmes périphériques de la Confédération.

2.3.2.2 Niveau services métier

Les données et informations destinées au niveau applications sont traitées et préparées à ce niveau. Des informations destinées aux analyses y sont également mises à disposition.

2.3.3 Services de base / services centraux

Les services de base font partie intégrante du réseau IP EES et sont nécessaires à son exploitation efficace, efficiente et sécurisée. Les services sont nécessaires dans tous les réseaux partiels : réseau IP EES UT, réseau IP EES RZ, réseau IP EES Backbone et réseau IP EES VMZ-CH. Le sous-niveau « Gestion OT » regroupe les systèmes nécessaires à la gestion technique, tandis que le sous-niveau « Services OT » fournit les services requis pour la gestion technique.

2.3.4 Niveau national de gestion du trafic

La centrale suisse de gestion du trafic (VMZ-CH) utilise le niveau de gestion du trafic pour diffuser des messages, par exemple sur les panneaux à messages variables (WTA), et pour commander la signalisation, notamment lors de la réaffectation de la bande d'arrêt d'urgence (R-BAU) aux heures de pointe.

2.3.5 Région de gestion du trafic

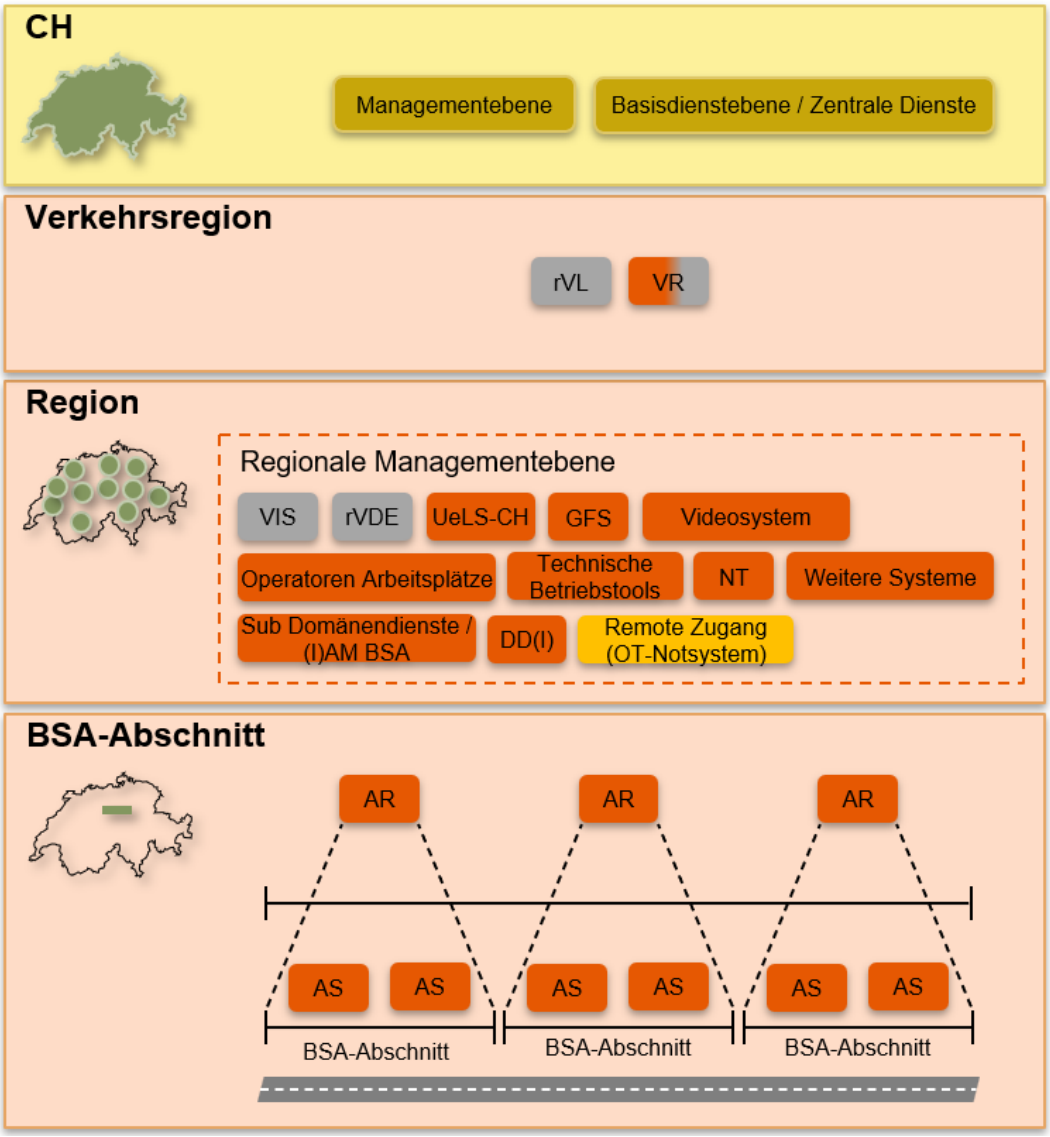
La région de gestion du trafic couvre un périmètre défini qui dépasse les limites des unités territoriales et des filiales. Elle regroupe l'ensemble des mesures de gestion du trafic. La région de gestion du trafic est définie selon une logique de trafic et englobe tous les secteurs fonctionnellement liés, même s'ils relèvent d'organisations de projet et d'exploitation différentes.

2.3.6 Niveau de gestion régional

Les unités territoriales sont responsables de leur périmètre d'influence respectif à partir du niveau de gestion régional. Les unités territoriales assurent l'exploitation et l'entretien des équipements d'exploitation et de sécurité ainsi que des systèmes OT dans leur périmètre. Elles veillent à la disponibilité de ces systèmes et, le cas échéant, à la mise en place des redondances.

2.3.7 Section EES / Section IP

Le périmètre d'influence que représente la section EES fait partie de la route nationale. D'un point de vue fonctionnel, il constitue une unité autonome pour les équipements d'exploitation et de sécurité. Un serveur de gestion section (AR) assure la surveillance et le pilotage de niveau supérieur des installations de la section EES, ainsi que la connexion au système de gestion générale suisse (UeLS-CH) de l'unité territoriale correspondante. Du point de vue du réseau, on parle de section IP, laquelle correspond à 95 % à la section EES. Dans certains cas, la section IP est plus étendue que la section EES.



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

Figure 3 : Étendue spatiale des éléments d'architecture (représentation logique)

2.3.7.1 Étendue spatiale de la gestion et du monitorage spécifiques du trafic (éléments d'architecture)

L'architecture est conçue différemment pour la gestion et le monitorage du trafic : sur les tronçons à ciel ouvert, aucun AR spécifique n'est prévu et l'AS n'est utilisée que de manière limitée. Cette architecture logique est décrite ci-après :

L'étendue spatiale de l'architecture de gestion du trafic spécifique est définie comme suit :

Tableau 1 : Étendue spéciale de la gestion du trafic

Étendue spatiale	Champ d'action
CH	Commande opérationnelle de toutes les installations de gestion du trafic
Région de gestion du trafic	Les dispositifs temporaires de gestion du trafic à portée régionale ou les calculateurs de trafic seront remplacés par la FA VL-CH.
Région	Les commandes temporaires à portée régionale des WTA/WWW ainsi que la saisie des données de trafic pour la gestion du trafic seront remplacées par la FA VL-CH.
Section IP	La gestion du trafic fonctionne sur la base des sections IP. Les installations de gestion du trafic (composantes de l'EES) sont généralement situées sur le tronçon à ciel ouvert. Les autres EES servant à la gestion du trafic sont également utilisés dans le tunnel.

Les éléments sont présentés en détail au chapitre 3.

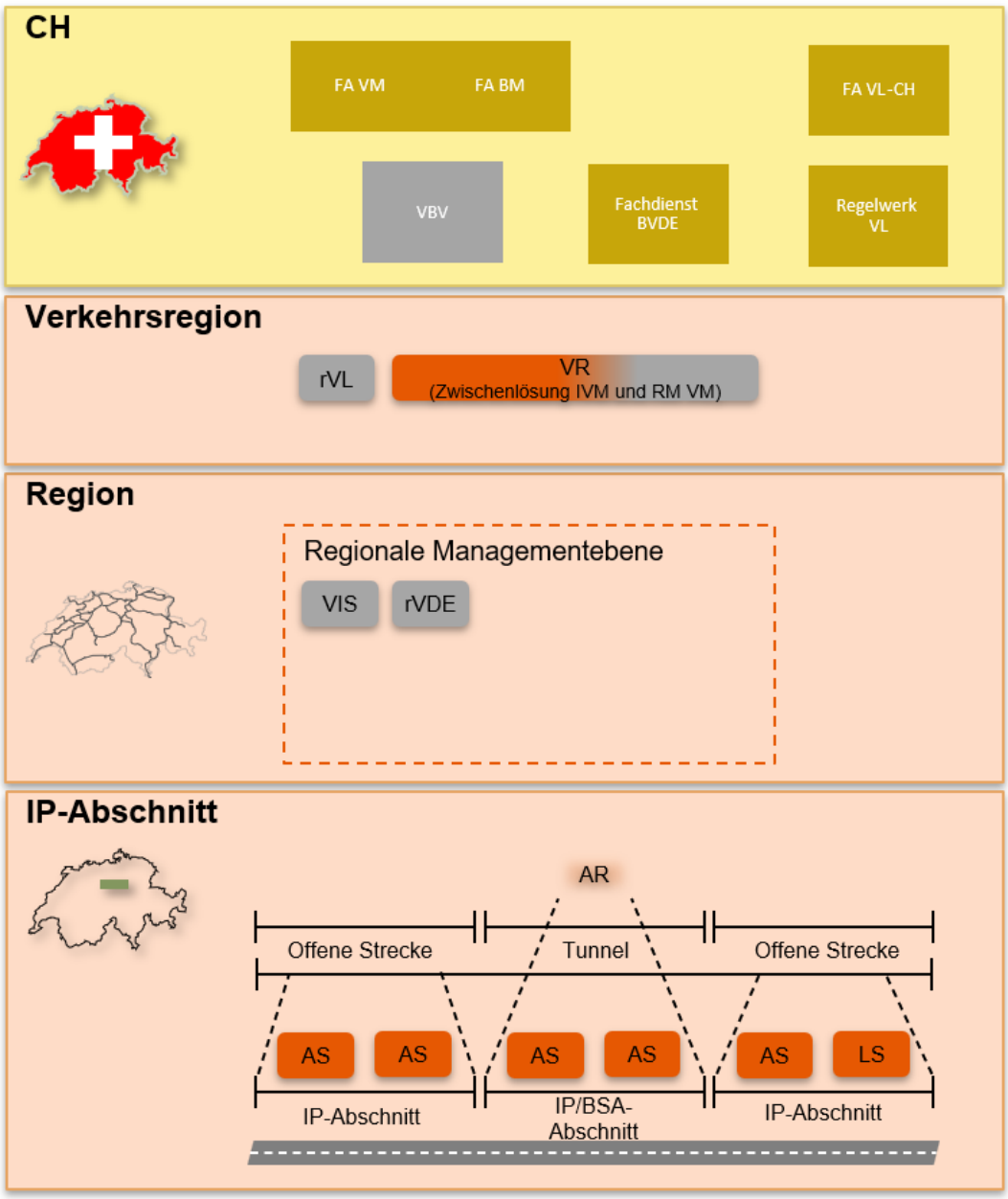


Figure 4 : Étendue spatiale des éléments spécifiques de l'architecture de gestion du trafic (représentation logique)

2.3.8 Systèmes de la Confédération, systèmes tiers et installations spéciales

L'architecture du système intègre des interfaces destinées à fournir des informations et des données aux systèmes internes de la Confédération ainsi qu'à des systèmes tiers externes au réseau IP EES. Selon la situation, les installations spéciales sont connectées via le réseau IP ou gérées comme des systèmes tiers. Ce point doit être défini dans le cadre du projet EES de la filiale.

2.3.8.1 Systèmes de la Confédération et systèmes tiers

Chaque connexion est examinée individuellement et intégrée en conséquence dans l'architecture. Seules des liaisons unidirectionnelles via des « Service User » sont mises en œuvre, sous réserve d'une approbation préalable du CAB OT Security.

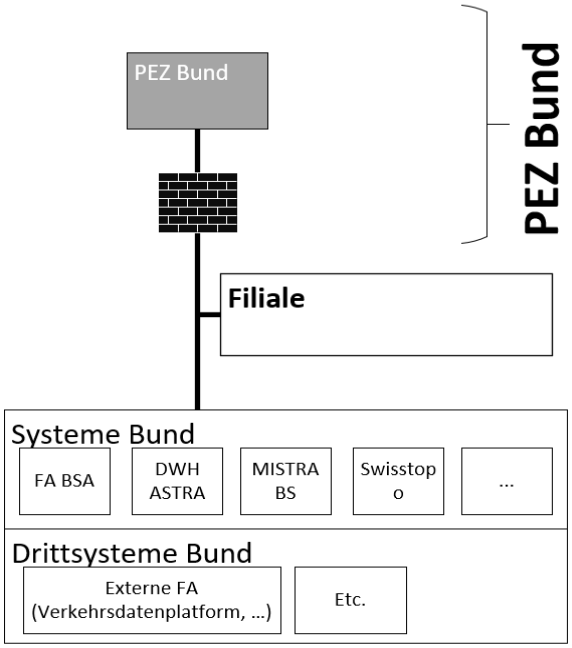


Figure 5 : Vue d'ensemble des systèmes de la Confédération et des systèmes tiers

2.3.8.2 Installations spéciales

Ces installations sont généralement exclusivement exploitées par du personnel externe (voir Organisation administrative et opérationnelle BSA-OT), et s'inscrivent dans un cadre réglementaire complexe propre au domaine technique concerné. Ces installations sont évaluées spécifiquement pour chaque projet, tant au niveau de l'intégration globale que de l'intégration dans l'architecture de communication. Les prescriptions spécifiques à chaque corps de métier sont précisées dans les directives/conventions correspondantes. Vue d'ensemble des installations spéciales :

Cantons, villes et communes :

- Installation de signalisation lumineuse (lorsque les nœuds sont régulés par des tiers) ;
- Détection des marchandises dangereuses ;
- Alimentation en eau ;

Sous-groupe bilan de la Confédération (sGrB Conf) :

- Photovoltaïque ;

Service d'intervention / pompiers :

- Système de défense incendie ;
- Portail thermique ;

Police :

- Centres de contrôle du trafic lourd (CCTL) ;
- Installation de contrôle de franchissement de feux rouges ;
- Mesure de distance inter-véhicule ;
- Installation de pesée de véhicules ;
- Installation de mesure de hauteur et de gabarit ;
- Installation de mesure de vitesse.

2.4 Périmètre d'influence

L'architecture système dispose de différents périmètres d'influence géographiques, qui correspondent généralement aux limites des filiales ou des unités territoriales et se réfèrent aux kilomètres de routes nationales. Les périmètres d'influence sont importants pour les utilisateurs des systèmes, tels que la centrale de gestion du trafic, la police et les unités territoriales. Lors de la planification et de la mise en œuvre des différents systèmes, leurs périmètres d'influence doivent par conséquent impérativement être considérés attentivement, afin que les utilisateurs puissent accomplir les tâches qui leur incombent dans leur domaine de responsabilité.

Du point de vue des utilisateurs, les périmètres d'influence suivants doivent être pris en compte :

Tableau 2 : Périmètres d'influence du point de vue des utilisateurs

Utilisateur	Périmètre d'influence
VMZ-CH	Ensemble des installations de gestion du trafic sur les routes nationales suisses des 1re, 2e et 3e classes
Police	Utilisation conjointe des EES pour la sécurité du trafic à l'intérieur des frontières cantonales
Unités territoriales	Tous les systèmes OT et EES au sein de l'unité territoriale

Pour la planification et la réalisation des EES, il convient de prendre en compte les périmètres d'influence suivants du point de vue des systèmes :

Tableau 3 : Périmètre d'influence - perspective systémique

Systèmes	Périmètre d'influence
Application métier	En règle générale : échelle nationale
VR	Dans des cas exceptionnels (phase temporaire/transitoire), plusieurs calculateurs de trafic (VR) peuvent être déployés au sein d'une même région de gestion du trafic. Il s'agit toutefois d'une exception qui doit être justifiée. Ces VR seront remplacés par la FA VL-CH.
UeLS-CH	à l'échelle de l'unité territoriale
rVDE, VIS, NT	à l'échelle de l'unité territoriale
Section EES / Section IP	à l'échelle de l'objet

3 Architecture SA-CH

Ce chapitre décrit les différents niveaux de l'architecture ainsi que les éléments qui la composent. Les exigences relatives aux éléments de chaque niveau ne sont pas détaillées ici. Les exigences de performance et les exigences fonctionnelles sont décrites dans les chapitres 4 et 5.

3.1 Niveau gestion

Le niveau gestion est le niveau le plus élevé de l'EES. Il constitue le niveau de commande et de contrôle central et supérieur pour l'ensemble de la Suisse. Des fonctions et des périmètres d'influence géographiques peuvent être attribués aux utilisateurs en fonction de leurs rôles et de leurs tâches. Le niveau gestion comprend le niveau applications et le niveau services métier.

3.1.1 Niveau applications

Le niveau applications regroupe les fonctions des applications métier utilisées à l'échelle nationale et ayant un impact sur tout le territoire. Il permet aux utilisateurs disposant de rôles spécifiques d'interagir avec le système via des interfaces utilisateurs. Les utilisateurs des applications peuvent être la VMZ-CH, la police et les unités territoriales.

Les applications métier (AM) soutiennent les processus métier de tous les utilisateurs concernés. Chaque AM dispose d'une interface utilisateur et d'une logique de commande associée, qui fait appel aux services métier ou aux services de base sous-jacents. Chaque utilisateur et chaque groupe d'utilisateurs disposent, selon leurs rôles et leurs droits d'accès définis dans le modèle d'utilisateurs (voir chapitre 3.2.1.4), de vues spécifiques dans une ou plusieurs applications métier. Plutôt que de réimplémenter des fonctionnalités identiques, les applications métier à développer doivent, dans la mesure du possible, utiliser les services de base et les services spécialisés existants.

Les AM suivantes sont déjà réalisées ou en cours de planification :

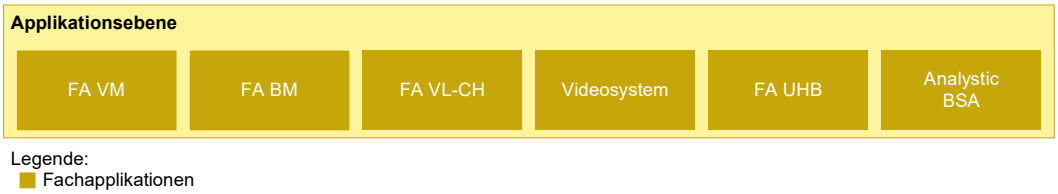


Figure 6 : Niveau applications

3.1.1.1 AM VM

L'AM Gestion du trafic (AM VM) soutient la diffusion de l'information et à la régulation du trafic, afin de garantir une fluidité maximale sur le réseau routier national (trafic individuel motorisé et transport lourd).

3.1.1.2 AM BM

L'AM Gestion de chantier (AM BM) garantit une vue d'ensemble constamment actualisée de tous les chantiers prévus et en cours sur la route nationale. Elle contient des informations relatives à la durée du chantier ainsi qu'aux restrictions de circulation affectant le tronçon concerné.

3.1.1.3 AM VL-CH

L'AM Gestion du trafic Suisse (AM VL-CH) est destinée à la gestion du réseau, des axes, des nœuds et à l'information routière afin de garantir la fluidité du trafic à l'échelle nationale. Elle comprend des fonctions de gestion du trafic, de gestion opérationnelle et de régulation

automatisées à l'aide d'algorithmes (voir directive ASTRA 15019), et permet aux utilisateurs d'accéder et de piloter toutes les installations de gestion du trafic sur les routes nationales (voir directive ASTRA 15003).

3.1.1.4 Système vidéo

Les systèmes vidéo du niveau de gestion font partie du système vidéo VIDEO-CH destiné à l'archivage manuel de séquences d'images sélectionnées liées à des événements. Après validation de l'UT, les séquences d'images présentant une valeur archivistique sont transférées des mémoires locales de l'UT vers l'archive centrale. L'archive est gérée selon des règles définies et dans le respect des dispositions relatives à la protection des données.

3.1.1.5 AM UHB

L'application métier Entretien et exploitation (AM UHB) soutient les unités territoriales dans l'exploitation opérationnelle et l'entretien des EES. En cas d'événements, les unités territoriales peuvent piloter les installations EES et ainsi soutenir les services d'intervention sur place. L'AM UHB contribue par ailleurs à une gestion efficace des actifs via l'acquisition et l'analyse des données d'exploitation des EES. Cet aspect sera précisé ultérieurement dans le cadre de la mise à jour de la directive.

3.1.1.6 Analytics BSA

Analytics BSA garantit l'exploitabilité de la base de données. Un ou plusieurs outils, toutefois tous connectés aux services spécialisés « Analyse de la base de données » et « Datawarehouse EES », peuvent être utilisés à cet effet.

Les outils Analytics permettent également de recourir à des technologies modernes d'analyse de données, telles que les fonctionnalités d'intelligence artificielle (IA). Cet aspect sera précisé ultérieurement dans le cadre de la mise à jour de la directive.

3.1.2 Niveau services métier

Les services métier mettent à disposition des fonctionnalités ou des données spécialisées encapsulées. Dans le périmètre d'un thème donné (p. ex. gestion de réseau), une fonctionnalité spécialisée complète comprend aussi bien l'application métier qu'un ou plusieurs services métier. Des fonctions spécifiques à l'OFROU au niveau gestion, telles que les prévisions de trafic, sont mises à disposition par les services métier.

Les fonctions et données des services métier couvrent en principe l'ensemble du territoire et sont accessibles par toutes les applications métier. Les services métier suivants sont planifiés ou déjà opérationnels :

Figure 7 : Niveau services métier

3.1.2.1 VBV

Vehicle-By-Vehicle (VBV) est un système qui recueille les données brutes d'un véhicule individuel émises par les postes de comptage ou les contrôleurs de comptage de trafic (ZSC), les traite et les transmet aux applications métiers. Les ZSC doivent être démantelés en coordination avec la migration du réseau IP EES.

3.1.2.2 Réglementation VL (logique de régulation du trafic)

La réglementation de la gestion du trafic (VL) inclut les fonctions spécialisées de l'AM VL-CH. Elle comprend les algorithmes spécifiques ainsi que les procédures de régulation nécessaires pour garantir une régulation dépendante du trafic sur la base des données de trafic actuelles, et pour déterminer les mesures requises du point de vue du trafic. La réglementation VL coordonne les demandes de commande manuelles et automatiques basées sur la régulation. Elle suit à cet effet des priorités définies et des règles paramétrables. Les prescriptions et exigences correspondantes figurent dans la directive 15019.

3.1.2.3 Service métier BVDE

Le service métier « Acquisition des données d'exploitation et de trafic » (BVDE) remplace le système VBV. Il traite toutes les données de trafic provenant de différentes sources et les met à disposition des applications dans les formats et agrégations souhaités (y c. les postes de comptage logiques du trafic).

3.1.2.4 Réglementation UHB

Ce service métier dépend de la mise en œuvre de l'AM UHB. Cet aspect sera précisé ultérieurement dans le cadre de la mise à jour de la directive.

3.1.2.5 Informations géographiques (SIG (Maps))

Informations géographiques centralisées fournies sous forme de données matricielles ou vectorielles (p. ex. vues aériennes ou Maps/cartes) pour le positionnement ou la localisation d'objets, telles qu'elles sont utilisées dans les systèmes de géoinformation (SIG) ou par d'autres applications nécessitant un contexte géospatial (p. ex. en tant qu'arrière-plan d'une carte). Ce service sera employé pour toutes les informations géographiques utilisées au sein du réseau IP EES.

3.1.2.6 Analyse de base de données

Ce service métier permet d'effectuer des analyses variées à partir des données disponibles au sein du réseau IP EES. Cet aspect sera précisé ultérieurement dans le cadre de la mise à jour de la directive.

3.1.3 EES Datawarehouse (DWH)

Ce service métier centralise différentes données, les enrichit le cas échéant, et les met à disposition en vue d'un traitement ultérieur. Cet aspect sera précisé ultérieurement dans le cadre de la mise à jour de la directive.

3.2 Niveau services de base / services centraux

Les services essentiels à la gestion des systèmes pertinents pour l'exploitation sont situés au niveau des services de base et des systèmes centraux. Les fonctions inter-réseaux sont exécutées (notamment la synchronisation de l'horloge commune) à ce niveau. Les services d'exploitation de niveau supérieur, qui offrent aux différentes parties prenantes une vue d'ensemble des systèmes, sont également intégrés à ce niveau.

Les services de base font partie intégrante du réseau IP EES et sont nécessaires à son exploitation efficace, efficiente et sécurisée.

3.2.1 Gestion OT

La gestion OT met à disposition, au sein des services de base, des systèmes centraux indispensables au fonctionnement de la communication réseau et des systèmes OT. Elle fournit également des portails centraux permettant d'accéder aux applications métier. Afin de garantir la sécurité, il convient, dans la mesure du possible, de limiter les droits d'accès au strict nécessaire.

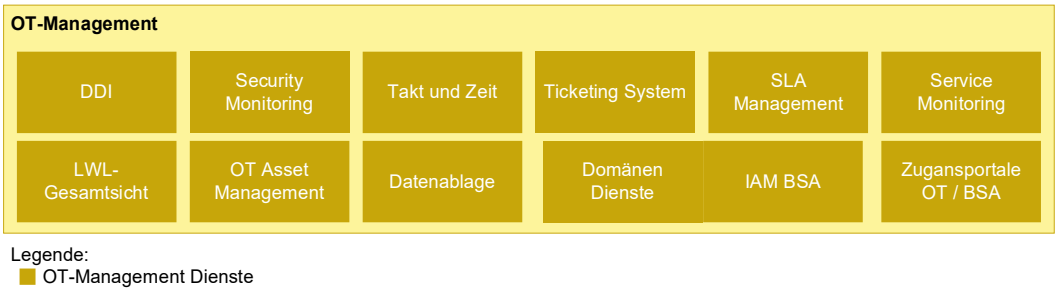


Figure 8 : Gestion OT

3.2.1.1 DDI

L'outil de gestion DNS, DHCP et adresses IP (DDI) est le système central de gestion des adresses IP mis à disposition de toutes les unités territoriales. Parallèlement à la gestion des adresses IP, il fournit également aux serveurs DNS et DHCP des unités territoriales les données nécessaires, notamment pour la résolution de noms. Chaque unité territoriale dispose d'un mandant dédié.

3.2.1.2 Security Monitoring

Le Security Monitoring vise à garantir la surveillance continue de la sécurité des systèmes OT. Des informations provenant de différentes sources (logs) sont collectées et analysées à cette fin. L'objectif est d'identifier les anomalies, les opérations suspectes ou les modifications non autorisées des systèmes OT ou du réseau, afin de pouvoir prendre les mesures appropriées.

3.2.1.3 Temps et horloge

Le niveau de gestion OT fournit une source d'horloge et de temps. Le « temps » fait référence à l'heure système usuelle composée de l'heure du jour (sur 24 heures) et de la date. L'« horloge » fait référence à un signal purement technique qui permet d'extraire une fréquence et une phase référentielles sans information intrinsèque sur le temps absolu.

Les autres prescriptions figurent dans la documentation ASTRA 83044.

3.2.1.4 Service de domaine et IAM EES

Les EES disposent d'un domaine propre « nationalstrassen.admin.ch », qui comprend un sous-domaine respectivement dédié aux UT, à la VMZ-CH et aux BD. Le domaine « nationalstrassen.admin.ch » est exclusivement réservé aux EES et géré de manière centralisée par l'OFROU. Les sous-domaines, y compris les serveurs AD et DNS correspondants des UT et de VMZ-CH, sont exploités par les UT/VMZ-CH.

Tous les objets utilisateurs et groupes d'utilisateurs (groupes de rôles) sont gérés de manière centralisée dans l'IAM EES. La synchronisation entre l'Active Directory (AD) des UT et l'IAM EES central est assurée par l'IAM EES. Les services DNS et DHCP nécessaires sont par ailleurs mis à jour par le DDI.

3.2.1.5 IAM EES

L'IAM (Identity and Access Management) EES est le système central de gestion des identités et des accès de l'OT/EES. Il garantit la gestion de tous les utilisateurs et rôles du domaine des routes nationales. Les identités ne sont gérées qu'une seule fois et les autorisations sont attribuées individuellement par chaque UT, par la VMZ-CH, ainsi que par les

BD/RZ EES. L'IAM EES est exclusivement utilisé pour l'OT/EES au sein du réseau IP EES et ne dispose d'aucune connexion avec d'autres services d'annuaires de la Confédération.

3.2.1.6 Portails d'accès OT/EES

Différents portails d'accès centralisés sont mis à disposition des utilisateurs autorisés dans les services centraux IP EES. Les portails d'accès garantissent l'accès aux systèmes autorisés au sein du réseau IP EES depuis l'extérieur de ce réseau, par exemple depuis Internet (Privileged Access Management, PAM). Les accès servent à la maintenance des systèmes (accès à distance) ou à l'accès aux applications métiers. Conformément à la documentation ASTRA 83042 Network Security Policy (NSP), ils font l'objet d'une protection particulière. Toutes les activités sont enregistrées et traçables.

3.2.1.7 Vue d'ensemble FO

La vue d'ensemble des fibres optiques (FO) offre un aperçu complet de l'infrastructure FO et sert de support aux exploitants et aux projets. En tant que prestataire de la Confédération, l'OFROU fournit différentes connexions FO destinées au Réseau optique des autorités fédérales (ROAF). La gestion des câbles FO relève de la responsabilité des unités territoriales de l'OFROU. Il s'agit ici uniquement d'une vue d'ensemble globale sans informations détaillées (celles-ci se trouvent au niveau des unités territoriales).

3.2.1.8 OT Asset Management

L'OT Asset Management sert à la saisie et à la gestion de l'inventaire OT, tant au niveau des unités territoriales que des services de base. Chaque unité territoriale dispose d'un mandant dédié.

3.2.1.9 Stockage des données

Le stockage des données comprend tous les documents de niveau supérieur, principalement axés sur l'exploitation du réseau IP EES, et mis à la disposition des exploitants.

3.2.1.10 Gestion des SLA (gestion des Service Level Agreements)

Un Service Level Agreement (SLA) désigne un accord entre un prestataire de services et un bénéficiaire et régit les caractéristiques de performance garanties. La gestion des SLA définit les notions telles que le temps de service, le temps de réaction, et le temps de rétablissement pour les EES. Elle fixe par ailleurs les valeurs possibles pour chacune des caractéristiques de performance. L'objectif est de définir et de gérer des SLA standardisés afin de garantir une articulation cohérente des différentes prestations et leur coordination sur le plan opérationnel.

3.2.1.11 Système de tickets

Le système de tickets vise à soutenir les principaux processus d'exploitation, tels que la gestion des incidents, la gestion des problèmes, la gestion des changements et les demandes de service. Ce système de tickets de niveau supérieur reçoit les messages des systèmes de tickets des UT nécessaires à l'exploitation globale.

3.2.1.12 Monitorage des services

Le monitorage des services offre une vue d'ensemble de l'état du réseau IP EES, des connexions au réseau IP EES Backbone et des services et outils centraux. Cette vision de service de bout en bout est impérative lorsqu'un incident affecte plusieurs UT et qu'une analyse et une résolution de l'incident au niveau supérieur s'avèrent nécessaires (remontée des incidents).

Le monitorage des services est un outil central exploité et utilisé par l'organisation centrale (ou par le service opérationnel de niveau supérieur).

3.2.2 Services OT

Figure 9 : Services OT

3.2.2.1 Gestion du service hivernal et services météo

La gestion du service hivernal comprend des systèmes et services destinés à identifier de façon précoce les chaussées dangereuses et les conditions météorologiques, afin de permettre une planification et une conduite optimales des mesures de service hivernal. Les services météo comprennent les composants centraux permettant l'acquisition des données météorologiques sur les routes nationales. Ils incluent notamment les systèmes d'alerte précoce de verglas.

3.2.2.2 Services de certificats

Pour garantir la sécurité du trafic de données, y compris au sein du réseau IP EES, seuls des protocoles sécurisés sont autorisés. Des certificats numériques, délivrés par un organisme de certification privé interne (Certificate Authority, CA), sont à cet effet nécessaires. Ces certificats permettent d'attester l'identité électronique des partenaires de communication. La CA privée est également conçue comme un service intégré aux services de base. Les certificats délivrés par cette CA servent exclusivement à la communication des EES au sein du réseau IP EES et sont spécialement conçus pour répondre à leurs besoins spécifiques.

3.2.2.3 Services vidéo

Les services vidéo font partie du système vidéo VIDEO-CH et sont destinés à la transmission des images et flux vidéo à différentes parties prenantes extérieures au réseau IP EES ou à l'OFROU. Les images vidéo sont mises à la disposition des différents groupes de destinataires conformément aux dispositions relatives à la protection des données en vigueur et dans le respect des dispositions de sécurité de l'OT Security.

3.2.2.4 Services de mise à jour

Différents services de mise à jour assurent l'actualisation des logiciels, des correctifs de sécurité ou des fichiers de signature utilisés pour la protection antivirus. Aucun accès direct des systèmes OT aux services de mise à jour des fabricants n'étant autorisé, les services de mise à jour fournissent les données nécessaires de manière centralisée via des mécanismes de sécurité spécifiques.

3.2.2.5 Passerelles applications métier externes

Les passerelles permettent aux applications métier d'échanger des données avec des services et des applications métier spécifiques situés en dehors du périmètre du réseau IP EES. Les passerelles font partie de l'infrastructure de sécurité du réseau IP EES. Les différentes passerelles sont décrites en détail dans l'architecture système des BD ou dans les architectures système des AM.

3.2.2.6 Outils techniques d'exploitation

Les outils techniques d'exploitation sont destinés à la gestion et à la surveillance des services de base du réseau IP EES UT, des environnements de virtualisation des services de base et des éléments de sécurité. Les systèmes sont principalement utilisés pour soutenir les processus d'exploitation, gérer l'inventaire matériel et logiciel, et configurer les composants système. Ils jouent par ailleurs un rôle clé dans l'identification et l'élimination des perturbations et contribuent à la sécurité du réseau et des systèmes.

Les outils techniques d'exploitation incluent notamment le système de gestion du réseau (NMS) ou la surveillance (Monitoring) et l'alerte (Alarming). La définition et les exigences relatives au NMS figurent dans la directive 13040.

3.3 Niveau de gestion du trafic suisse

Afin de permettre aux opérateurs, aux ingénieurs en trafic et aux administrateurs d'effectuer leurs tâches, la VMZ-CH utilise différents éléments de l'architecture système au niveau de gestion du trafic suisse. La VMZ-CH a accès aux différentes applications métier ainsi qu'à la vue VM dans l'UeLS-CH et, dans certains cas, directement aux installations VM.

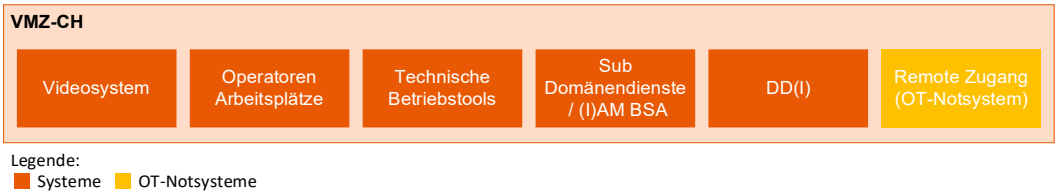


Figure 10 : Niveau de gestion du trafic suisse

3.3.1.1 Système vidéo

Le système vidéo de la VMZ-CH fait partie du système vidéo VIDEO-CH et sert à diffuser les flux vidéo sur les postes de travail des opérateurs et sur le mur vidéo de la VZM-CH. La sélection des flux vidéo peut être préconfigurée manuellement ou automatiquement en fonction des événements. Il est possible de sélectionner des images en direct ou des images enregistrées dans la mémoire circulaire.

3.3.1.2 Postes de travail des opérateurs

Les postes de travail des opérateurs sont principalement destinés à la surveillance, à la gestion et à l'exploitation des systèmes de gestion du trafic. Il ne s'agit pas de postes de travail de l'administration fédérale, mais de postes de travail dédiés de l'OT EES.

3.3.1.3 Outils techniques d'exploitation

Les outils techniques d'exploitation sont destinés à la gestion et à la surveillance du réseau IP EES VMZ-CH, des environnements de virtualisation de la VMZ-CH et des éléments de sécurité. Les systèmes sont principalement utilisés pour soutenir les processus d'exploitation, gérer l'inventaire matériel et logiciel, et configurer les composants système. Ils jouent par ailleurs un rôle clé dans l'identification et l'élimination des perturbations et contribuent à la sécurité du réseau et des systèmes.

Les outils techniques d'exploitation incluent notamment le système de gestion du réseau (NMS) ou la surveillance et l'alerte. La définition et les exigences relatives au NMS figurent dans la directive 13040.

3.3.1.4 Services de sous-domaines / (I)AM BSA

Les services de sous-domaines comprennent le sous-domaine « vmzch.nationalstrassen.admin.ch », l'Active Directory correspondant, ainsi que les services DNS et DHCP. L'IAM ESS transmet directement à l'AD les données actuelles relatives aux utilisateurs et aux groupes d'utilisateurs.

3.3.1.5 DD(I)

Les données nécessaires, par exemple pour la résolution de noms, sont transmises aux serveurs DNS et DHCP de la VMZ-CH par le DDI central. En cas de panne des composants centraux IAM EES et DDI, les services locaux tels que l'AD, le DNS et le DHCP restent opérationnels sans restriction pour l'exploitation quotidienne.

3.3.1.6 Accès à distance (système de secours OT)

L'accès distant local de la VMZ-CH sert d'accès de secours en cas de panne du service

« Portails d'accès OT-EES » au niveau supérieur des services de base. Les autorisations d'accès sont limitées au minimum requis pour garantir la sécurité.

3.4 Régions de gestion du trafic

Une région fortement interconnectée sur le plan du trafic et considérée comme une unité du point de vue de la circulation constitue une région de gestion du trafic. Elle peut s'étendre au-delà des limites des UT ou des filiales (voir Figure 5) et, pour la gestion et le monitorage du trafic, concerner l'ensemble de la Suisse. La région de gestion du trafic est définie selon une logique de trafic, et non selon une logique administrative. Elle englobe tous les secteurs qui sont liés sur le plan fonctionnel. L'objectif est de garantir une vision et une planification cohérentes de l'espace de circulation sur la base de liaisons de transport réelles.

Le calculateur de trafic (VR) assure, à titre de solution transitoire, la coordination inter-tronçons des systèmes inférieurs (commande d'installation signalisation (AS-S) ou commande locale (LS)), lorsque de telles fonctions de trafic sont nécessaires dans la zone concernée (p. ex. états d'exploitation étendus ou harmonisation des vitesses inter-tronçons (sur plusieurs tronçons ou jonctions/échangeurs) ; cette mesure est généralement requise dans les régions EES plus complexes sur le plan du trafic). L'objectif est de limiter le déploiement de VR par région, afin de préserver les fonctions principales suivantes :

- Coordination et pilotage des AS subordonnées (notamment en cas de chevauchements et de dépendances) ;
- Activation des états d'exploitation combinés (standard) de toutes les mesures de gestion du trafic à l'aide d'une prévisualisation/image réelle, conformément à la direction 15019 ;
- Mise en œuvre des dépendances entre tronçons (signalisation de dangers, signaux de vitesse) ;
- Régulation des R-BAU et des dosages de rampes.

Installations non conformes à la directive 15019 :

- Régime de circulation temporisé en cas de défaillance de la saisie des données de trafic ;
- États d'exploitation couvrant l'ensemble du territoire (80 km/h, chaussée glissante, etc.) ;
- La synchronisation entre plusieurs VR voisins doit être garantie.

Les VR constituent une solution provisoire et seront ultérieurement remplacés par l'AM VL-CH (voir chapitre 6 Migration).

3.4.1 Gestion de réseau par tronçon ou à l'échelle nationale

La gestion du trafic peut s'effectuer aussi bien au niveau d'un tronçon spécifique qu'à l'échelle nationale. Dans le déploiement final, l'AM VL-CH régulera au minimum les HV-AD, les DoRa et les R-Bau conformément à la logique de régulation du trafic, ainsi que les PMV.

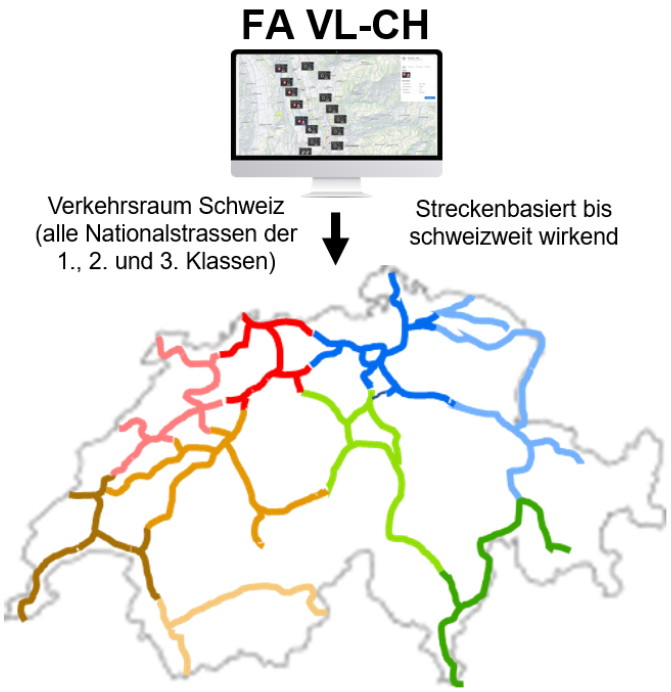


Figure 11 : Périmètre d'influence de l'AM VL-CH

3.4.2 Exemple d'une gestion de trafic par tronçon

Quelques exemples des installations de gestion du trafic actuellement en place dans le cadre de la gestion du trafic par tronçon sont présentés ci-après.

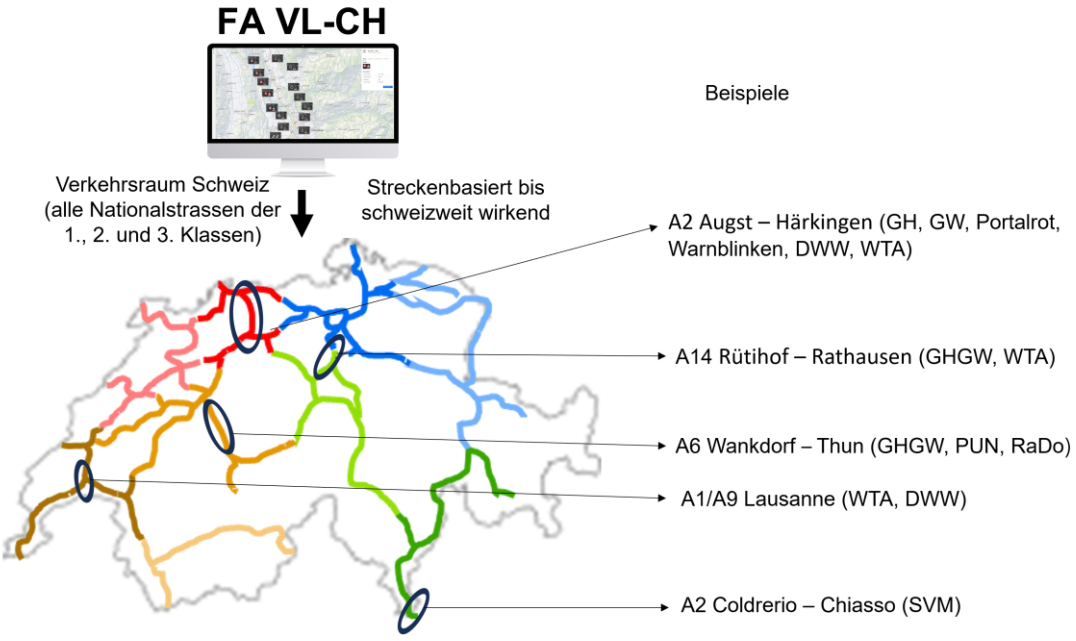


Figure 12 : Gestion du trafic par tronçon

3.4.2.1 A2 Augst – Härkingen (HV, AD, feu rouge au portail, feux clignotants avertisseurs, SVI, PMV)

La réduction à une voie de circulation en direction de Berne (rampe de raccordement depuis l'A2 vers l'A1) et le trafic important sur l'A1 entraînent un bouchon qui se prolonge sur la rampe sud du Belchen sur l'A2. La logique de régulation du trafic réduit automatiquement la vitesse. À partir d'une certaine longueur de bouchon, la VMZ-CH réduit la vitesse dans le tunnel du Belchen ou dans la zone qui précède ou qui suit, et active l'avertissement de bouchon et les feux de détresse dans le tunnel. Si le bouchon se prolonge, le tunnel est temporairement bloqué (feu rouge au portail). Si le bouchon s'allonge encore, des mesures similaires sont mises en place dans les trois autres tunnels : Oberburg, Ebenrain et Arisdorf. À partir d'un certain retard, les destinations éloignées telles que Chiasso (I), le Gotthard et Lucerne via l'A3, ainsi que l'échangeur de Birrfeld vers l'échangeur A1 Wiggertal, sont également déviées à l'aide des WTA.

3.4.2.2 A14 Rütihof – Rathausen (HV-AD, PMV)

Le bouchon quotidien des pendulaires sur l'A14, avant l'échangeur de Rotsee, est régulé par un système HV-AD. La VMZ-CH observe l'évolution du trafic et prend si nécessaire d'autres mesures. Il peut s'agir de WTA mis en place avant la fin du bouchon pour prévenir les usagers, ou encore de déviations depuis Zurich via le Wiggertal, dans la mesure où l'itinéraire bis est libre.

3.4.2.3 A6 Wankdorf-Thoune (HV-AD, R-BAU, DoRa)

Une HV-AD automatisée est déployée sur l'ensemble du tronçon, et un dosage de rampe (DoRa) entièrement automatique est en place à l'entrée de la jonction de Rubigen. En cas d'accident sur la bretelle d'accès, la police et la VMZ-CH doivent pouvoir désactiver le DoRA. Si nécessaire, les tronçons avec R-BAU entre Muri et Wankdorf sont vérifiés visuellement par la VMZ-CH, puis autorisés (ou non).

3.4.2.4 A1/A9 Lausanne (PMV, SVI)

La VMZ-CH en Suisse romande ne dispose que de quelques caméras et d'aucun système, à l'exception des WTA et de la SVI. Ces derniers sont notamment utilisés de manière combinée lorsque des perturbations du trafic sont constatées ou que des fermetures sont mises en place sur l'A1 en direction de Berne, sur l'A9 entre Lausanne et Vevey ou sur l'A12. Les systèmes régionaux sont gérés par la centrale régionale de gestion du trafic, et seront à l'avenir également exploités via la FA VL-CH.

3.4.2.5 A2 Coldrerio – Chiasso (GTL)

Un système de régulation/compte-gouttes est en place pour le trafic poids lourds entre l'aire de ravitaillement de Coldrerio et la douane commerciale de Chiasso. Ce système est activé manuellement par la VMZ-CH en cas de bouchon provenant de la douane commerciale de Chiasso vers l'A2. Si le bureau de douane Chiasso-Brodega constate un engorgement de l'ensemble du trafic, le système peut également être utilisé pour la réduction de la vitesse et l'avertissement des dangers.

3.4.3 Éléments d'architecture spécifiques à la gestion du trafic basés sur les tronçons

La majorité des éléments d'architecture de la gestion du trafic sont situés sur un « tronçon à ciel ouvert » et déployés sous forme d'installations dédiées (utilisation principale en exploitation normale). Si le tronçon défini comporte également des tunnels, les installations de gestion du trafic (installations combinées, p. ex. rouge au portail, caméras, signal de vitesse, etc.) sont également intégrées dans cette zone.

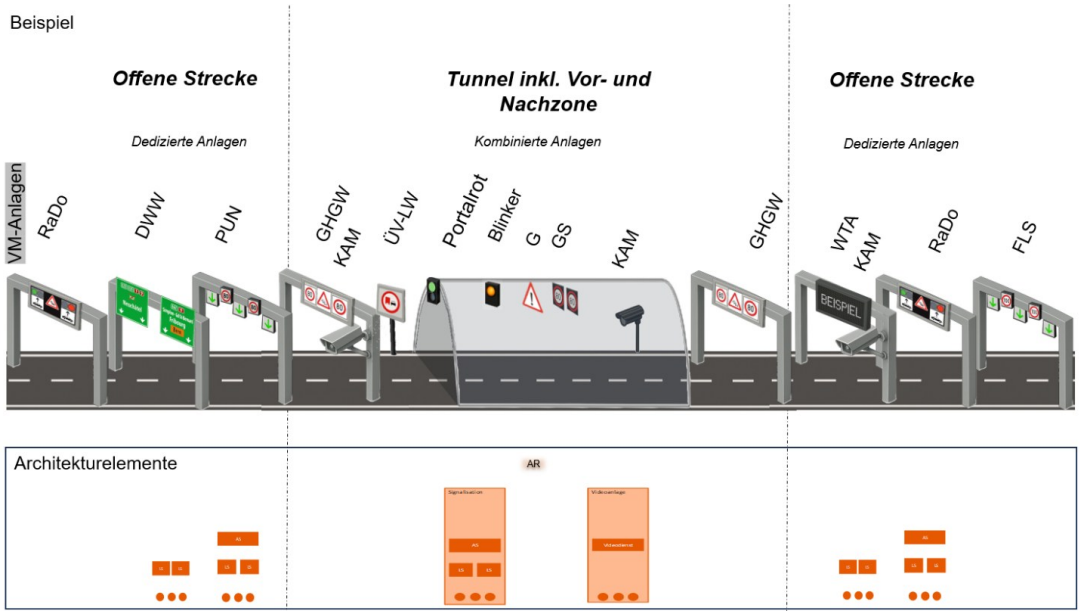


Figure 13 : Exemple d'« installations dédiées » et d'« installations combinées »

Exemple de HV-AD sur un tracé comprenant des tronçons à ciel ouvert et un tunnel :

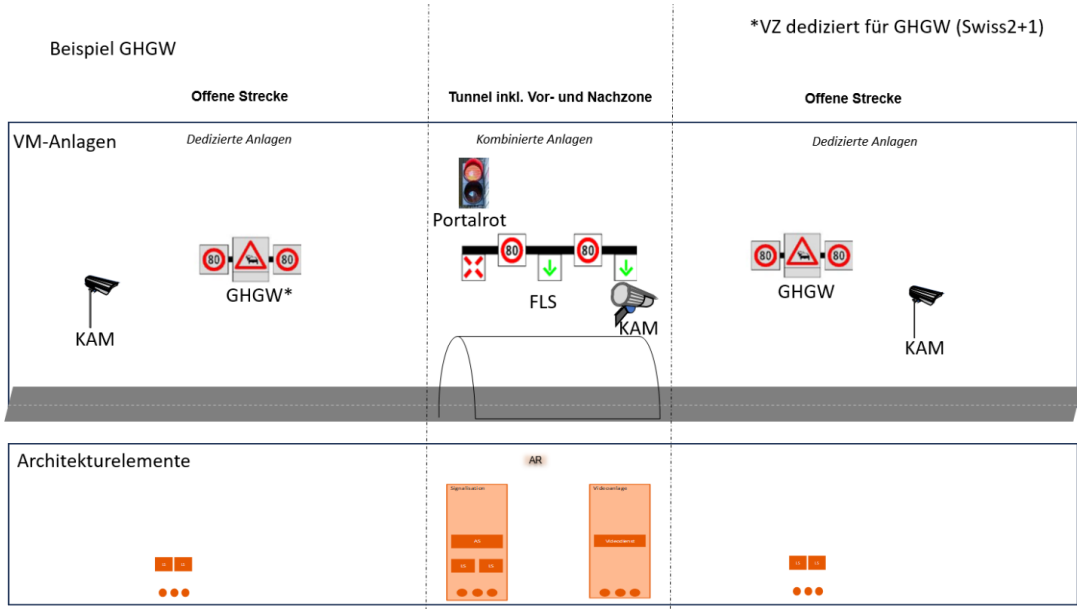


Figure 14 : Exemple de HV-AD avec « installations dédiées » et « installations combinées »

3.5 Niveau de gestion régional UT

Le niveau de gestion régional UT comprend les systèmes OT/EES implantés au sein d'une unité territoriale. L'UeLS-CH et les systèmes OT/EES régionaux spécifiques sont inclus.

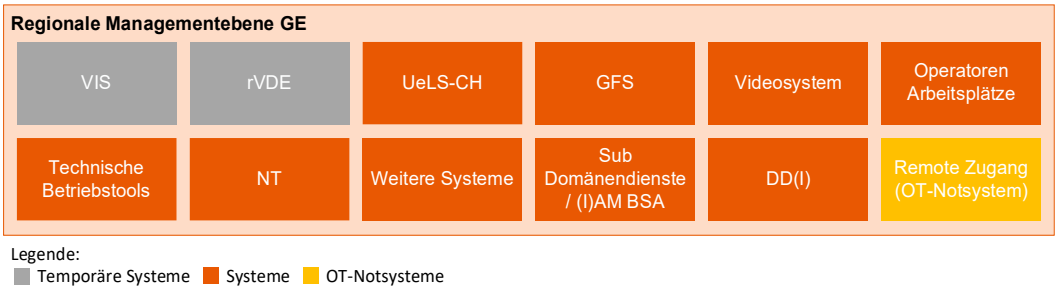


Figure 15 : Niveau de gestion régional des unités territoriales

3.5.1 Système d'information routière (VIS)

Le système d'information sur le trafic (VIS) commande et coordonne le panneau à messages variables (PMV) et la signalisation variable de direction (WWW) dans les sections EES sans calculateur de trafic (VR). Les systèmes d'information routière (VIS) signalent les perturbations du trafic, les travaux, les conditions routières particulières ou des dangers sur les routes nationales.

Les VIS constituent une solution provisoire et seront ultérieurement remplacés par l'AM VL-CH (voir chapitre 6 Migration).

3.5.2 Acquisition régionale des données de trafic (rVDE)

L'acquisition régionale des données du trafic ou le contrôleur de comptage de trafic (ZSC) recueille et traite les données des postes de comptage et les met à disposition des services spécialisés. Les ZSC doivent être démantelés en coordination avec la migration du réseau IP EES.

3.5.3 UeLS-CH

Le système de gestion générale suisse (UeLS-CH) assiste les utilisateurs dans la surveillance et la commande des équipements d'exploitation et de sécurité au sein d'une unité territoriale. De plus amples informations sont disponibles dans la documentation ASTRA 83054.

Les UeLS-CH sont connectés aux serveurs de gestion section (AR) via le réseau IP EES.

3.5.4 Installation de surveillance et d'alarmes météo (GFS)

Les données de l'installation de surveillance et d'alarmes météo (également appelée système de détection du verglas) sur les routes nationales sont traitées au sein du réseau IP EES et mises à disposition de toutes les parties prenantes autorisées.

3.5.5 Système vidéo

Le système vidéo du niveau gestion régional se compose de différents éléments et fait partie du système vidéo VIDEO-CH. Le système est conçu de manière à garantir le fonctionnement autonome de la fonctionnalité vidéo au sein d'une UT.

Il met à disposition des fonctions d'analyse d'images et de détection d'événements dans les objets, et des mémoires circulaires sont fournies pour le stockage des images vidéo. Les utilisateurs disposent de clients vidéo qui leur permettent de contrôler immédiatement la caméra et d'accéder aux images en direct, aux vidéos enregistrées et aux métadonnées.

La définition et les exigences relatives à VIDEO-CH figurent dans la directive 13005.

3.5.6 Postes de travail des opérateurs

Les postes de travail opérateurs sont destinés à la surveillance, la gestion et l'exploitation des systèmes. Les postes de travail fédéraux en sont exclus.

3.5.7 Outils techniques d'exploitation

Les outils techniques d'exploitation sont destinés à la gestion et à la surveillance du réseau IP EES UT, des environnements de virtualisation des locaux techniques OT et des éléments de sécurité. Les systèmes sont principalement utilisés pour soutenir les processus d'exploitation, gérer l'inventaire matériel et logiciel, et configurer les composants système. Ils jouent par ailleurs un rôle clé dans l'identification et l'élimination des perturbations et contribuent à la sécurité du réseau et des systèmes.

Les outils techniques d'exploitation notamment le système de gestion du réseau (NMS), le système de surveillance et d'alerte ainsi qu'un système de tickets. La définition et les exigences relatives au NMS figurent dans la directive 13040.

3.5.8 Téléphone de secours (NT)

Les prescriptions actuelles figurent dans la fiche technique 23 001-11650 du manuel technique. Cet aspect sera précisé ultérieurement dans le cadre de la mise à jour de la directive.

3.5.9 Autres systèmes

Les « autres systèmes » désignent des systèmes régionaux destinés à soutenir des tâches métier spécifiques.

3.5.10 Services de sous-domaines / IAM EES

Les services de sous-domaines comprennent le sous-domaine « ge.nationalstrassen.admin.ch », l'AD correspondant, ainsi que les services DNS et DHCP. L'IAM ESS transmet directement à l'AD les données actuelles relatives aux utilisateurs et aux groupes d'utilisateurs.

3.5.11 DD(I)

Les données nécessaires, par exemple pour la résolution de noms, sont transmises aux serveurs DNS et DHCP des unités territoriales par le DDI central. En cas de panne des composants centraux IAM EES et DDI, les services locaux tels que l'AD, le DNS et le DHCP restent opérationnels sans restriction pour l'exploitation quotidienne.

3.5.12 Accès à distance (systèmes de secours OT)

L'accès distant local de l'UT sert d'accès de secours en cas de panne du service « Portails d'accès OT-EES » au niveau supérieur des services de base. Les autorisations d'accès sont limitées au minimum requis pour garantir la sécurité.

3.6 Section EES

Une section EES désigne une portion fonctionnellement autonome de la route nationale comprenant des équipements d'exploitation et de sécurité. Le niveau section EES est représenté dans la figure Figure 3 du chapitre 2.3.7.

3.6.1 Serveur de gestion section (AR)

Le serveur de gestion section fait partie de la section EES et assure la liaison entre les commandes d'installation et le niveau de gestion régional. Ses tâches principales incluent la visualisation de la section EES, la communication, l'exploitation, le traitement des interdomaines (automatiques, semi-automatiques, et manuels), ainsi que des alarmes et des messages de toutes les installations qui lui sont rattachées.

3.6.2 Commande d'installation et commande locale

Le niveau installation comprend les commandes d'installation (AS) et les commandes locales (LS).

3.6.2.1 Commande d'installation (AS)

La commande d'installation (AS) de la section EES surveille et pilote d'installation correspondante. Elle met à disposition la logique des processus spécifique à l'installation et, le cas échéant, l'interface MMI (à l'exception des installations de gestion du trafic). Les installations et parties d'installation suivantes disposent d'une AS.

- Distribution d'énergie (E) ;
- Éclairage (B) ;
- Ventilation (L) ;
- Signalisation (S), désignée AS-S et à utiliser pour AS-WTA, AS-DoRa ou AS-HVAD ;
- Pour les installations de surveillance (U) :
  - Installation de détection incendie tunnel (MBT), resp. AS fumée et AS thermique ;
  - Installations vidéo (VMS) ;
  - Installation de surveillance et d'alarmes météo (GFS) ;
  - Installation de surveillance et d'alarmes des dangers naturels (SLM) ;
  - Système de gestion installation divers (DIV) ;
- Pour la communication et le système de gestion (KL) :
  - Installations radio (FE via AS DIV) ;
  - Téléphone de secours (NT).

Aucune AS n'est prévue pour les galeries de sécurité (SISTO). Les différentes parties d'installation de la SISTO doivent être intégrées dans l'AS correspondante. Le cas échéant, une intégration dans l'AS Divers est possible.

Dans des cas exceptionnels, certaines AS peuvent être intégrées dans l'AS DIV et surveillées et pilotées par celle-ci. Ces exceptions doivent être définies dans le mandat de projet.

La liste suivante offre un aperçu des principales fonctions de l'AS :

- Contient la logique d'installation, qui fait partie de la logique de processus. La logique de processus se trouve sur l'AS ou la LS. La configuration dépend de l'architecture et doit être définie en fonction de chaque projet ;
- Fournit une interface standardisée avec les points de données spécifiés pour la communication avec le serveur de gestion section ;
- Génération de messages ;
- Communication avec les commandes locales (LS) ;
- Échange des interdomaines.

Les AS communiquent avec l'AR, avec leurs propres commandes locales (LS) et, le cas échéant, avec d'autres AS (uniquement pour les interdomaines de type 1).

3.6.2.2 Séparation des tubes de l'AS

Une séparation par tube est nécessaire dans des cas justifiés (complexité, disponibilité, migration, transformation). Pour les ouvrages à circulation unidirectionnelle (plusieurs tubes), l'AS peut, selon le projet, être conçue séparément pour chaque tube. La commande d'installation peut également prendre en compte une séparation par tube / par direction.

3.6.2.3 Commande locale (LS)

Les commandes locales surveillent ou pilotent une partie d'installation. Il peut aussi bien s'agir d'un sous-domaine en termes d'étendue, tel que la commande d'un tronçon partiel d'un tunnel ou d'un tube, ou en termes de fonction (commande d'une fonction partielle des installations).

Les LS doivent toujours être conçues séparément pour chaque tube. Dans le cas des petits tunnels à un seul tube et une seule centrale, la fonction de la commande locale peut être assurée par la commande de l'installation.

3.6.3 Capteurs et actionneurs

Le niveau le plus bas de l'EES (niveau terrain) comprend les actionneurs et les capteurs. Ceux-ci sont spécifiques au domaine et doivent être, dans la mesure du possible, des composants standard. Exemples : luminaires, servomoteurs, signaux de circulation, postes de comptage trafic, détecteurs de fumée, etc. Les capteurs et actionneurs peuvent également constituer des systèmes plus complexes. Exemples : systèmes de portes, ventilateurs, PMV, etc.

3.7 Systèmes de la Confédération

Les systèmes de la Confédération, tels que le Datawarehouse (DWH) de l'OFROU, fonctionnent indépendamment de l'architecture système. Il est donc nécessaire de définir des interfaces précises, afin de permettre une intégration (transfert de données unidirectionnel) dans l'architecture système.

Pour accéder au réseau IP EES, toutes les passerelles réseau entre les réseaux IP EES et les systèmes de la Confédération doivent passer par la Policy Enforcement Zone (PEZ) des services de base.

3.8 Systèmes tiers

Les systèmes tiers fonctionnent indépendamment de l'architecture système. Il est donc nécessaire de définir des interfaces précises, y compris des responsabilités clairement établies, afin de permettre leur intégration dans l'architecture système. Concrètement, il peut par exemple s'agir de l'intégration dans l'architecture système de systèmes de guidage de parties externes ainsi que d'installations de signalisation lumineuse appartenant aux cantons et aux communes.

3.9 Installations spéciales

Les installations spéciales appartiennent à l'OFROU et sont, en règle générale, exclusivement exploitées et utilisées par des tiers. Selon la situation, ces installations peuvent être connectées aux EES de l'OFROU via le réseau IP EES UT, ou gérées comme des systèmes tiers. Ce point doit être défini et approuvé dans le cadre des projets EES.

4 Exigences de performance

Les sous-chapitres suivants abordent les possibilités de mise en œuvre technologique permettant de garantir à la fois une continuité opérationnelle maximale et un niveau de sécurité élevé. Il s'agit ainsi de déterminer quelles technologies peuvent être déployées dans quelles conditions-cadres pour assurer l'exploitation ininterrompue souhaitée.

4.1 Utilisation de la virtualisation

Conformément à la directive 13009, les composants correspondants doivent être installés dans les locaux décrits ci-après. D'autres prescriptions figurent dans la directive ASTRA 13009. La virtualisation vise à garantir une protection contre la défaillance d'un serveur physique et à optimiser l'utilisation des ressources.

4.1.1 Local technique OT

Les systèmes du niveau de gestion régional sont hébergés dans les locaux techniques OT (OTTR, 2 par UT). Ces locaux accueillent principalement des systèmes de serveurs et de stockage ainsi que, dans certains cas, la liaison backbone.

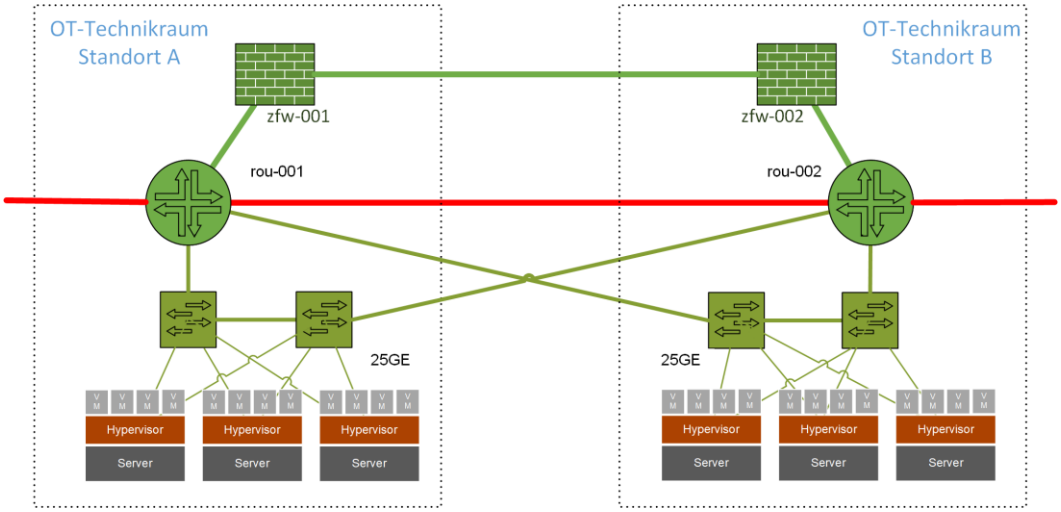


Figure 16 : Local technique OT

Des plateformes de virtualisation sont en principe utilisées dans les OTTR. Ces plateformes de virtualisation doivent être mises en place de manière géoredondante. Le dimensionnement dépend fortement des ressources nécessaires. L'objectif est d'exploiter largement les plateformes de virtualisation et d'y déployer tous les services et applications virtualisables du niveau gestion régional.

4.1.2 Locaux techniques/centrales techniques

Les locaux techniques/centrales techniques servent principalement à héberger les installations techniques nécessaires au maintien de l'exploitation (telles que les infrastructures de communication, les serveurs de gestion section et, dans certains cas, les commandes d'installation (p. ex. VMS)). L'utilisation de plateformes virtualisées (AR-Hosts) est également requise.

Selon les exigences, ces plateformes de virtualisation peuvent être déployées de manière simple dans une seule centrale, ou de manière géoredondante dans deux centrales. Le dimensionnement des plateformes de virtualisation dépend là aussi fortement des ressources nécessaires. Afin de se protéger contre la défaillance d'un serveur physique, deux serveurs au minimum doivent être prévus.

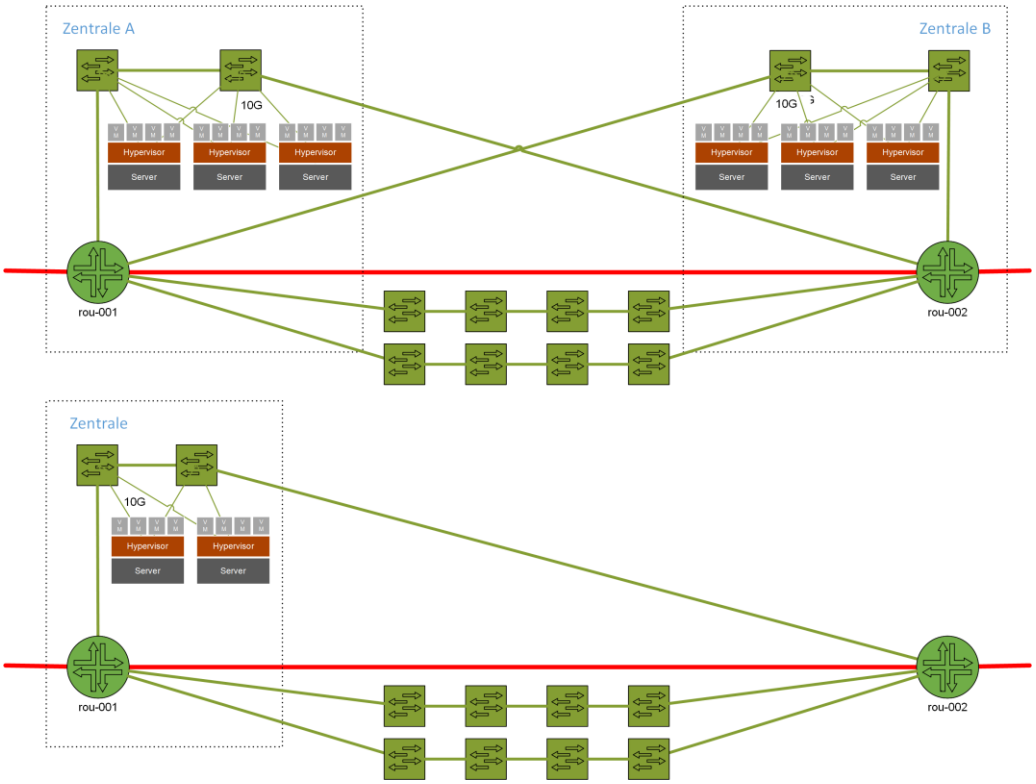


Figure 17 : Local technique/centrale technique

Pour les tunnels de plus de 600 m équipés d'un système de ventilation, les AR, et donc les plateformes de virtualisation, doivent être conçus de manière redondante. Dans la mesure du possible, une géoredondance doit être visée. Dans tous les autres cas, il convient de déterminer si une plateforme de virtualisation simple est suffisante du point de vue de la disponibilité.

4.2 Systèmes d'exploitation et redondances

4.2.1 Systèmes d'exploitation et plateforme de virtualisation

Compte tenu de la multitude de systèmes d'exploitation (souvent de différentes générations) utilisés dans les environnements OT et EES, il est nécessaire de pouvoir exploiter et maintenir un large éventail de technologies.

Étant donné la grande variété de systèmes d'exploitation invités (Guest-OS) installés sur les machines virtuelles (VM), la plateforme de virtualisation doit couvrir un large éventail de technologies, autrement dit les prendre en charge et pouvoir les exploiter. Dans ce domaine, une harmonisation visant à limiter le nombre de technologies doit à l'avenir être mise en œuvre. Des systèmes d'exploitation et des bases de données largement reconnues sur le marché devront notamment être utilisés.

4.2.2 AR redondants

Pour les tunnels de plus de 600 m équipés d'un système de ventilation, les AR doivent être conçus de manière redondante. À cet égard, les prescriptions suivantes s'appliquent :

- La redondance doit être garantie à l'intérieur de l'objet ou de la section IP correspondante. La redondance ne peut pas être établie à l'aide de moyens extérieurs à la section IP ;
- Différents mécanismes peuvent être utilisés pour la mise en œuvre technique :
  - Sur le plan applicatif, via les mécanismes de l'AR sur deux plateformes de virtualisation réparties dans deux centrales ;

  - Utilisation des redondances des plateformes de virtualisation. Les fabricants de ces plateformes proposent généralement des possibilités spécifiques à chaque plateforme (p. ex. High Availability) ;
  - Combinaisons des deux mécanismes ci-dessus.
- La décision concernant les mécanismes à mettre en œuvre doit être prise pour chaque objet ou section IP.

4.2.3 AS en version redondante

Les principes suivants s'appliquent pour les commandes d'installation :

- L'AS du système de ventilation doit être conçue de manière redondante (commande) ;
- L'installation de détection incendie tunnel est à considérer comme intrinsèquement redondante avec une AS thermique et une AS fumée distinctes (variante 2, voir annexe V, figure V.9), ou la partie d'installation fumée doit être intégrée dans l'installation de ventilation (variante 3, voir annexe V, figure V.10) ;
- L'AS signalisation n'est pas conçue de manière redondante (les exceptions doivent être approuvées par l'I-FU), mais le feu rouge au portail doit être activé par des interdomaines « incendie ». Une communication directe est à cet effet établie entre l'AS BMT et la LS SIG. La touche de commande d'urgence de l'UeLS-CH n'est pas transmise de manière redondante.

La redondance doit être conçue de sorte que toutes les données pertinentes pour le processus soient en permanence à jour et identiques sur les deux commandes (représentation du processus). L'état d'exploitation de l'AS est géré en parallèle et de manière équivalente sur les deux commandes. Le processus de récupération après une commutation de l'AS active à l'AS passive doit être possible sans perte de données et ne doit pas entraîner de « retour automatique ». Les interdomaines sont uniquement exécutés par l'AS active. Si un ou plusieurs interdomaines sont en attente après une commutation, l'interdomaine ayant la priorité la plus élevée est exécuté. Les exigences du réseau pour l'échange de données doivent pouvoir être satisfaites via le réseau IP existant ou le réseau IP EES.

La communication avec l'AR et les LS est garantie à tout moment, l'AR communiquant toujours via l'AS active. L'état de redondance de l'AS est communiqué à l'AR via des points de données (actif/passif, disponible). Une seule AS peut être active à la fois. Si les deux AS sont actives, l'AS effectivement active est déterminée via la surveillance service ou système AR-AS. Si les deux AS sont actives et que les deux surveillances système ou service sont disponibles, l'AS normalement indiquée comme active est utilisée pour la communication. La solution décrite est comparable à la redondance applicative dans l'AR.

Au niveau de l'installation, les solutions de haute disponibilité des commandes utilisées sont mises en œuvre. Grâce à l'utilisation des types de communication prédéfinis (voir chapitre 5.10), cela est possible sans conséquences supplémentaires.

4.3 Application de virtualisation

4.3.1 Autonomie et niveaux de repli

Afin d'assurer un fonctionnement 24 heures sur 24 et 7 jours sur 7, l'autonomie de chaque objet doit être prise en compte conformément au chapitre 5.8. Les systèmes (qu'ils soient physiques ou virtuels) doivent donc être installés à l'intérieur de la section IP (qui, selon la définition, peut inclure plusieurs sections EES, notamment dans le cas de « tronçons à ciel ouvert ». L'autonomie des différents niveaux doit être garantie. Aucune dépendance vis-à-vis de niveaux supérieurs n'est donc admise.

Les niveaux de repli en matière de commande et d'exploitation assurent la continuité de l'exploitation en cas de défaillances partielles (voir chapitre 5.6). Différents niveaux, qui s'étendent du niveau gestion à l'AR, sont à cet effet définis.

La question de l'autonomie liée aux installations et aux objets est abordée plus en détail dans le cadre des exigences fonctionnelles (voir chapitre 5).

4.3.2 Virtualisation des systèmes de gestion et de commande

L'utilisation de la virtualisation dépend du domaine d'application et de l'autorisation (validation) du fabricant, comme indiqué dans le tableau suivant :

Tableau 4 : Utilisation de la virtualisation dans les niveaux système de l'architecture

Partie de l'EES	Virtualisable	Remarque
UeLS-CH (BL)	Oui	Centralisé au niveau de gestion régional (dans les deux locaux techniques OT)
AR Host (matériel) / Plateforme de virtualisation	Non	Doit être situé dans la section IP
AR = fonction de serveur de gestion section - interface entre l'UeLS-CH (BL) et le serveur de gestion section (application virtuelle sur l'AR)	Oui	Doit être situé dans la section IP
AR MMI	Oui	Doit être situé dans la section IP
AS (API, y c. logiciel de processus)	Non	Doit être situé dans la section IP
AS (Guest-OS, p. ex. VMS)	Oui	Doit être situé dans la section IP
AS MMI	Oui	Doit être situé dans la section IP

4.3.3 Schéma de la virtualisation de l'AR (objectif)

Le schéma suivant présente l'objectif des systèmes AR selon deux approches différentes.

Première approche avec VM séparée pour AR et AR MMI :

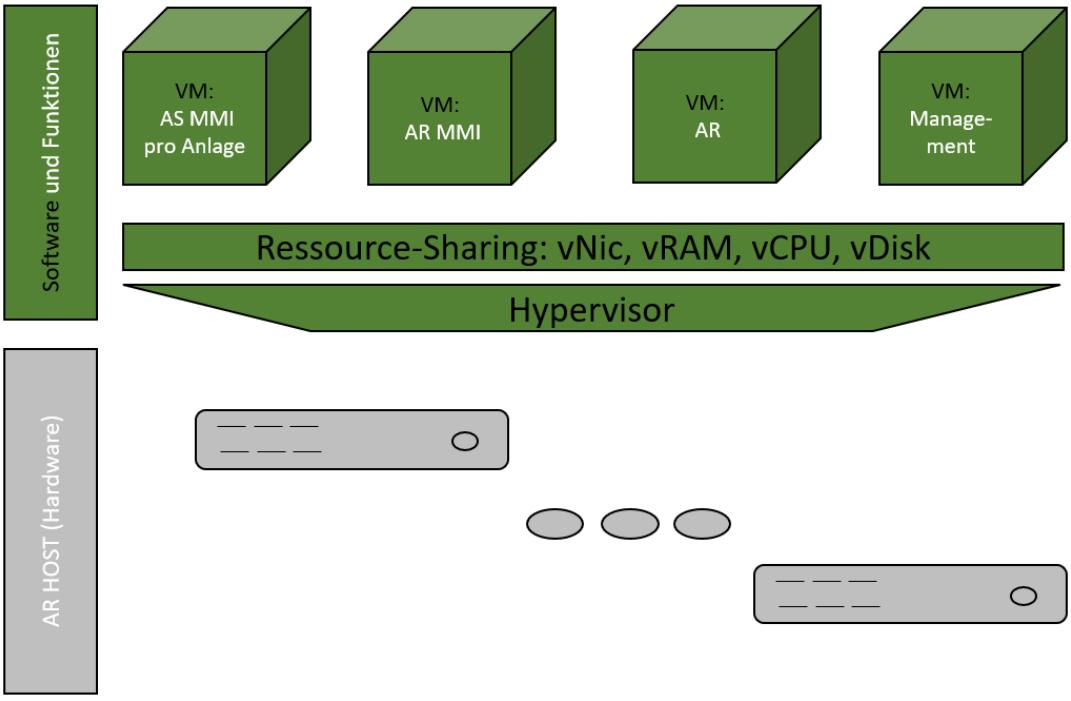


Figure 18 : Schéma de l'objectif de la virtualisation de l'AR - AR, AR MMI et AS MMI sur des VM distinctes

Deuxième approche avec VM commune pour AR et AR MMI :

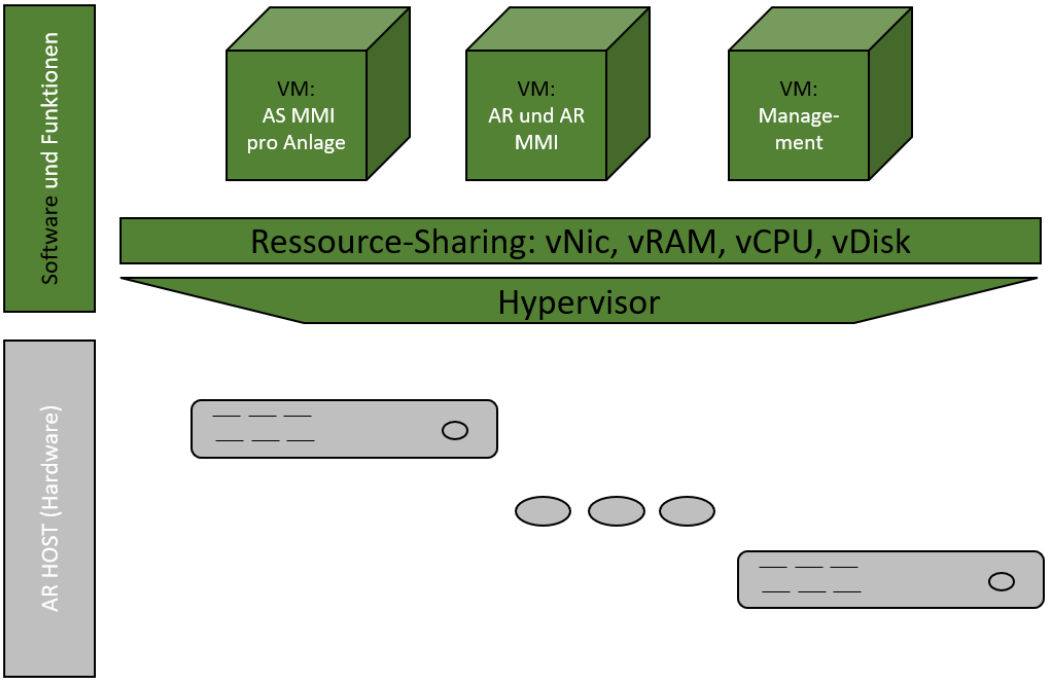


Figure 19 : Schéma de l'objectif de la virtualisation de l'AR - AR et AR MMI sur une VM commune

L'objectif peut être mis en œuvre via les 2 variantes suivantes.

Variante 1

Dans cette variante de mise en œuvre, la virtualisation ne peut pas être utilisée. Dans des cas exceptionnels, le matériel est utilisé selon sa fonction, p. ex. un serveur pour AR et AR-MMI et un serveur séparé pour AS et AS-MMI. Les accès sont toutefois possibles depuis des clients généraux (non liés à une fonction) :

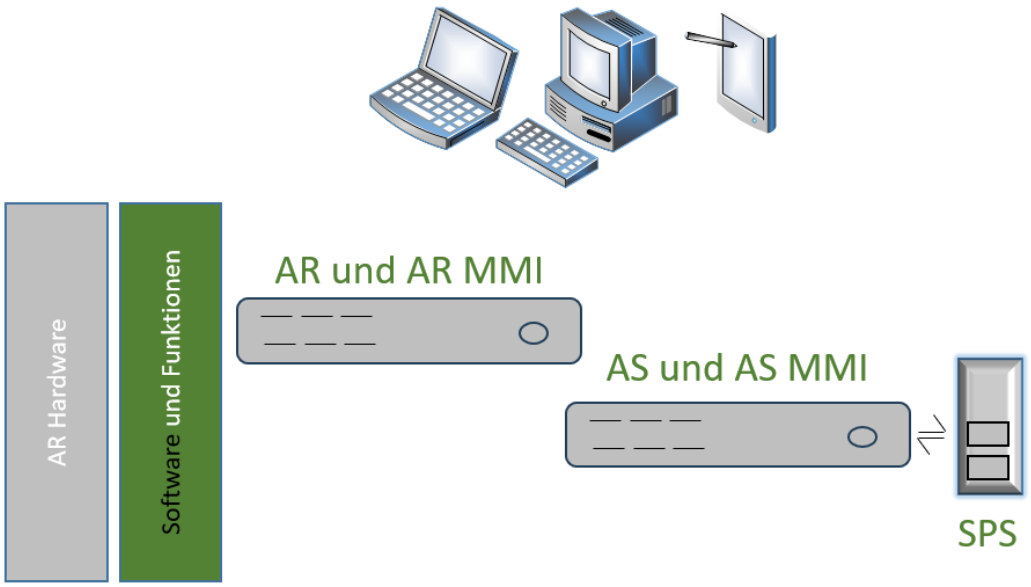


Figure 20 : Variante 1 - schéma de l'AR non virtualisé (dans des cas exceptionnels)

Variante 2

Dans cette variante de mise en œuvre, AR et AR-MMI sont implémentés séparément. Les accès AS-MMI sont par ailleurs réservés aux produits spécifiques au fabricant (ou certifiés).

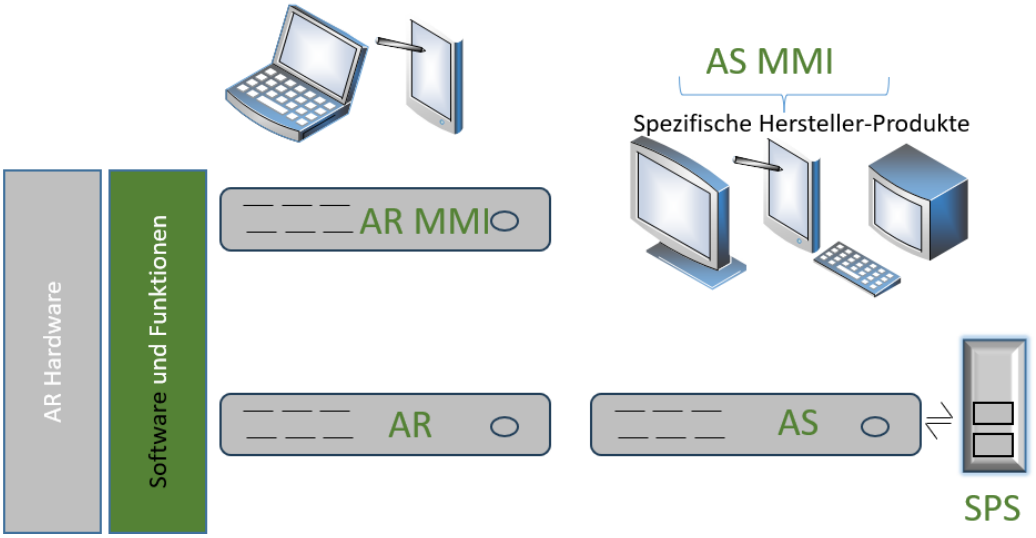


Figure 21 : Variante 2 - les éléments d'accès sont spécifiques au fabricant et liés à leur fonction

4.3.4 UeLS-CH (BL) dans le local technique OT

Les UeLS-CH (BL) sont installés dans les locaux techniques OT. Ces locaux techniques OT doivent être conçus de manière géoredondante, soit deux sites par UT, conformément à la directive 13009.

Les deux sites peuvent être exploités selon le concept actif-passif, actif-actif ou d'autres variantes spécifiques. Le principe est le suivant : en cas de défaillance d'un local technique OT, le deuxième doit prendre intégralement le relais, si possible sans interruption.

Pour une utilisation dans ce domaine, les infrastructures classiques de serveurs et de stockage ainsi que les infrastructures VSAN sont autorisées.

Les infrastructures hyperconvergées (HCI) dotées de commutateurs réseau intégrés ne sont pas autorisées car elles ne sont pas conformes aux exigences définies pour le matériel réseau. Si des variantes HCI sans commutateurs réseau intégrés venaient à être disponibles sur le marché, leur utilisation pourrait être soumise à l'approbation du CAB OT Security.

4.4 Structure de l'AR (exemple d'un serveur unique)

Le serveur de gestion section (AR) se compose des éléments suivants :

- Un AR HOST (l'ensemble du serveur) ;
- Au moins une machine virtuelle AR (VM AR) ;
- Des machines virtuelles optionnelles de type « application » (VM Management).

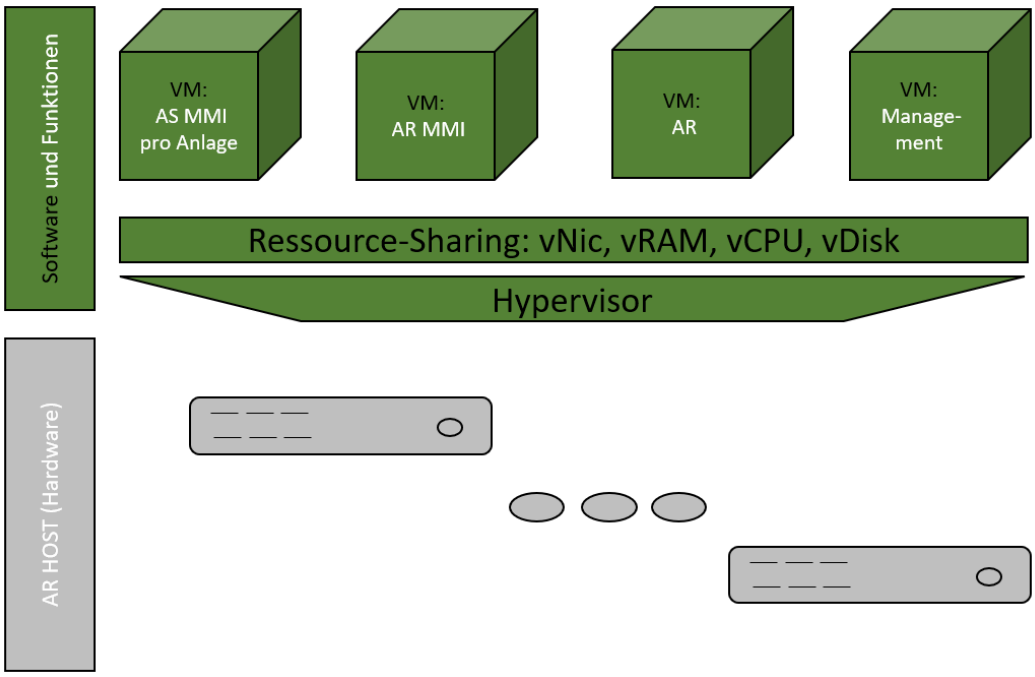


Figure 22 : Structure de base d'un AR Host : séparation des fonctions des VM - variante 1

Une VM AR contient le système d'exploitation, le logiciel applicatif et les moyens auxiliaires nécessaires, tels que OPC UA serveur/client, pilotes de communication etc., le logiciel système pour la sauvegarde/restauration, ainsi que d'autres auxiliaires (agent SNMP externe par ex.). Les moyens auxiliaires supplémentaires destinés à l'administration, la configuration ou la programmation des AS raccordées doivent être installés sur une ou plusieurs autres VM.

Une VM AP contient le système d'exploitation et d'autres logiciels optionnels, tels que le logiciel d'automatisation pour la conception, le logiciel de programmation des systèmes de commande (AS), le logiciel système pour la sauvegarde/restauration, la visualisation/commande de l'AS, un agent SNMP (Simple Network Management Protocol) externe, etc. En concertation avec les fabricants concernés, différents logiciels d'automatisation et diverses visualisations et commandes peuvent être installés. En cas d'impossibilité, une VM AP supplémentaire doit être utilisée (les conteneurs ne sont pas pris en charge).

Les combinaisons concernant une même installation sont autorisées, soit VM AR et AR MMI. Les AS MMI sur la même VM sont également autorisées (voir figure 23).

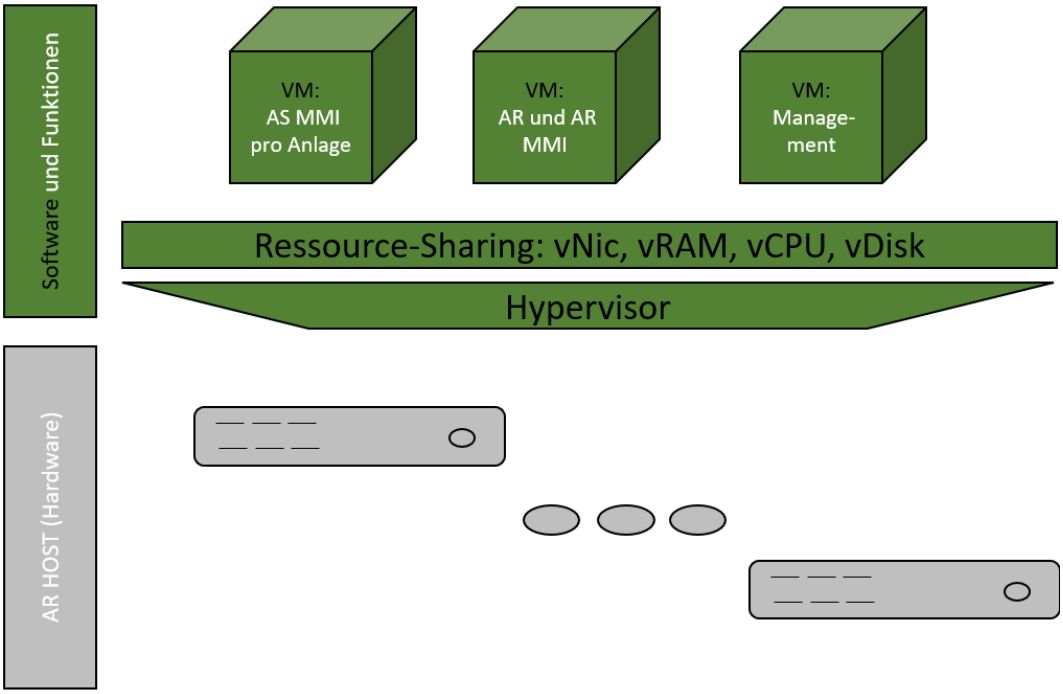


Figure 23 : Structure de base d'un AR Host : séparation des fonctions des VM - variante 2

4.4.1 Compatibilité des navigateurs web pour les GUI-MMI

La compatibilité des navigateurs web pour les GUI-MMI doit être mise en œuvre conformément à la documentation ASTRA 83050. Les GUI techniques standardisées spécifiques au fabricant, telles que NMS-GUI, constituent une exception.

4.5 Structure de l'AS

Une commande d'installation (AS) doit être prévue pour chaque objet (tunnel) et chaque installation (voir chapitre 3.6.2).

4.5.1 AS critiques pour la sécurité (y c. LS)

Les installations BMT et ventilation ainsi que le feu rouge au portail sont considérés comme critiques pour la sécurité.

Les exigences générales relatives aux AS mises en œuvre avec un API sont définies ci-après.

4.5.2 Exigences relatives aux AS (API)

Les composants utilisés doivent répondre à des critères spécifiques. Le respect des exigences suivantes est impératif.

- Système d'exploitation ou micrologiciel :
  - doit faire partie intégrante du matériel et être stocké dans une mémoire non volatile (persistante) ;
  - doit être embarqué et provenir du fabricant de SPS ;
  - doit garantir un comportement temporel (temps réel, temps de cycle, temps de traitement)
  - L'accès au système d'exploitation à des fins de mise à jour/niveau doit avoir lieu par le biais de programmes particuliers et respecter la protection définie (a minima utilisateur, mot de passe, et par la suite IAM EES). L'accès peut s'effectuer via le réseau (interface de gestion) ;

  - Le système d'exploitation ne doit pas être modifié pendant l'exploitation (un redémarrage rétablit automatiquement la dernière version opérationnelle du système).
- Le matériel :
  - doit pouvoir être monté sur un rail standardisé ou intégré dans une armoire 19" ;
  - présente une structure modulaire qui peut être étendue/modifiée de l'extérieur sans outil auxiliaire (p. ex. une carte enfichable dans un boîtier de PC n'est pas modulaire) ;
  - ne comporte pas de ventilateur ;
  - fonctionne sans pièce rotative (p. ex. disque dur). Le transfert de données non importantes pour l'exploitation sur des pièces rotatives, comme le disque dur, est permis ;
  - doit répondre aux déclarations et normes suivantes :
    - CE (marque de conformité) ;
    - SN EN 61000-6-4 (compatibilité électromagnétique CEM) ;
    - SN EN 61131-2 (exigence relative au matériel de contrôle) ;
    - SN EN 60068 (influences environnementales) ;
    - IEC 62443 (cybersécurité) ;
  - doit supporter une température de fonctionnement comprise entre - 20 °C et + 50 °C sans condensation ;
  - ne doit pas contenir de batteries tampon.
- Le logiciel :
  - est conçu conformément à SN EN 61131 ;
  - est programmé conformément à SN EN 61131 (liste exhaustive) :
    - Bloc fonctionnel (FBS) ;
    - Texte structuré (ST) ;
    - Schéma de contacts KoP) (uniquement avec justification suffisante) ;
    - Liste d'instructions (AWL) (uniquement avec justification suffisante).
- Données/informations :
  - Après une panne ou un redémarrage de la commande, l'« état sûr » prédéfini est appliqué pour chaque corps de métier.

Les commandes réalisées sur un système d'exploitation non embarqué (non-embedded) avec un temps de cycle fixe ne sont pas acceptées. Le « SoftPLC » en est un exemple courant, en sachant que le terme « SoftPLC » est défini de manière différente selon les manuels de référence. L'OFROU, considère le « SoftPLC » comme un programme autonome fonctionnant sur un système d'exploitation non compatible avec le temps réel, p. ex. dans un PC « classique », en tant que programme gérant différentes entrées et sorties.

Le « texte structuré » est privilégié comme langage de programmation (portabilité). Le logiciel doit par ailleurs être suffisamment documenté (en-tête, auteur, version, commentaires). Un concept de nommage est utilisé pour les différents éléments (p. ex. variables).

4.5.3 API

L'utilisation des automates programmables industriels (API) garantit une programmation simple, une mise en service rapide, un faible besoin de maintenance et une durée d'utilisation prolongée. Dans certains cas, il peut être judicieux d'examiner des unités de redondance des API modernes. En règle générale, l'AS n'est pas conçue de manière redondante (voir chapitre 4.2.3).

L'API en version matérielle est actuellement le composant fonctionnel privilégié en tant qu'AS.

4.5.4 API virtuels

Les API virtuels nécessitent un entretien logiciel supplémentaire (OS) ainsi qu'une protection contre les maliciels. Leur utilisation n'est par conséquent pas autorisée.

4.5.5 IPC

À ce niveau, les ordinateurs industriels (IPC) nécessitent un entretien logiciel supplémentaire, notamment pour le système d'exploitation (OS) et la sécurité contre les maliciels. Leur utilisation n'est par conséquent pas conseillée.

4.5.6 MMI (GUI)

L'API peut également être commandé à l'aide d'un écran dédié, d'un panneau de commande, ou via AS-MMI dans l'AR.

4.6 Structure de la LS

Les commandes locales (LS) doivent toujours respecter l'exigence de séparation par tube (voir chapitre 3.6.2).

4.6.1 Exigences relatives aux LS

Les exigences générales relatives aux LS mises en œuvre avec un API sont définies dans le chapitre 4.5.2.

4.7 Licences

Les licences doivent être établies au nom du propriétaire (OFROU) ou de l'exploitant. Toutes les licences, qu'elles soient sous forme papier ou électronique, doivent être remises aux personnes ou à la boîte mail de groupe désignées par la centrale/la filiale ou l'UT.

4.7.1 Licences sans lien avec le matériel

Les licences ne doivent pas être liées au matériel et doivent être transférables.

Si le fabricant ne peut pas satisfaire à cette exigence, il doit fournir à ses propres frais la licence pour le matériel de remplacement. Pour les API, cette garantie doit couvrir une période d'au moins 10 ans à compter de l'acquisition du matériel

4.8 Disponibilité des éléments

Lors de la conception de tous les niveaux d'architecture et de l'ensemble des installations, il convient de choisir l'une des technologies informatiques présentées au chapitre 4.1. Le niveau de disponibilité à atteindre pour la technologie informatique choisie dépend à la fois des besoins de disponibilité de l'objet (tunnel, tronçon à ciel ouvert) et des possibilités de l'organisation d'exploitation.

4.8.1 Heures de service

Les **heures de service** désignent la période pendant laquelle la prestation de service est convenue ou pendant laquelle l'installation est en fonctionnement. Le service ou l'installation est surveillé de manière proactive ou réactive. En cas de défaillance du service (défini comme interruption de service dans le tableau ci-dessous) pendant les heures de service ou de dysfonctionnement de l'installation, un ticket est ouvert dans le délai de réaction prévu dans le contrat, afin de pouvoir lancer sans délai la procédure de rétablissement du service.

Les heures de service pour l'ensemble des installations et des services des EES sont toujours 7x24h. Aucune heure de service alternative n'est définie !

Tableau 5 : Niveau de service heures de service

Niveau de service	Valeur	Méthode de mesure / remarques
Heures de service 7x24	7x24 (365 jours)	• Du lundi au dimanche, à 00h00 à 24h00, y compris jours fériés nationaux • Aucune interruption planifiée, à savoir aucune fenêtre de maintenance périodique avec interruption de service, mais des interventions de maintenance prévues et annoncées • Les maintenances et les changements impliquant une interruption de service se font seulement après entente • Les travaux impliquant une interruption de service sont autorisés dans le cadre d'une procédure spécifique impliquant les utilisateurs (min. 15 jours ouvrables à l'avance)

4.8.2 Heures d'assistance

Les heures d'assistance correspondent à la période durant laquelle un utilisateur bénéficie de prestations d'assistance (aide à l'utilisation d'un service) pour un service ou une installation. Les heures d'assistance peuvent différer des heures de service.

Les prestations administratives ne font pas partie des prestations d'assistance.

Tableau 6 : Heures d'assistance selon le niveau de service

Niveau de service	Valeur minimale	Méthode de mesure / remarques
Heures d'assistance 5x9	5x9h	• Du lundi au vendredi, de 08h00 à 17h00, hors jours fériés régionaux et nationaux
Heures d'assistance 7x24	7x24h	• 7 jours sur 7, 24 heures sur 24, y c. jours fériés

4.8.3 Disponibilité

La disponibilité décrit la manière dont la fonctionnalité exigée et convenue doit être assurée à un moment donné ou sur une période définie. La disponibilité est exclusivement définie par le **« downtime » (indisponibilité)**. Aucune indication alternative sous forme de taux de disponibilité calculé en pourcentage (p. ex. 99,99 %) n'est fournie.

Dans ce contexte, l'indisponibilité **(Downtime)** correspond à la somme de toutes les interruptions de service, exprimées en heures et en minutes, survenant au cours de la période de mesure définie et durant lesquelles un service ou une installation n'est pas disponible pendant les heures d'assistance convenues et, partant, où la fonctionnalité minimale n'est pas assurée. L'interruption de service commence dès la survenue d'une défaillance, c'est-à-dire lors de sa détection par le système de surveillance ou de la réception d'un message par un utilisateur, et se termine une fois le service rétabli ou la défaillance corrigée. En cas de surveillance réactive, le temps d'indisponibilité commence lorsque l'utilisateur signale la panne au centre de services (création du ticket).

Tableau 7 : Niveau de service mesuré en downtime

Niveau de service	Valeur	Méthode de mesure / remarques
Downtime 2h	<= 2h par an	• Ne peut être atteint que par des systèmes redondants • Mesuré par an et par système redondant • 1 défaillance totale max. admise par an • En cas de défaillances partielles, un basculement vers le système redondant est généralement effectué, entraînant une perte de redondance sans aucune interruption • Correction de la perte de redondance <24h
Downtime 8h	<= 8h par an	• Mesuré par an et par système • 1 défaillance max. admise par an
Downtime 12h	<= 12h par trimestre	• Mesuré par trimestre et par système • 1 défaillance max. admise par trimestre
Downtime Best Effort	Pas de prescription	• L'objectif est de corriger une défaillance dans les 24h

Une perte de redondance n'est pas considérée comme une interruption de service, mais doit être corrigée dans les 24 heures suivant sa constatation (ouverture d'un ticket).

Le tableau suivant fournit des valeurs pratiques servant de base au choix de la technologie informatique ainsi qu'à la définition des exigences techniques et d'exploitation des EES. Ces valeurs peuvent être utilisées comme référence pour les accords de niveau de service (SLA).

Tableau 8 : Disponibilité standard mesurée en downtime

Système / Installation	SLA	Disponibilité	Technologie / Architecture
Niveau gestion y compris FA	**Downtime 2h**	<= 2h par an, 1 défaillance max. admise par an, correction de la perte de redondance <24h	• Cluster HA (au moins 3 ordinateurs) • Redondance applicative supplémentaire répartie sur deux sites géoredondants
Connexion UT au réseau IP EES Backbone (routeur et pare-feu BB)	**Downtime 2h**	<= 2h par an, 1 défaillance max. admise par an, correction de la perte de redondance <24h	• Connexion géoredondante au réseau IP EES Backbone
Anneaux de raccordement du réseau IP EES, y c. services réseau de proximité (noyau)	**Downtime 2h**	<= 2h par an, 1 défaillance max. admise par an, correction de la perte de redondance <24h	• Par section, deux routeurs d'anneau de raccordement connectés à deux centrales ou locaux techniques distincts • Routage géoredondant des anneaux de raccordement • Services réseau de proximité déployés de manière géoredondante dans les deux OTTR
rVL, VL, autres éléments suprarégionaux (temporairement, période transitoire)	**Downtime 8h**	<= 8h par an, 1 défaillance max. admise par an	• API ou équipement à 2 serveurs, Failover Cluster

Tableau 8 : Disponibilité standard mesurée en downtime

Système / Installation	SLA	Disponibilité	Technologie / Architecture
UeLS-CH	**Downtime 2h**	<= 2h par an, 1 défaillance max. admise par an, correction de la perte de redondance <24h	• Cluster HA (au moins 3 ordinateurs par site) • Redondance applicative supplémentaire répartie sur deux locaux techniques OT
Serveur de gestion section (hôte)	**Downtime 2h**	<= 2h par an, 1 défaillance max. admise par an, correction de la perte de redondance <24h	• Cluster HA (au moins 2 serveurs par site) • Redondance applicative supplémentaire répartie sur deux centrales techniques
Commande d'installation (systèmes non critiques pour la sécurité)	**Downtime 8h**	<= 8h par an, 1 défaillance max. admise par an	• API
Commande d'installation (systèmes critiques pour la sécurité)	**Downtime 2h**	<= 2h par an, 1 défaillance max. admise par an, correction de la perte de redondance <24h	• API redondant
Commande locale (systèmes non critiques pour la sécurité)	**Downtime 8h**	<= 8h par an, 1 défaillance max. admise par an	• API
Commande locale (systèmes critiques pour la sécurité)	**Downtime 2h**	<= 2h par an, 1 défaillance max. admise par an, correction de la perte de redondance <24h	• API redondant (cf. variantes BMT)

4.9 Application des technologies spécifiques aux installations

Au niveau du local technique OT, il est possible de centraliser les fonctions présentant une importance régionale et donc étendue (GUI/MMI ou outils, services métier et applications métier) :

Applications et outils :

- UeLS-CH ;
- Services de sous-domaines ;
- (i)AM EES ;
- DD(I) ;
- Accès à distance / maintenance ;
- Outils techniques d'exploitation (NMS, etc.) ;
- Autres systèmes (système de tickets, etc.) ;
- GFS ;
- VIS (temporairement, période transitoire) ;
- rVDE (temporairement, période transitoire) ;
- rVL (temporairement, période transitoire) ;
- VR (temporairement, période transitoire).

Les parties d'installation suivantes et leurs fonctions partielles font également partie de cette catégorie :

Tableau 9 : Parties d'installation et leurs fonctions partielles

Dés. AKS	Désignation de l'installation / partie d'installation	Fonctions explicites
ZES	Système de gestion – signalisation	VL-CH
VMS	Installation vidéo	Fonctions régionales
FE	Système de radiocommunication (radio, intercalation, Polycom)	Intercalation
NT	Téléphone de secours	
TTZ	Porte / porte carrossable / contrôle d'accès	Autorisation de programmation électronique des clés

Si cela est pertinent, la gestion (et uniquement celle-ci) de certaines installations et parties d'installation peut être centralisée au niveau régional. La confirmation préalable du fabricant est toutefois nécessaire.

4.9.1 Utilisation des fonctions de disponibilité dans le local technique OT

À ce niveau, les fonctions Fault Tolerance ou High Availability des VM (Guest OS) intégrées la plateforme de virtualisation, ainsi que les fonctions de redondance décrites au chapitre 4.2, sont autorisées.

Les MMI ou outils suivants des installations/parties d'installation sont virtualisables jusqu'au niveau de la fonction AR (mais pas au niveau AS ou LS).

Tableau 10 : Vue d'ensemble de la virtualisation de l'installation partielle

Dés. AKS	Désignation de l'installation / partie d'installation	Fonctions explicites
NST	Alimentation sans coupure	
ZEB	Système de gestion – éclairage	
DB	Éclairage de traversée	
BN	Éclairage de secours en cas d'incendie	
FWB	Éclairage du chemin de fuite	
ZEL	Système de gestion – ventilation	
AL	Air vicié	
LL	Ventilation longitudinale	
ZL	Apport d'air frais	
FWL	Ventilation du chemin de fuite	
ZES	Système de gestion – signalisation	Tunnel AS
VM	Signalisation dynamique	
LSA	Installation de signalisation lumineuse	
SER	Signalisation des dispositifs de sécurité	
BMT	Installation de détection incendie tunnel	
VTV / VMS	Installation vidéo	• Cas exceptionnels dans l'objet pour la détection automatique d'incidents (ED) • Enregistrement d'images (mémoire circulaire)

Tableau 10 : Vue d'ensemble de la virtualisation de l'installation partielle

Dés. AKS	Désignation de l'installation / partie d'installation	Fonctions explicites
IPE	Réseau de communication Réseau IP Anneau de raccordement	
IPA	Réseau de communication Réseau IP Niveau d'accès	
LTA	Système de gestion section	
FE	Système de radiocommunication (radio, interphonie, Polycom)	Radio et Polycom
NT	Téléphone de secours	Extincteur/armoire d'alarme dans l'installation divers et déclenchement d'un interdomaine
HI	Installation électrique intérieure	
HLK	Chauffage, ventilation, climatisation	
BMG	Installation de détection incendie bâtiment	
POR	Système de pompage	
LOE	Système de défense incendie	
WV	Alimentation en eau	
SAA	Installation d'évacuation et de traitement des eaux de chaussée	

4.9.2 Utilisation des fonctions de disponibilité AR

À ce niveau, les fonctions Fault Tolerance ou High Availability des VM (Guest OS) intégrées à la plateforme de virtualisation ainsi que les fonctions de redondance (cf. chapitre 4.3) sont autorisées.

4.9.3 Utilisation des fonctions de disponibilité AS/LS

Des systèmes hot-standby et cold-standby doivent être mis en place pour garantir les redondances requises.

4.10 Consolidation des différentes fonctions de l'installation sur la plateforme de virtualisation

Dans le local technique OT ou les centrales techniques, les ressources disponibles sont exploitées de manière optimale et la disponibilité est renforcée. Il convient à cet égard de tenir compte du dimensionnement approprié indiqué dans l'annexe V.3 Matériel informatique et de stockage des données.

Le schéma suivant illustre la consolidation dans un objet :

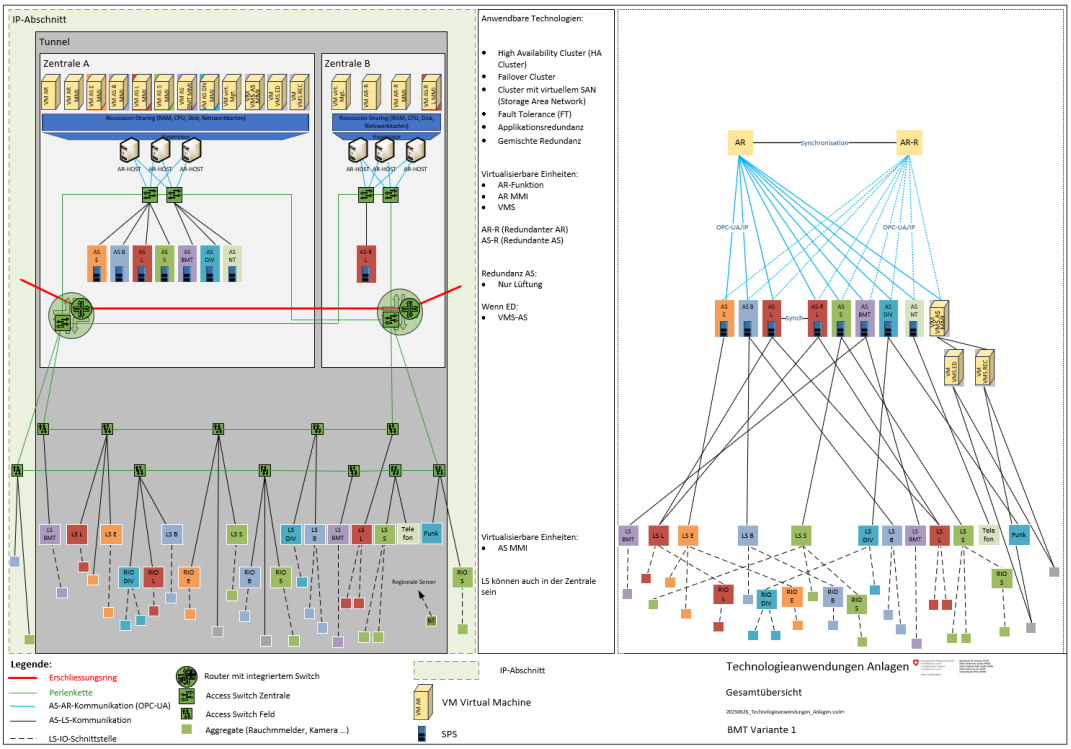


Figure 24 : Schéma de l'application de la technologie (un tube)

Les couleurs utilisées dans le schéma représentent l'installation dans son ensemble (et non les entreprises).

Les schémas illustrant l'application de la technologie pour un ou deux tubes sont disponibles dans les annexes V.1 et V.2. Ces deux variantes sont également présentées de manière spécifique à l'installation.

4.10.1 Local technique OT (deux sites par UT dans une ou deux sections IP dédiées)

Dans cette partie, la densité maximale de consolidation est requise (c'est-à-dire que tous les systèmes virtuels doivent être installés sur le même hôte).

4.10.2 Locaux techniques (deux sites à l'intérieur de la section IP)

Dans les locaux techniques, la consolidation est effectuée conformément au chapitre 4.9 Application des technologies spécifiques aux installations. Tous les éléments pouvant être virtualisés conformément au présent chapitre sont installés sur la même plateforme de virtualisation (voir chapitre 4.2.1), composée de plusieurs ensembles de matériel informatique.

Si, pour des raisons justifiées, un corps de métier souhaite/doit utiliser des serveurs séparés malgré l'autorisation de virtualisation, cette demande est étudiée/approuvée par l'I-FU. Des systèmes hot-standby et cold-standby doivent être mis en place pour garantir les redondances requises (si ces systèmes ne sont pas virtualisés ; dans le cas contraire, les prescriptions des chapitres 4.2 et 4.3) s'appliquent.

4.10.2.1 Autonomie liée à l'objet

Afin de garantir une disponibilité d'exploitation maximale, les installations critiques pour la sécurité et l'exploitation sont présentées dans différents scénarios d'exploitation au chapitre 5.6. Ce chapitre explique de quelle manière les principes régissant les scénarios d'exploitation sont définis. L'exploitation doit être garantie à tout moment. Aussi convient-il de mettre en place plusieurs niveaux de repli, même si toutes les fonctions ne sont pas disponibles à chaque niveau.

Les installations critiques pour la sécurité et l'exploitation doivent être disponibles, y compris la capacité de gestion/commande dans l'objet concerné (le cas échéant, il peut s'agir d'une commande manuelle sur site). Par conséquent, ces unités ne peuvent pas être centralisées au niveau régional, car la capacité d'exploitation serait compromise en cas de défaillance du niveau de gestion régional ou de défaillance partielle du réseau IP EES entre l'objet et les locaux techniques OT. Dans un tel cas, le déclenchement de l'alerte ne serait plus garanti, ce qui nécessiterait une intervention sur site dans le tunnel, impossible à gérer.

4.10.2.2 Exigences relatives aux délais de rétablissement

La documentation ASTRA 86053 définit les délais de rétablissement, tout en précisant qu'il s'agit d'un délai maximal et qu'il convient de viser une remise en service plus rapide. Sur la base des exigences minimales, les unités territoriales déterminent les stocks de pièces de rechange qui sont nécessaires et doivent être disponibles.

La disponibilité de l'architecture du système doit être choisie en fonction des exigences minimales propres à chaque corps de métier. Pour les éléments qui peuvent être consolidés selon 4.9, l'OTTR ou l'hôte AR doit être dimensionné en fonction de l'exigence la plus stricte.

4.10.3 Exigences relatives à la garantie de maintenance et d'assistance (SLA)

Afin de respecter les niveaux de disponibilité définis, des accords de niveau de service (SLA), incluant les aspects liés à la réassurance tels que la maintenance par le fabricant et les contrats d'assistance des partenaires d'intégration, doivent être conclus dans le cadre de la réalisation des objectifs par les instances responsables (selon le domaine concerné : centrale, filiale ou UT).

4.11 Conservation des données

En règle générale, les données brutes sont conservées pendant les périodes légalement définies. Étant donné qu'à l'exception de l'IAM EES (partie Identity), aucune donnée personnelle n'est traitée et aucun enregistrement n'est effectué dans le système de gestion des affaires (GEVER), la procédure est définie comme suit :

Seules les données brutes (structurées ou non) sont conservées à long terme. Les données déjà traitées au niveau du capteur /de l'actionneur dans le cadre du processus font exception.

Les données brutes traitées ultérieurement, par exemple à des fins d'enrichissement ou d'agrégation, ne sont pas sauvegardées car elles sont reproductibles. Cette règle ne s'applique pas aux sauvegardes dans le format final de publication ; celles-ci sont toutefois généralement effectuées en dehors de l'OT, dans l'infrastructure IT.

Le tableau suivant indique les durées de conservation minimales et/ou maximales des « données non personnelles » :

Tableau 11 : Cycle de vie des « données non personnelles »

Niveau données	Données brutes/bases de données	Fichiers journaux
Réseau IP EES Systèmes de la Confédération Systèmes tiers	Aucune	>= 12 mois < 24 mois
Niveau de gestion régional Services de base / services centraux Niveau gestion Niveau gestion du trafic Région de gestion du trafic	*Sauvegarde quotidienne : >= 7 jours *Sauvegarde hebdomadaire : >= 4 semaines *Sauvegarde mensuelle : >= 3 mois *Sauvegarde annuelle : en fonction des besoins Informations des installations VM : 10 ans	>= 12 mois < 24 mois

*Selon le logiciel de sauvegarde utilisé, différents types et mécanismes de sauvegarde sont mis en œuvre. Ce tableau est fourni à titre indicatif et doit être appliqué conformément au chapitre 4.12.5.

Des délais de conservation plus longs spécifiques à certaines applications métier peuvent être définis au niveau gestion. Le fournisseur de l'application métier est alors tenu de les garantir.

En cas d'incident, les données concernées sont copiées dans un espace de stockage distinct, conformément aux instructions.

Des dispositions spécifiques, conformes aux prescriptions des corps de métier, s'appliquent pour les systèmes EES (LS, AS et AR).

4.11.1 Droit de propriété et d'utilisation

L'Office fédéral des routes (OFROU) détient la souveraineté sur l'ensemble des données.

L'Office fédéral des routes (OFROU) dispose des droits d'utilisation illimités sur l'ensemble des données.

L'utilisation des données par le fournisseur doit être divulguée. La transmission des données à des tiers est interdite.

4.11.2 Logiciels et programmes d'application

Les CG[1] de la Confédération s'appliquent pour l'ensemble du cycle de vie des logiciels et programmes d'application.

4.12 Traçabilité

Des recherches et des audits sur les systèmes et les événements, notamment concernant les opérations de commande et les messages générés automatiquement par les installations, doivent pouvoir être menés à tout moment. La traçabilité est abordée en détail dans la directive ASTRA 13030. Les données et informations sont classées selon différents niveaux. Les détails figurent dans la documentation ASTRA 83042.

4.12.1 Journalisation

Un système de journalisation central doit être mis en place dans chacun des réseaux partiels (réseau IP EES BD, WMZ et toutes les UT). La liste ci-dessous indique les données et informations qui doivent être conservées pour des raisons de sécurité et de traçabilité. Au sein des EES (AR à LS), la réglementation doit être effectuée à ce niveau.

4.12.1.1 Événements techniques

Enregistrement de tous les événements techniques, tels que les journaux système, qui ont été générés en fonction des événements.

4.12.1.2 Fichiers journaux

Les fichiers journaux doivent être en lecture seule (écriture protégée), mais sans exigences de traçabilité).

4.12.2 Journalisation du système

Chaque système doit disposer d'une journalisation complète dans son périmètre.

4.12.3 Hiérarchie et agrégation des données

La pyramide des données est présentée dans la directive ASTRA 13032. Celle-ci illustre la rationalisation des informations du niveau terrain jusqu'au niveau de gestion régional.

[1] Lien vers les CG : CG de la Confédération (admin.ch)

Seules les données pertinentes pour le niveau supérieur sont transmises. Le principe de réduction de la communication des données s'applique donc de l'agrégat au niveau gestion. Les agrégations spécifiques à un domaine sont traitées dans les services métier ou les applications métier, à l'exception de certaines AS qui prennent directement en charge cette fonction.

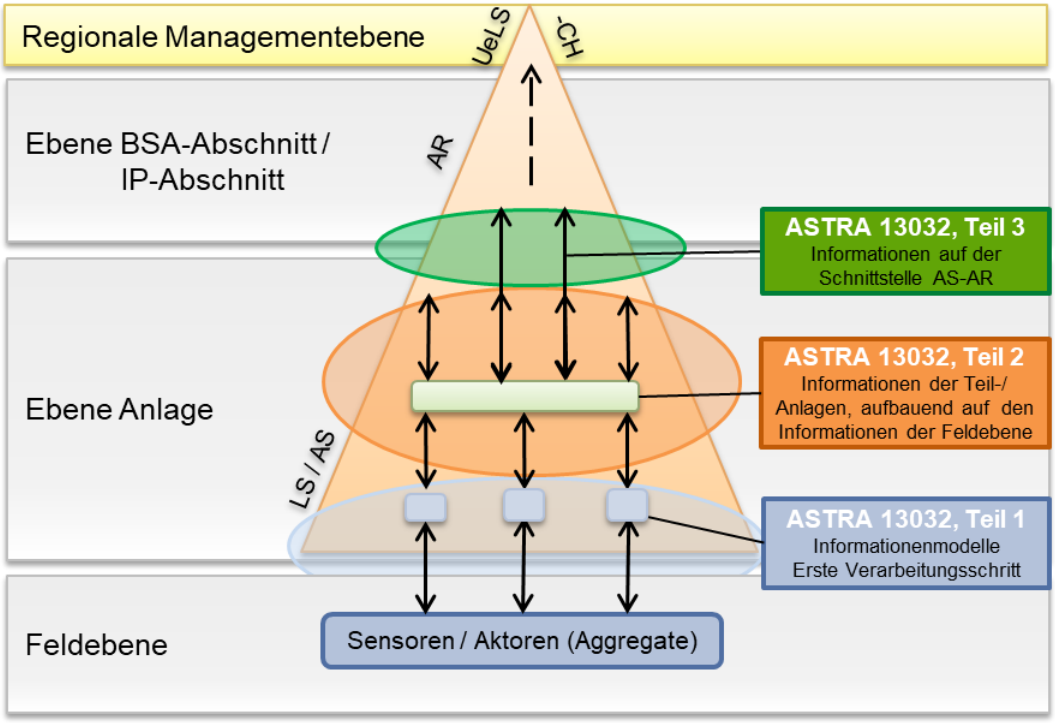


Figure 25 : Pyramide des données

4.12.4 Archivage

L'archivage désigne la conservation à long terme, systématique et contrôlée des données sous forme électronique. On distingue alors :

- l'archivage non conforme aux exigences de traçabilité (sauvegarde à long terme) et ;
- l'archivage conforme aux exigences de traçabilité.

Dans le domaine des EES, un archivage conforme aux exigences de traçabilité n'est généralement pas requis. S'il s'avère toutefois nécessaire d'archiver certaines données conformément aux exigences de traçabilité, par exemple en cas de litiges, cette procédure est effectuée via GEVER. Aucun autre archivage conforme aux exigences de traçabilité n'est géré dans le domaine des EES.

- Sauvegarde à long terme :

  Pour la conservation à long terme (archivage non conforme aux exigences de traçabilité), les directives du tableau mentionné au chap. 4.11 s'appliquent. Le traitement des données personnelles est régi par la loi fédérale sur la protection des données (LPD). Les données doivent être supprimées à l'issue du délai d'archivage.

4.12.5 Sauvegarde et restauration

Les prescriptions de la directive ASTRA 13030, GS-7 et GS-8, s'appliquent. Remarques complémentaires :

- Les solutions déployées pour la sauvegarde et la restauration doivent offrir des fonctionnalités très étendues pour les sauvegardes à la fois physiques et virtuelles dans différents environnements. La sauvegarde d'anciens et de nouveaux systèmes doit être

possible, même s'ils sont séparés de plus 3 générations. La prise en charge de plusieurs systèmes d'exploitation et de bases de données variées doit être assurée ;
- Un concept de sauvegarde et de restauration clairement défini doit être élaboré par l'UT et mis en œuvre après validation par le soutien technique du réseau IP EES. Les exigences minimales mentionnées au chapitre 4.11 doivent être satisfaites ;
- Un produit acheté de manière centralisée est disponible si nécessaire. Des exemples de concepts peuvent également être demandés ;
- Supports de sauvegarde autorisés : Backup2Disk (l'espace de stockage doit être séparé de l'espace de stockage normal et pouvoir être mise hors ligne), p. ex. un NAS ;
- Supports de sauvegarde non autorisés : disques durs externes, clés USG, DVD, etc.

4.13 Synchronisation horaire

La documentation ASTRA 83044 « Distribution de temps et d'horloge dans le réseau IP EES » décrit en détail comment le temps système de tous les composants est garanti sur la base du temps atomique unifié, afin d'assurer à tout moment l'intégrité des données en matière d'horodatage.

4.14 Reporting

Sur la base des informations/données brutes, des traitements ultérieurs sont effectués à des fins diverses. Différentes formes de reporting sont utilisées pour effectuer des agrégations ou des enrichissements d'informations (p. ex. à partir d'autres systèmes). Certains systèmes disposent de leurs propres fonctions de reporting, qui peuvent être utilisées. Ce service peut être mis en place pour réaliser des analyses approfondies ou si aucune fonction de reporting n'est disponible (voir chapitre 5.5).

Aucune donnée brute ou donnée permettant de retrouver une identité n'est transférée en dehors du réseau IP EES (protection des données).

4.15 OT Security

4.15.1 Instructions 73006

Les instructions ASTRA 73006 couvrent le cadre réglementaire de la technique de pilotage et de commande des EES (systèmes OT). et contiennent ce qui suit :

- Objectifs de l'OT Security Governance (voir chap. 4.1) ;
- Différents éléments constitutifs permettant de soutenir les niveaux stratégique, fonctionnel et opérationnel ;
- Règles : processus, rôles et organisation ;
- Personnes : qualification et formation des collaborateurs ;
- Technologie : prescriptions techniques ;
- Différentiation entre IT et OT sur les routes nationales (voir chap. 3.1) ;
- Principaux organes de l'organisation de sécurité OT (voir chap. 5.4).

4.15.2 Directive 13030

La directive ASTRA 13030 définit les exigences et mesures de protection des éléments des équipements d'exploitation et de sécurité (ESS) au moyen des technologies OT, afin de garantir un niveau de sécurité suffisant.

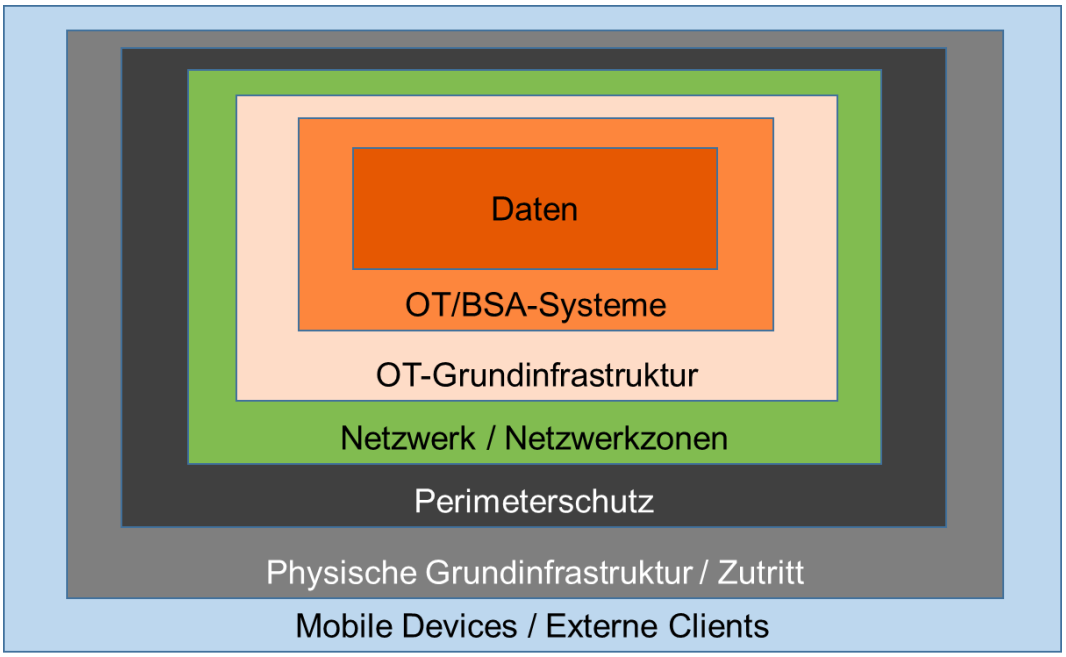


Figure 26 : Principe des exigences et mesures de sécurité à plusieurs couches – Principe de défense en profondeur « Defense in Depth »

4.15.3 Documentation 83042

La documentation ASTRA 83042 constitue la base de la sécurité du réseau. À cet effet, elle établit des normes et recouvre les aspects suivants :

- elle définit des notions communes ;
- elle définit le modèle de zones et fixe les exigences minimales applicables aux zones du réseau ainsi qu'à leur exploitation ;
- elle fixe les exigences minimales applicables aux passerelles réseau entre les zones au sein d'une unité territoriale (réseau IP EES UT), ainsi qu'entre les zones de transition vers d'autres unités territoriales, la VMZ-CH, les services de base, les centres de calcul EES ou des réseaux externes ;
- elle fixe les exigences minimales applicables aux systèmes qui peuvent être connectés au réseau.

4.15.4 Documentation 83056

La documentation ASTRA 83056 décrit les exigences spécifiques relatives à la gestion des identités et des accès, y compris les portails d'accès, dans le périmètre d'influence du domaine des routes nationales.

4.15.5 Manuel technique 23001-11880 Sécurité physique des systèmes OT et directive 13009

La fiche technique 23001-11880 relative à la sécurité physique des systèmes OT présente les mesures de protection de l'infrastructure comprenant les équipements de communication OT de l'OFROU (locaux techniques OT, locaux techniques destinés à l'exploitation de l'infrastructure OT, armoires normalisées, coffrets, boîtes de jonction et boîtiers de raccordement).

Cette « fiche technique » (TM) décrit les types de locaux et les exigences minimales requises pour la protection physique de l'infrastructure OT. Ces exigences sont intégrées dans la directive 13009 et la TM sera supprimée.

5 Exigences fonctionnelles

Le chapitre suivant décrit les exigences fonctionnelles relatives à la SA-CH.

5.1 Accès

5.1.1 Groupes d'utilisateurs

Les groupes d'utilisateurs comprennent les collaborateurs des unités territoriales, les collaborateurs externes ainsi que les collaborateurs des services fédéraux, y compris le personnel de l'OFROU. Les exigences sont fixées par l'IAM EES.

5.1.2 Rôles des utilisateurs

Les rôles des utilisateurs et leur concept d'autorisation sont décrits dans les instructions ASTRA 73002. Il existe à la fois des rôles généraux et des rôles détaillés, qui sont définis dans la documentation ASTRA 83056.

5.2 Interfaces utilisateurs

5.2.1 Principe de visualisation

La visualisation de l'**UeLS-CH** via l'interface MMI doit toujours s'effectuer sur le serveur UeLS-CH.

L'interface MMI d'une section EES se trouve sur le **serveur de gestion section (AR)**. Les images pertinentes des installations sont ainsi générées et enregistrées sur l'AR dans leur représentation détaillée.

L'un des trois principes ci-après doit être choisi pour la visualisation de la **commande d'installation (AS)**. Le choix se fait en fonction du projet, de la faisabilité technique ainsi que des exigences de disponibilité et d'autonomie définies dans la présente directive :

Tableau 12 : Principes de visualisation

Principe 1	La MMI et le serveur (SPS) sont séparés l'un de l'autre. Un SPS est utilisé pour l'AS. La MMI est visualisée en tant que VM sur l'AR hôte. Plusieurs MMI peuvent ainsi être exécutées simultanément en tant que VM sur un même ensemble matériel (hôte AR). En cas de panne de l'hôte AR sans redondance, le fonctionnement de l'AS via la MMI de l'AS n'est cependant plus garanti. Le cas échéant, les processus de l'AS continuent toutefois de fonctionner.
Principe 2	La MMI et le serveur (SPS) sont séparés l'un de l'autre. Des SPS sont utilisés pour l'AS. La MMI de l'AS fait partie de la MMI de l'AR. En cas de panne de l'hôte AR sans redondance, le fonctionnement de l'AS via la MMI de l'AR/AS n'est plus garanti. Le cas échéant, les processus de l'AS continuent toutefois de fonctionner.
Principe 3	L'AS est un SPS (selon 4.5.5) ou est installée sur un ordinateur séparé. La MMI de l'AS et les processus ne se trouvent pas sur le même matériel. En cas de panne de l'hôte AR sans redondance, l'AS et sa commande peuvent continuer à fonctionner.

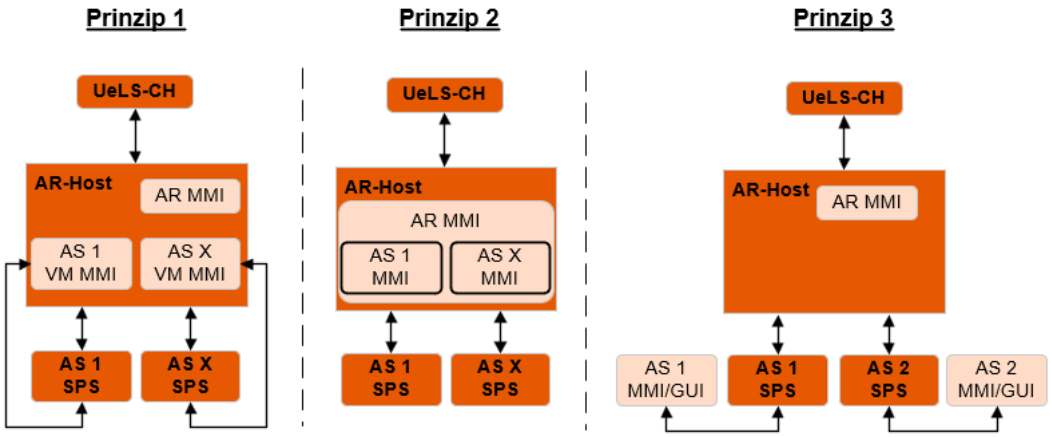


Figure 27 : Principes de visualisation

5.2.2 Possibilités de commande

Le tableau suivant présente les possibilités de commande autorisées. Il convient de faire la distinction entre les possibilités de commande dans l'UeLS-CH/serveur de gestion générale (BL) et sur site (locaux techniques/centrales techniques). Les conditions d'accès définies dans la directive ASTRA 13030 doivent par ailleurs être remplies.

Tableau 13 : Possibilités de commande

Niveau :	Groupe d'éléments	Élément ou composant	Possibilités de commande :	
			UeLS-CH	**Sur site**
Niveau applications	Applications métier (FA VM/BM)		Selon l'application	n/d
Niveau des services métier	Service métier		Selon l'application	n/d
Gestion OT	Services de gestion OT		Selon l'application	n/d
Services OT	Services OT		Selon l'application	n/d
Niveau gestion du trafic (VMZ-CH)	Systèmes	VMS	Selon l'application Poste de travail	n/d
Zones de transport		rVL ou VL	Accès web / Application client Poste de travail	• Postes de travail des opérateurs
Niveau de gestion régional	Systèmes	UeLS-CH et VMS-B	MMI / GUI (voir 5.2.3)	• Accès web
Section EES	Systèmes	AR	MMI (interface web)	• Accès web • Appareil connu du réseau • Possibilité de définir le mode d'exploitation et de commande • Accès d'urgence via un jumphost
	Systèmes	AS (SPS)	MMI (interface web)	• Appareil connu du réseau • Possibilité de définir le mode d'exploitation et de commande • Accès d'urgence via un jumphost • Pas de panneaux de commande, si nécessaire, ceux-ci doivent être définis dans le cadre du projet (PI / Pdét)
	Systèmes, actionneurs / capteurs	LS (SPS)	Le cas échéant, MMI (interface web)	• Appareil connu du réseau • Possibilité de définir le mode d'exploitation et de commande • Le cas échéant, accès d'urgence via un jumphost • Pas de panneaux de commande, si nécessaire, ceux-ci doivent être définis dans le cadre du projet (PI / Pdét)

5.2.3 Interfaces utilisateur

Les interfaces utilisateur des applications métier doivent être conçues conformément aux guides de style des documentations ASTRA 83050 à 83052 ainsi qu'à la directive ASTRA 73002. Elles sont appelées MMI.

Pour les composants et outils standard (NMS p. ex.) principalement utilisés par les administrateurs et non par les opérateurs, une dérogation au guide de style est possible. Ils sont appelés GUI.

La mise en œuvre et l'utilisation des MMI et GUI sont présentées en annexe I.2.

5.3 Commande

5.3.1 Modes d'exploitation

Les modes d'exploitation régissent les actions des utilisateurs et l'échange de données entre les différents niveaux de l'architecture du système : niveau de gestion régional, région, section, installation et niveau terrain.

Le choix du mode d'exploitation s'effectue depuis la MMI. Le mode d'exploitation peut uniquement être modifié dans la MMI correspondante (p. ex.: AS locale = changement dans l'AS-MMI). Le moyen utilisé pour accéder à la MMI correspondante (p. ex. via un navigateur) n'a pas d'incidence sur le mode d'exploitation.

Remarque : les autorisations de base des utilisateurs ne sont pas définies dans les modes d'exploitation, mais dans la gestion des utilisateurs ou dans la prise de main. Seuls les utilisateurs autorisés peuvent modifier les modes d'exploitation.

Pour les installations EES, on distingue les modes d'exploitation suivants :

Tableau 14 : Modes d'exploitation

Distant	En mode d'exploitation « distant », les données d'exploitation actuelles sont transmises au niveau immédiatement supérieur, et tous les ordres provenant de ce niveau sont acceptés.
Local	En mode d'exploitation « local », les données d'exploitation actuelles sont transmises au niveau immédiatement supérieur, mais aucun ordre émis par des utilisateurs de ce niveau n'est accepté. Les ordres et consignes du processus de commande du niveau immédiatement supérieur sont toutefois pris en compte. Tous les interdomaines sont émis ou reçus et les réactions correspondantes sont déclenchées.
Maintenance	En mode d'exploitation « maintenance », aucune donnée d'exploitation actuelle n'est transmise au niveau immédiatement supérieur, et aucun ordre n'est reçu de ce dernier. Tous les composants en mode d'exploitation « maintenance » sont isolés du processus de l'installation. Aucun interdomaine n'est émis ou reçu. Les réactions correspondantes ne sont pas déclenchées.

Le tableau ci-dessous définit quels modes d'exploitation doivent être mis en œuvre à chaque niveau ainsi que les exigences spécifiques à chaque niveau.

Tableau 15 : Modes d'exploitation spécifiques à chaque niveau

Systèmes et agrégats	Modes d'exploitation		
	Distant	**Local**	**Maintenance**
UeLS-CH	Dans l'environnement EES, les modes d'exploitation régissent les relations avec le niveau immédiatement supérieur. Les UsLS-CH représentent le niveau hiérarchique le plus élevé de l'architecture EES. Il n'existe donc aucun niveau supérieur pour ces systèmes ; par conséquent, les UeLS-CH ne disposent pas de modes d'exploitation au sens de cette définition.		
AR	✓	✓	
	Pour l'AR, le mode d'exploitation « Maintenance » n'est pas pertinent sur le plan fonctionnel. Il n'existe donc pas. La mise en œuvre fonctionnelle des modes d'exploitation « Distant » et « Local » est définie conformément au tableau 13.		
AS/LS	✓	✓	✓
	Trois modes d'exploitation peuvent être pertinents pour l'AS / la LS. La mise en œuvre fonctionnelle des modes d'exploitation est définie conformément au tableau 13. Les verrouillages servent à protéger les personnes, les biens et l'environnement. Ils doivent être mis en place en fonction des spécificités de chaque projet.		
Champ (Actionneurs, capteurs)	Aucune distinction entre les modes d'exploitation n'est effectuée. Les actionneurs et les capteurs commandables peuvent être actionnés via une possibilité d'intervention d'urgence. Cette possibilité permet une commande manuelle directe des actionneurs individuels ou des groupes d'actionneurs sur site. La commande des composants concernés à partir de l'AS ou de la LS est désactivée. Les verrouillages servent à protéger les personnes, les biens et l'environnement. Ils doivent être mis en place en fonction des spécificités de chaque projet.		

Tous les modes d'exploitation différents du mode « distant » ainsi que les interventions d'urgence doivent être affichés sur tous les niveaux supérieurs.

Les directives ASTRA 15010 « Plans de feux – Régulation du trafic » et 15019 « Logique de régulation du trafic - Exigences fonctionnelles minimales pour la conception et l'exploitation des systèmes de gestion du trafic en vue de fluidifier le trafic » décrivent les modes d'exploitation des installations de gestion du trafic. Les modes d'exploitation des installations EES correspondent, conformément au tableau suivant, aux modes d'exploitation des installations de gestion du trafic :

Tableau 16 : Installations EES et installations de gestion du trafic

Installations EES (directive 13031)	**Installations de gestion du trafic** (directives 15010 et 15019)
Distant	Exploitation normale
Local	Exploitation locale
Maintenance	-
-	Mode simulation
-	Mode autonome
-	Signal éteint (correspond au fonctionnement aveugle)

5.3.2 Modes de commande

Les modes de commande agissent sur l'état des agrégats d'une EES.

On distingue les modes de commande suivants selon les agrégats et leurs fonctions :

- Automatique (commandé par la logique de processus de l'installation) ;
- Manuel (commandé/activé par un utilisateur).

Le mode de commande suivant peut, en option, être utilisé au niveau de l'installation et non des agrégats :

- Programmes (en option, exécutés selon un déroulement prédéfini ; relèvent du mode de commande automatique).

Les modes de commande s'excluent mutuellement. Chaque agrégat ne peut se trouver que dans un seul mode de commande à un instant donné. Les modes de commande « Programmes » (en option) et « Manuel » ont toujours la priorité sur le mode de commande « Automatique ».

Tableau 17 : Types de commande

Mode automatique	En mode de commande « Automatique », le processus d'installation suit les informations qu'il reçoit de ses capteurs connectés ou de processus en cours sur d'autres EES. Il commande les actionneurs de l'installation conformément à ces instructions. Ce mode de commande agit sur tous les agrégats de l'installation et constitue le fonctionnement normal.
Mode manuel	En mode de commande « Manuel », le processus d'installation suit les instructions données manuellement par les utilisateurs, indépendamment des valeurs fournies par une grandeur de commande. Il commande les actionneurs conformément aux instructions manuelles fournies. Ce mode de commande agit sur des agrégats ou des parties d'installation spécifiques. Le mode de commande des agrégats non concernés est maintenu. Le mode automatique est actionné par les utilisateurs. En cas de commande manuelle, le système de commande de niveau supérieur doit vérifier si les commutations sont autorisées. En l'absence de consignes correspondantes ou d'autres mesures adaptées, les commutations non autorisées ne doivent pas être exécutées.
Programme (en option)	En mode de commande « Programme », le processus d'installation suit un déroulement prédéfini, indépendamment de valeurs de la grandeur de commande. Les actionneurs sont commandés selon le déroulement défini dans le programme. Ce mode de commande peut agir sur l'ensemble de l'installation ou des parties d'installation spécifiques, et commande ainsi tous les agrégats de l'installation ou les parties d'installation concernées. Le mode de commande des agrégats non concernés est maintenu. Les programmes peuvent être activés par les utilisateurs ou se déclencher automatiquement (interdomaines, fonctions temporelles, etc.)

Tous les modes d'exploitation différents du mode « Automatique » doivent être affichés sur tous les niveaux supérieurs.

5.3.3 Fonctions

Les fonctions suivantes sont disponibles dans tous les modes d'exploitation.

5.3.3.1 Fonctions de test

Diverses fonctions de test sont mises à disposition pour les essais et les mises en service d'installations neuves, en cas de remplacement ou pour les essais à répéter dans le cadre de l'entretien courant (p. ex. IGT, voir directive ASTRA 13028).

Les fonctions de test suivantes sont à prévoir :

- Forçage :
  Cette fonction permet de forcer (ou simuler) des valeurs (mesures, etc.) et ainsi de tester les fonctions de commande. Dans cet état, le processus EES utilise la valeur de remplacement saisie pour la commande de l'installation. La valeur d'origine des capteurs n'est pas prise en compte.
- Test de l'installation :
  Les messages sont transmis à des utilisateurs test spécifiques et non aux opérateurs. Des groupes d'utilisateurs dédiés sont à cet effet définis.
- Déclenchement d'interdomaines :
  Tous les interdomaines peuvent être déclenchés individuellement, côté source ou côté récepteur.
- Mode aveugle et mode éteint :
  Pour les tests des installations de signalisation, des commutations en mode aveugle ou en mode éteint peuvent être prévues afin de ne pas perturber inutilement le trafic et d'éviter les situations dangereuses.

Toutes les fonctions de test doivent être affichées à tous les niveaux.

5.3.3.2 Fonctions d'inhibition

Différentes fonctions d'inhibition destinées à divers cas d'utilisation sont disponibles. Selon la fonction, l'inhibition concerne l'AR, l'AS, la LS ou les agrégats. L'inhibition est permanente. Compte tenu de l'incidence possible sur les messages liés à la sécurité, l'inhibition doit être utilisé avec la prudence requise.

- Inhibition des messages :
  Tous les messages d'alarme et de perturbation peuvent être inhibés afin de maintenir l'exploitation en dépit de dysfonctionnements techniques.
- Inhibition des interdomaines :
  Tous les interdomaines peuvent être inhibés côté source ou côté récepteur.
- Désactivation :
  Cette fonction permet de désactiver les capteurs. La commande ne tient alors pas compte du capteur concerné.

L'inhibition d'un point de données doit être visualisée et affichée dans la liste des alarmes/messages.

Pour la gestion du trafic (installation de signalisation), l'inhibition est définie comme une passivation. Pour plus de détails, se référer à la directive ASTRA 15019.

5.3.3.3 Verrouillage

Les verrouillages destinés à empêcher des états, actions ou opérations non autorisés (p. ex. pour la ventilation, la signalisation ou l'alimentation électrique) peuvent être réalisés par matériel ou par logiciel et doivent être définis en fonction du domaine et du projet.

5.4 Monitoring

Le service de gestion OT « Monitoring des services » surveille l'ensemble des systèmes

des niveaux gestion et services de base. Les installations gérées via l'UeLS-CH s'auto-surveillent. La surveillance s'effectue selon une approche descendante (top-down). L'UeLS-CH reçoit toutes les annonces de perturbation.

5.5 Reporting

Le reporting permet de mettre en évidence les données et informations pertinentes, et fournit ainsi les bases nécessaires aux processus de gestion et de prise de décision. Un reporting sera déployé dans différents domaines et champs thématiques. Une fois établies, ces consignes seront transmises aux responsables.

Les informations sont agrégées selon le principe de la pyramide des données. Le reporting du niveau de gestion régional est par exemple agrégé au niveau des services de base et mis à disposition pour un traitement ultérieur.

Le reporting clé dans le domaine de la sécurité sera agrégé dans l'ISMS (Information Security Management System) de l'OFROU.

Les principales valeurs de référence (indicateurs clés) prises en charge sont les suivantes :

- Mise à disposition d'une base homogène pour chaque domaine thématique ;
- Mise à disposition des bases pour la prise de décision ;
- Présentation des données et informations axées sur les parties prenantes ;
- Amélioration de la transparence ;
- Établissement d'une base de comparaison ;
- Soutien de la gestion d'exploitation et stratégique ;
- Identification précoce des tendances de développement ;
- Contrôle de la conformité aux exigences.

5.6 Niveau de repli

En cas de défaillance d'un niveau de l'architecture SA-CH, le niveau inférieur garantit la continuité de l'exploitation et constitue le niveau de repli du niveau supérieur.

Cette structure permet l'autonomie des différents niveaux. Chaque niveau forme une unité fonctionnellement et techniquement autonome et ses fonctions fondamentales ne dépendent pas du niveau supérieur.

Ce principe fonctionne jusqu'au niveau 2 (AR). Ces différents niveaux sont illustrés dans le schéma ci-dessous :

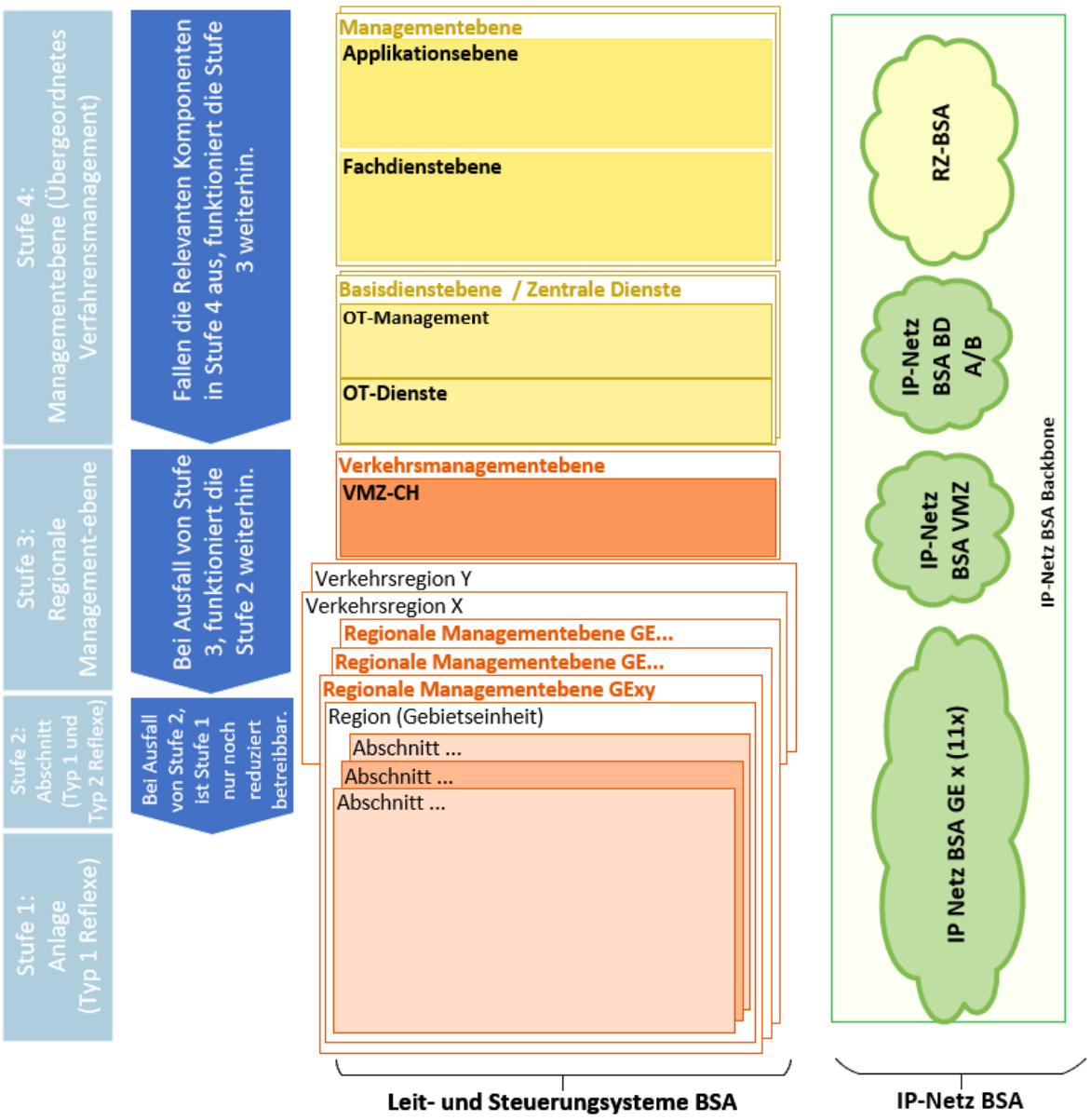


Figure 28 : Niveaux de repli SA-CH

Niveau 4

S'étend du niveau de gestion au niveau des services de base / services centraux. En cas de défaillance des composants critiques du niveau 4, le niveau 3 reste opérationnel. L'exploitation peut se poursuivre au niveau 3, éventuellement de manière limitée.

Niveau 3

Ce niveau inclut le niveau de gestion régional et le niveau de gestion du trafic. En cas de défaillance du niveau 3, le niveau 2 reste opérationnel. L'exploitation peut se poursuivre au niveau 2, éventuellement de manière limitée.

Niveau 2

Section (interdomaines de type 1 et 2) / AR : En cas de défaillance du niveau 2, le niveau 1 ne peut plus fonctionner que de manière limitée, car les interdomaines de type 2 ne sont plus actifs. L'exploitation peut se poursuivre au niveau 1, éventuellement de manière limitée.

Niveau 1

AS, LS, capteurs (interdomaines de type 1). En cas de défaillance du niveau 1, aucune exploitation n'est plus possible.

5.7 Liens WEB utiles pour l'exploitation

Tous les liens WEB collectés sur les MMI et les GUI doivent être sauvegardés séparément et conservés afin d'être disponibles en cas de reprise après sinistre. Ces liens WEB permettent d'accéder directement à l'AR ou à l'AS/LS en cas de défaillance de l'UeLS-CH.

5.8 Autonomie

Le chapitre 4.3.1 a abordé la question de l'autonomie liée à l'objet. Celle-ci désigne la capacité à fonctionner de manière autonome dans la section. Les tableaux ci-après présentent les scénarios d'exploitation possibles en tenant compte des installations critiques pour la sécurité. La question de l'autonomie énergétique ou de l'autonomie spécifique des installations n'est pas abordée ici.

5.8.1 Fonction de l'installation selon le scénario d'exploitation

Les parties d'installation qui doivent au minimum être opérationnelles pour garantir la sécurité de l'exploitation sont définies ci-après. Les dépendances relatives à la communication interne et externe à la section sont présentées dans le chapitre 5.8.7.

Tableau 18 : Parties d'installation nécessaires à une exploitation minimale sécurisée

Dés. AKS	Désignation de l'installation / partie d'installation	Remarque
ZEE	Système de gestion – énergie	
HS	Haute tension (apport d'énergie)	
NS	Basse tension (distribution d'énergie)	
NST	Alimentation sans coupure	
ZEB	Système de gestion – éclairage	
DB	Éclairage de traversée	
BN	Éclairage de secours en cas d'incendie	
FWB	Éclairage du chemin de fuite	
ZEL	Système de gestion – ventilation	
AL	Air vicié	
LL	Ventilation longitudinale	
ZL	Apport d'air frais	
FWL	Ventilation du chemin de fuite	
ZES	Système de gestion – signalisation	
VM	Signalisation dynamique	
LSA	Installation de signalisation lumineuse	
SER	Signalisation des dispositifs de sécurité	
BMT	Installation de détection incendie tunnel	
VTV	Installation vidéo	ED ou enregistreur d'images
DI	Système de gestion installation divers	Ouverture de porte
IPE	Réseau de communication Réseau IP Anneau de raccordement	
IPA	Réseau de communication Réseau IP Niveau d'accès	

Tableau 18 : Parties d'installation nécessaires à une exploitation minimale sécurisée

Dés. AKS	Désignation de l'installation / partie d'installation	Remarque
LTA	Système de gestion section	
FE	Système de radiocommunication (radio, interphonie, Polycom)	
NT	Téléphone de secours	
HI	Installation électrique intérieure	
HLK	Chauffage, ventilation, climatisation	
BMG	Installation de détection incendie bâtiment	
POR	Système de pompage	
LOE	Système de défense incendie	
TTZ	Porte / porte carrossable / contrôle d'accès	
WV	Alimentation en eau	
SABA	Installation d'évacuation et de traitement des eaux de chaussée	

5.8.2 Scénarios d'exploitation relatifs à l'autonomie de la section

Les scénarios d'exploitation suivants s'appliquent :

- Exploitation normale (tous les modes d'exploitation et toutes les possibilités de commande sont opérationnels) ;
- Exploitation limitée (toutes les fonctions automatiques (interdomaines) sont possibles, mais pas de possibilité de commande ou de communication avec l'UeLS-CH) ;
- Exploitation d'urgence avec valeurs de repli prédéfinies ;
- Pas d'exploitation.

La cause déclenchante ainsi que les fonctions disponibles sont présentées de manière générale ci-après.

5.8.3 Exploitation normale

Pas de déclencheur.

Principe :

- Communication interne et externe opérationnelle, y compris les accès ;
- Tous les interdomaines sont opérationnels.

5.8.4 Exploitation limitée

Déclencheur : communication à l'extérieur de la section totalement interrompue.

Principe :

- Communication interne opérationnelle, y compris les accès ;
- Tous les interdomaines sont opérationnels (connexions réseau AS-AR-AS) ;
- Commande : pertinente pour l'autonomie de la section (fonctionnement automatique autonome AVEC/SANS intervention d'un opérateur (sur place dans la section)) ;
- Sans déclenchement d'alerte en dehors de la section.

5.8.5 Exploitation d'urgence

Déclencheur : communication à l'intérieur de la section **partiellement** interrompue.

Principe :

- Communication interne partiellement interrompue ;

- Pertinente pour l'autonomie de la section (fonctionnement automatique autonome AVEC/SANS intervention d'un opérateur) ;
- Déclenchement d'alerte partiel en dehors de la section. Repli partiel vers la configuration de base ou les valeurs préprogrammées ;
- Ce scénario opérationnel est limité dans le temps et nécessite une autorisation. Il convient en principe de clarifier avec le chef d'intervention de l'UT et le chef d'intervention de l'OFROU dans quelle mesure un fonctionnement sûr peut être garanti.

5.8.6 Pas d'exploitation

Déclencheur : communication à l'extérieur de la section totalement interrompue.

Principe :

- Aucun interdomaine n'est opérationnel ;
- Aucune commande ou transmission de message possible depuis l'UeLS-CH ;
- Fermeture du tunnel déclenchée automatiquement par la fonction d'urgence de chaque AS.

5.8.7 Vue d'ensemble des scénarios d'exploitation

Le tableau suivant présente un aperçu des scénarios d'exploitation selon le principe et l'état.

Tableau 19 : Vue d'ensemble des scénarios d'exploitation

		Principes et état	Exploitation normale	Exploitation limitée	Exploitation d'urgence	Pas d'exploitation	Niveau de repli (voir 5.6)
Domaine thématique	Point de dé-	Réseau IP EES à l'extérieur de la section	Fonction complète	Pas de fonction	Défaillances partielles	Fonction complète	Niveau 2-4
		Réseau IP EES à l'intérieur d'une section	Fonction complète	Fonction complète	Défaillances partielles	Pas de fonction	Niveau 1-2
	Répercussion	Communication AR vers UeLS/BL(Z)	Fonction complète	Pas de fonction	Défaillances partielles	Pas de fonction	Niveau 2-3
		Commande via l'UeLS/BL(Z)	Fonction complète	Pas de fonction	Défaillances partielles	Pas de fonction	Niveau 3
		Communication au sein de la section	Fonction complète	Fonction complète	Défaillances partielles	Pas de fonction	Niveau 1-2
		Accès à AR, AS, LS	Fonction complète	Fonction complète	Défaillances partielles	Pas de fonction	Niveau 1
		Fonction AR, y c. redondance (dans la section IP)	Fonction complète	Fonction complète	Défaillances partielles	Pas de fonction	Niveau 1
		Intervention sur l'AR au sein d'une section	Fonction complète	Fonction complète	Défaillances partielles	Pas de fonction	Niveau 1
		Activité interdomaine	Fonction complète	Fonction complète	Défaillances partielles	Pas de fonction	Niveau 1
		Incidence sur l'exploitation du tunnel	Fonction complète	Fonction complète	Défaillances partielles	Pas de fonction	Niveau 1

5.8.8 Champ d'application

Les scénarios d'exploitation applicables à chaque catégorie de tunnel sont présentés ci-après de manière générale :

Tableau 20 : Vue d'ensemble de l'applicabilité selon la catégorie de tunnel

	Longueur du tunnel (GV et RV*)	Ventilation	Exploitation normale	Exploitation limitée	Exploitation d'urgence
Catégorie de tunnel	< 300 m	aucune	Admise	Admise	Admise
	< 600 m	aucune	Admise	Admise	Admise
	< 1000 m	Oui (sans aspiration d'air vicié)	Admise	Admise	**Non admise**
	< 3000 m	Oui (év. avec aspiration d'air vicié)	Admise	Admise	
	> 3000 m	Oui (tunnel spécial)	Admise	Admise	

** GV=trafic bidirectionnel, RV = trafic unidirectionnel*

5.9 Réseau IP EES

Le réseau IP EES prend en charge la communication à tous les niveaux de l'architecture du système. Le réseau de communication relie le niveau gestion aux services de base, au niveau de gestion du trafic et aux niveaux de gestion régionaux, et assure par ailleurs la communication au sein des installations ainsi qu'entre les installations. Le réseau IP EES prend en charge la transmission de données, de vidéo et de voix. Il utilise nativement un adressage Ipv6, tout en maintenant la compatibilité avec l'adressage IPv4 pour les systèmes hérités ou encore non compatibles avec IPv6.

Toute la communication des EES s'effectue via le réseau IP EES. Aucun réseau séparé n'est utilisé. Seules les installations isolées ou autonomes non raccordées au réseau IP EES peuvent faire l'objet d'une exception.

De plus amples informations relatives à la topologie ou la technologie sont disponibles dans la directive ASTRA 13040.

5.10 Principes de communication

5.10.1 Principes et exigences

Le réseau IP EES est un réseau IPv6 qui peut également transport de l'IPv4 (double pile). Les exigences suivantes s'appliquent :

- Tous les composants du réseau (routeurs d'anneau de raccordement, commutateurs) sont exclusivement gérés via IPv6 ;
- Tous les composants du réseau (routeurs d'anneau de raccordement, commutateurs) prennent en charge le transport simultané de IPv4 et de IPv6 (double pile) ;
- Le système de gestion du réseau (NMS) est également déployé en tant qu'instance IPv6 ;
- Les services réseau de proximité tels que NTP, DNS et DHCP doivent être déployés en tant qu'instances IPv4 et IPv6 ;
- L'équipement réseau et l'infrastructure centrale accèdent aux services tels que RADIUS, LDAP et AD via IPv6 ;
- L'infrastructure de base (serveur et stockage) destinée aux services centraux dans les locaux techniques OT doit être déployée et gérée en tant qu'instance IPv6 ;

- Les pare-feu et les clusters de pare-feu doivent également être configurés en tant qu'instances IPv6 ;
- Dans les UT, l'UeLS-CH et les serveurs de gestion section (AR) sont accessibles via Ipv6, tout comme les postes de travail opérateurs/postes de commande ;
- Toutes les installations/parties d'installation opérant à travers plusieurs sections IP (p. ex. système gestion vidéo, y c. caméras) doivent, lors de leur mise en place initiale ou de leur renouvellement, exclusivement être configurées en tant qu'instances IPv6 et être uniquement accessibles via IPv6 ;
- Les autres installations/parties d'installation doivent, dans la mesure du possible, être configurées en IPv6 lors de leur construction ou de leur renouvellement. La migration des installations existantes vers IPv6 n'est pas requise.

L'objectif principal est de déployer une infrastructure IPv6 de base dans les UT et d'assurer la connectivité native IPv6 vers et depuis les unités territoriales (et non via NAT64/46).

5.10.2 Protocoles

L'échange de données entre le niveau de gestion, le niveau de gestion régional et les serveurs de gestion de section s'effectue toujours via des protocoles basés sur IP. Le protocole de communication OPC UA est utilisé par défaut. Les installations de gestion vidéo utilisent des protocoles de streaming standardisés tels que RTSP.

La communication au sein d'une section IP peut s'effectuer via IP ou via Ethernet. Si nécessaire, les actionneurs et les capteurs peuvent également être pilotés à l'aide de protocoles série. Si le pilotage de commandes d'installation et locales ou d'actionneurs individuels (p. ex. caméras) doit couvrir plusieurs sections IP, il convient toujours d'utiliser des protocoles basés sur IP tels que OPC UA ou RTSP (Real-Time Streaming Protocol).

L'utilisation des protocoles est présentée en détail dans le guide *« IP-Netz BSA Leitfaden Migration Anlagennetze »*.

5.11 Modèle de données et points de données

La présente directive ASTRA 13031 explique de quelle manière les éléments communiquent entre eux et avec le niveau de gestion (régional). La modélisation des points de données et leurs processus sont décrits dans la directive ASTRA 13033 « Application du modèle de points de données SA_CH ».

La directive ASTRA 13032 (parties 1 à 6) décrit l'échange d'informations au sein des différents niveaux et entre ceux-ci (parties 1 à 3), les interdomaines (partie 4), la gestion des alertes (partie 5) ainsi que les exigences relatives à l'illustration graphique (partie 6). La directive 13034 régit l'utilisation d'OPC UA.

5.12 Échange de données

Ce chapitre décrit à la fois les échanges de données au sein de l'UeLS-CH et de l'AR, ainsi qu'entre l'AS et les systèmes périphériques.

5.12.1 UeLS-CH

Échange de données avec d'autres systèmes (0) :
L'UeLS fournit à d'autres applications et à leurs utilisateurs les alertes sélectionnées.

Échange de données avec l'ELS (0) :
L'UeIS-CH fournit au système d'aide à l'engagement (SAE) et à ses utilisateurs les alertes/événements sélectionnés.

Échange de données avec l'AR (1) :
Cette interface permet à l'UeLS-CH de commander et de surveiller les sections EES.

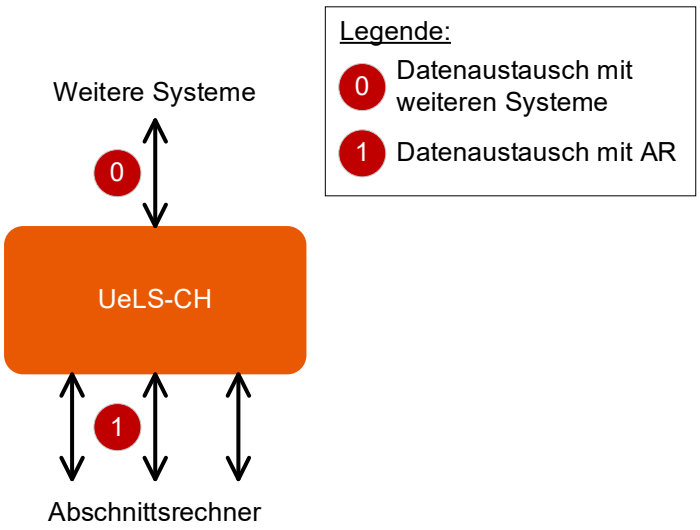


Figure 29 : Échange de données avec l'UeLS-CH

5.12.2 Serveur de gestion section

Échange de données avec le niveau de gestion régional (UeLS-CH) / utilisateur (1) :
L'AR fournit au niveau de gestion régional (UeLS-CH) / et à ses utilisateurs une sélection de points de données.

Échange de données avec l'AS (2) :
Cette interface permet à l'AR de commander et de surveiller les installations.

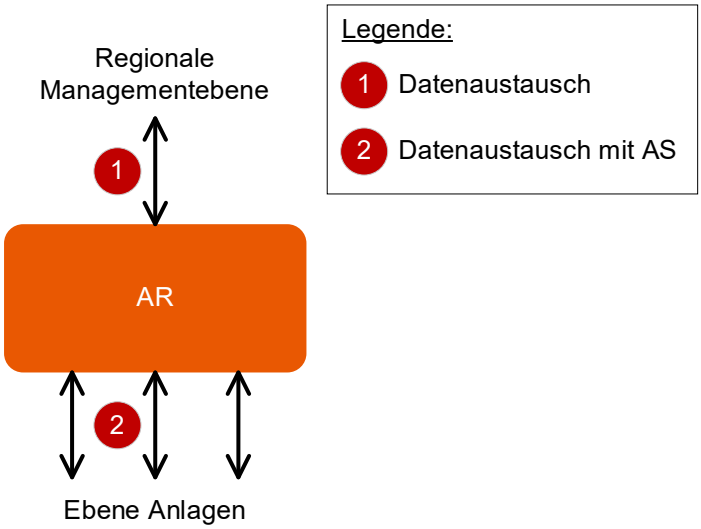


Figure 30 : Échange de données AR

5.12.3 Commande d'installation / commande locale

Échange de données entre l'AR et les utilisateurs (2) :
L'AS envoie des messages, des valeurs de mesure et des interdomaines source à l'AR, et reçoit des commandes ainsi que des interdomaines récepteurs de l'AR.

Communication de type 1 (3) :
La communication entre les AS s'effectue principalement par l'intermédiaire de l'AR. Une

connexion supplémentaire directe est prévue entre les AS pour les interdomaines de type 1 (cf. chap. 5.13).

Échange de données au sein de l'installation (4), (5), (6) :
L'AS échange des données et des ordres de commande avec les LS, leurs E/S distantes ainsi qu'avec les capteurs et les actionneurs.

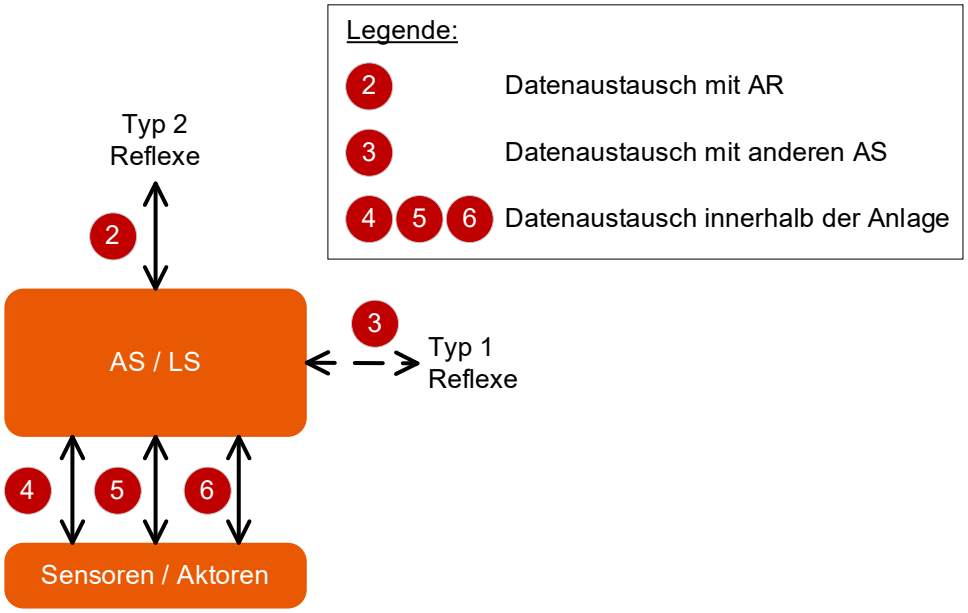


Figure 31 : Échange de données AS/LS

5.13 Interdomaines

Ce document aborde uniquement les différents types d'interdomaines et leur mode de transmission. L'utilisation des réflexes est décrite dans la directive ASTRA 13032 (partie 4).

5.13.1 Modes de transmission des interdomaines

Les interdomaines doivent en principe être transmis d'une source vers un récepteur. Il existe trois modes de transmission des interdomaines :

- En mode de **transmission automatique**, les interdomaines sont acheminés sans interruption de la source vers le récepteur ;
- En mode de **transmission semi-automatique**, les interdomaines ne sont pas transmis sans confirmation de l'AR (par l'opérateur), ou les interdomaines sont transférés par l'AR si un délai d'attente (timeout) pour l'acceptation ou le refus de l'interdomaine est paramétré dans un intervalle de temps défini (p. ex. en cas d'incendie) ;
- En mode de **transmission manuelle**, les interdomaines sont créés manuellement. Ce mode peut être utilisé si les interdomaines automatiques sont défaillants ou lors d'un test visant à vérifier le bon fonctionnement de l'installation.

L'AR est conçu pour être commandé manuellement par un opérateur.

Pour chaque projet, il convient toujours d'examiner quelle connexion constitue la variante la plus sûre compte tenu des dépendances avec les autres installations.

5.13.2 Types d'interdomaines

Compte tenu des exigences de sécurité attendues sur les routes nationales, les interdomaines sont classés en deux types. Ces deux types diffèrent selon les exigences de disponibilité, de transmission des interdomaines et des solutions techniques qui en découlent :

L'interdomaine de type 1 (critique pour la sécurité) est utilisé lorsque l'interdomaine a la priorité absolue et doit rester opérationnel même en cas défaillance d'une liaison de communication avec un élément de niveau supérieur, tel que l'AR.

L'interdomaine de type 2 (non critique pour la sécurité) est utilisé lorsqu'une situation dangereuse exige une action immédiate.

La liste des interdomaines de type 1 est définie dans la directive ASTRA 13032 (partie 4).

5.13.3 Architecture cible

L'augmentation de la disponibilité de l'AR permet d'intégrer les interdomaines de type 1 dans l'architecture des réflexes de type 2, mais uniquement si la preuve de la disponibilité requise est fournie.

5.13.3.1 Interdomaine critique pour la sécurité (type 1)

Le type 1 est utilisé lorsque l'interdomaine a la priorité la plus élevée. Il doit donc également être transmis en cas de défaillance d'une liaison de communication ou d'un élément au niveau AS ou AR. Les défaillances isolées sont prises en compte. Une disponibilité plus élevée doit être garantie pour ce type d'interdomaine (réseaux, commutateurs, commandes redondantes, etc.). Les interdomaines sont directement transmis à l'AS et/ou la LS concernée. L'interdomaine est toutefois transmis de manière redondante via le réseau IP EES. Pour traiter l'interdomaine, chaque sous-niveau doit se coordonner avec le niveau supérieur.

Une connexion directe peut être établie via le réseau IP EES à la place de la connexion matérielle.

Le couplage d'installations via des connexions d'interdomaine dédiées est autorisé. Ces connexions reposent sur des interfaces exclusivement destinées à la transmission des interdomaines entre les installations et distinctes des interfaces de communication AS-LS et AS-AR.

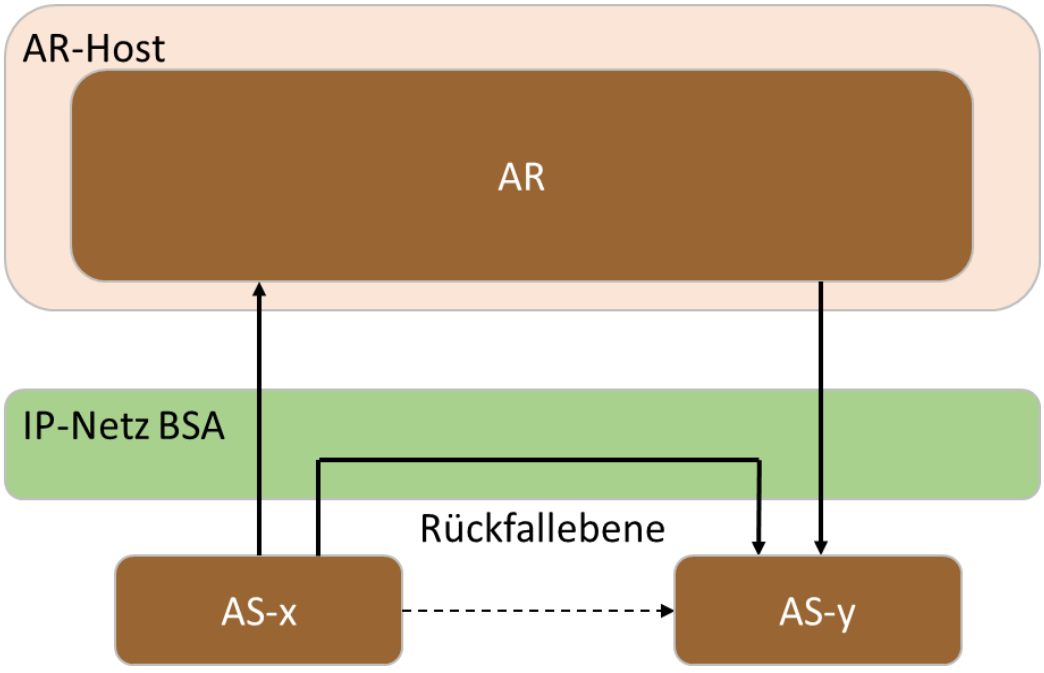


Figure 32 : Interdomaine de type 1

5.13.3.2 Interdomaine non critique pour la sécurité (type 2)

Le type 2 est utilisé pour tous les interdomaines non classés dans le type 1. Une disponibilité standard est suffisante pour ce type d'interdomaine. Les interdomaines de type 2 sont échangés via l'AR, sans transmission parallèle.

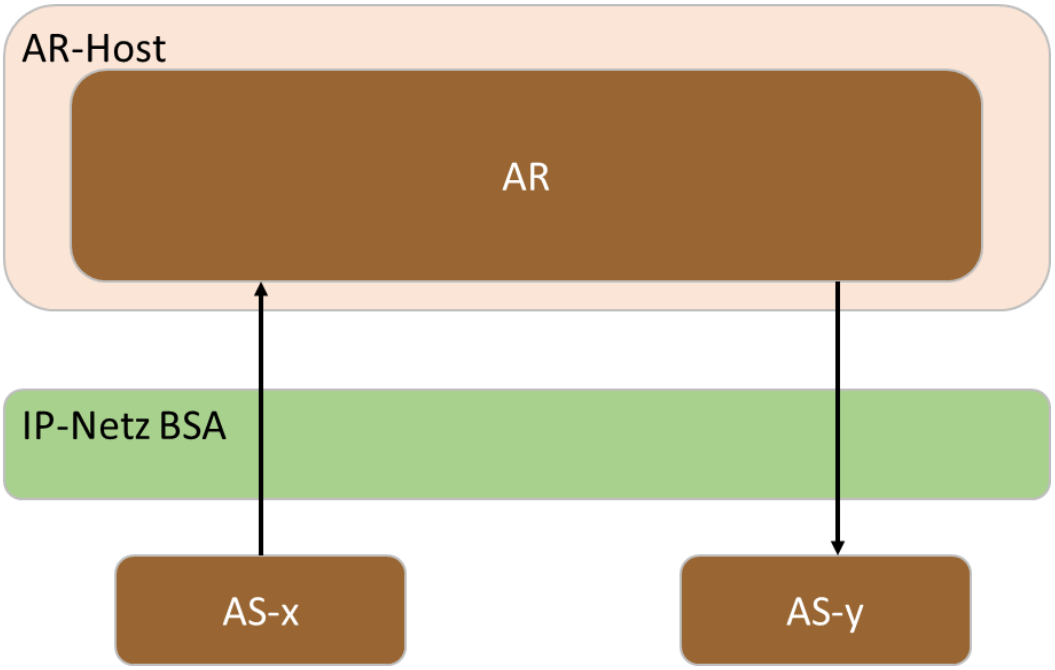


Figure 33 : Interdomaine de type 2

Les notions de « disponibilité standard » et « disponibilité élevée » sont définies dans le chapitre « disponibilité ».

5.14 Portails d'accès OT/EES et accès à distance (systèmes de secours OT)

Conformément à la documentation ASTRA 83056, ceux-ci sont assurés via les portails d'accès OT/EES.

5.15 Connexion des systèmes périphériques

Les systèmes périphériques doivent être reliés à l'architecture SA-CH via le réseau IP EES.

5.16 Communication mobile

La première génération d'intégrations M2M a été utilisée pour l'intégration sans fil de postes de comptage du trafic et de caméras de circulation. Cette intégration repose sur l'attribution dédiée de plages d'adresse IP issues de l'ensemble du domaine d'adressage BIT, ainsi que sur un couplage direct dans le réseau IP EES Backbone.

La prochaine génération (à partir de janvier 2025) sera utilisable à grande échelle pour différentes applications (au sein du réseau IP EES) et spécialement conçue pour les EES.

6 Migration

Pour atteindre l'architecture cible, des étapes intermédiaires seront nécessaires dans les infrastructures existantes. Les étapes intermédiaires possibles en vue de la réalisation de l'architecture cible sont présentées dans les sous-chapitres suivants.

Par migration, on entend le transfert de l'architecture existante vers la nouvelle architecture décrite ici. La migration est considérée comme achevée lorsque toutes les installations existantes ont été remplacées par des installations conformes. Ce processus s'étend par conséquent sur plusieurs années. (Objectif SA-CH : d'ici 2029)

Les aspects essentiels concernant la migration sont abordés dans les sous-chapitres suivants.

La mise en œuvre du projet est régie par les directives en vigueur au moment de l'approbation du PI/Pdét. Compte tenu de la longue durée des projets, certains étant parfois suspendus pendant une période prolongée en raison de recours, il convient de s'assurer, lors de l'appel d'offres, que le cahier des charges de la réalisation (RPH) est conforme aux prescriptions, directives et documents en vigueur. Les divergences doivent être discutées avec le Soutien technique SA-CH. Le chef de projet doit justifier les exceptions et une autorisation écrite est requise.

Les tests de conformité réalisés au cours des différentes phases SIA permettent d'établir le degré de réalisation des prescriptions. Le cas échéant, des dates de contrôles subséquents sont fixées afin de compenser les écarts importants (délais transitoires).

Tous les projets doivent respecter les zones du réseau et la sécurité conformément aux prescriptions. Aucun écart ne peut être autorisé, le non-respect des exigences empêchant le bon fonctionnement de la communication.

6.1 Adaptations organisationnelles de la structure et de la structure d'exploitation de l'OT/EES

Dans le cadre du développement de la structure et de la structure d'exploitation de l'OT/EES, les tâches existantes de l'EES et de l'OT sont clarifiées et de nouvelles tâches sont définies. Les responsabilités et les compétences sont établies et présentées. Ces adaptations sont mises en œuvre progressivement puis intégrées dans les conventions.

6.2 Informations générales sur le concept de migration

Le concept de migration doit intégrer toutes les étapes, y compris l'évaluation des risques. À cet effet, la procédure de test et le contrôle de conformité doivent être disponibles.

Chaque projet présentant des spécificités différentes, aucune architecture de migration générale ne peut être définie.

6.3 Communication et système de gestion

Les étapes intermédiaires sont détaillées dans le le guide *« IP-Netz BSA Leitfaden Migration Anlagennetze »*. Les normes de communication doivent être mises en œuvre conformément aux définitions (pas d'intégrations modifiées). Les chefs de projet Réseau IP EES des filiales et le support métier Réseau IP EES de la centrale sont disponibles pour apporter leur soutien.

6.3.1 Système de gestion (UeLS-CH intégration du système)

Ce chapitre décrit les variantes de mise en œuvre recommandées à partir de l'exemple du système de gestion (UeLS-CH et intégration du système). Cette directive présente l'état cible de l'architecture du système. La Figure 34 présente un aperçu de l'architecture de migration en lien avec le système de gestion.

La mise en œuvre dépend de l'état actuel spécifique du projet, des systèmes et des définitions de projets existants. Les variantes sont présentées et discutées au cours de la phase SIA 31 (MK) (voir documentation ASTRA 83055).

Pour une meilleure compréhension, chaque élément pertinent n'est représenté qu'une seule fois dans la Figure 34. La notation « 1…x » indique sa multiplicité. La figure présente par ailleurs deux variantes de mises en œuvre.

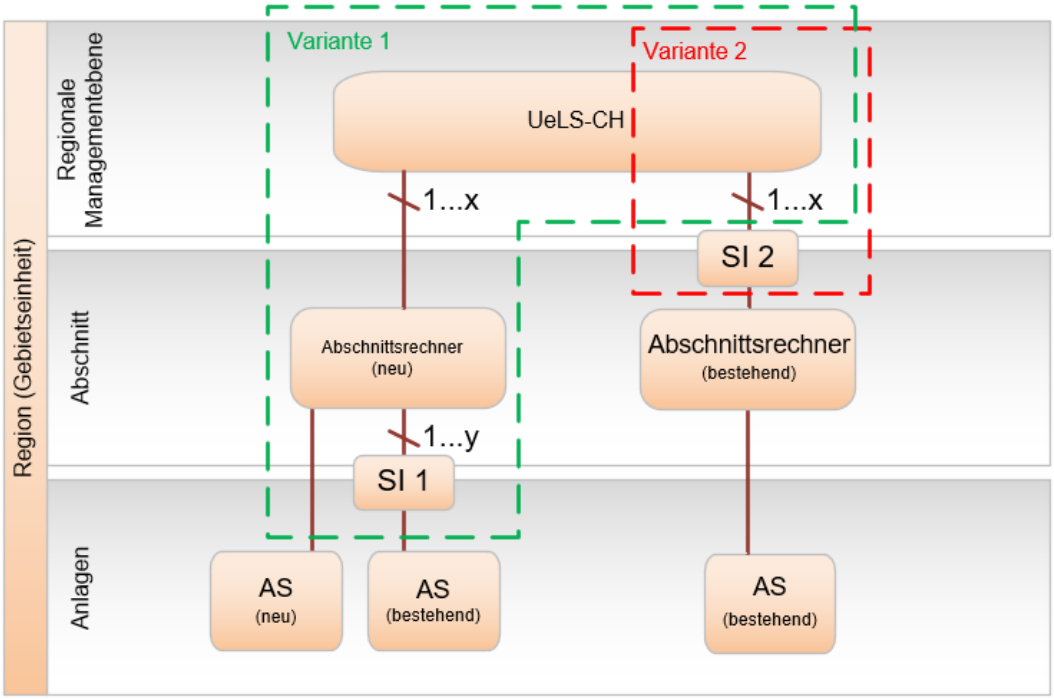


Figure 34 : Variantes de mise en œuvre du système de gestion (UeLS-CH et architecture du système), où nouveau = conforme SA-CH et existant = non conforme SA-CH

*nouveau = conforme SA-CH / *existant = non conforme SA-CH

Conformément à Figure 34Figure 34 , la migration peut s'effectuer selon les variantes suivantes :

Variante 1

Si des commandes d'installation (AS) existantes non conformes SA-CH sont intégrées dans des serveurs de gestion section (AR) conformes SA-CH, ces AS sont connectées aux AR correspondants via des « Service Integrators » (SI 1). Les SI garantissent le fonctionnement de l'interface AR <> AS conformément aux directives SA-CH.

Variante 2

Si des AR existants non conformes SA-CH sont intégrés avec des AS existantes dans un UeLS-CH, ces AR sont connectés à l'UeLS-CH via des « Service Integrators » (SI 2). Les SI garantissent le fonctionnement de l'interface UeLS-CH <> AR conformément aux directives SA-CH.

Ces variantes permettent une migration progressive des serveurs de gestion section et des commandes d'installation.

6.4 Systèmes de gestion du trafic

Tous les systèmes présentés ci-après constituent des solutions transitoires et seront démantelés ultérieurement.

6.4.1 Système Vehicle-by-Vehicle (VBV)

À moyen terme, le VBV sera progressivement remplacé par le service métier « Acquisition des données d'exploitation et de trafic (FD BVDE). Le VBV traite les données des postes de comptage du trafic et transmet ces informations aux systèmes périphériques dans différents formats.

6.4.1.1 Contrôleurs de comptage du trafic (ZSC)

Les ZSC doivent être démantelés en coordination avec la migration du réseau IP EES.

6.4.2 Système d'information sur le trafic (VIS)

La migration des systèmes d'information sur le trafic est planifiée par les filiales de OFROU. À noter : les temps d'indisponibilité doivent être réduits au minimum pendant la migration et planifiés au préalable avec la VMZ-CH. Une vérification des commandes existantes doit idéalement être effectuée avec la VMZ-CH, et les systèmes VIS actuels doivent si nécessaire être remplacés simultanément. À l'avenir, les WTA et WWW seront raccordés à la FA VL-CH en cours de mise en œuvre et seront ainsi pilotables de manière centralisée dans toute la Suisse.

6.4.3 Gestion régionale du trafic (rVL)

Après la phase transitoire, les rVL existantes seront remplacées par $VR_{RM\ VM\text{-}CH}$ ou VL-CH, et seront donc supprimées.

À noter : les temps d'indisponibilité doivent être réduits au minimum pendant la migration et planifiés au préalable avec la VMZ-CH. Une vérification des commandes existantes doit idéalement également être effectuée avec la VMZ-CH.

6.4.4 Acquisition régionale des données de trafic (rVDE)

Après la phase transitoire, les rVDE existantes seront soit directement connectées via l'infotransit des postes de comptage du trafic à $VR_{RM\ VM\text{-}CH}$ ou à VL-CH, et donc supprimées.

À noter : les temps d'indisponibilité doivent être réduits au minimum pendant la migration et planifiés au préalable avec la VMZ-CH. Une vérification des commandes existantes doit idéalement également être effectuée avec la VMZ-CH.

6.4.5 Calculateur de trafic régional (VR)

Les VR (solution intermédiaire IVM et RM VM) seront remplacés par la FA VL-CH après la phase transitoire.

Annexes

I Terminologie 81
I.1 Disponibilité (availability) 81
I.2 Haute disponibilité (High Availability) 81
I.3 Tolérance aux pannes (Fault Tolerance) 81
I.4 Redondance (Redundance) 81
I.5 Hot-standby 81
I.6 Cold-standby 82
I.7 Sauvegarde des données et du système (Backup) 82
I.8 Disaster-Recovery 82

II Redondances 83
II.1 Redondance applicative 83
II.2 Augmentation supplémentaire de la redondance 84
II.3 Cluster à haute disponibilité (cluster HA) 84
II.4 Cluster haute disponibilité (Failover Cluster) 85
II.5 Cluster avec SAN virtuel (Storage Area Network) 86
II.6 Cluster Fault Tolerance (FT) 86
II.6.1 Comparaison de la redondance AR 86

III Bases de la virtualisation 88
III.1 Plateforme de virtualisation 88

IV Architecture système Suisse (SA-CH) 90
IV.1 Architecture SA- CH 90
IV.2 Architecture SA- CH : mise en œuvre SA-CH GUI/MMI 91

V Applications technologiques 92
V.1 Applications technologiques pour un tube 92
V.2 Applications technologiques pour deux tubes 93
V.3 Exemple de calcul des ressources matérielles 95
V.3.1 Matériel hôte (serveur) 95
V.3.2 Infrastructure de stockage des données (storage) 97

I Terminologie

Les notions fondamentales et leurs définitions sont présentées ci-après.

I.1 Disponibilité (availability)

La disponibilité d'un système technique correspond à sa capacité à satisfaire des exigences définies sur une période donnée. Une indisponibilité (« downtime ») peut notamment être provoquée par des erreurs, des pannes et des interruptions survenant au sein du système ou dans les systèmes périphériques.

Dans le cas des EES, les exigences sont souvent implicitement définies par leur fonctionnalité : une installation est disponible tant qu'elle fonctionne. Pour les systèmes complexes, un SLA (Service Level Agreement) fixe p. ex. les exigences que le système doit satisfaire pour être considéré comme disponible.

Les processus métier et les systèmes associés doivent être fournis avec le minimum d'interruptions afin d'atteindre les objectifs de l'entreprise. La disponibilité doit ainsi correspondre au temps d'exploitation nécessaire. Pour les EES, le système doit par conséquent satisfaire aux exigences 24h/24 et 7j/7.

I.2 Haute disponibilité (High Availability)

La haute disponibilité désigne la capacité d'un système à garantir un niveau de disponibilité élevé. Les valeurs de disponibilité d'un système à haute disponibilité s'élèvent typiquement à 99,99 % (« four-9s ») ou 99,999 % (« five-9s »), soit une indisponibilité annuelle de 52 minutes ou 5,2 minutes en fonctionnement 24h/24 et 7j/7. Dans les systèmes complexes, ces valeurs de disponibilité élevées nécessitent impérativement une conception tolérante aux pannes et des redondances appropriées.

I.3 Tolérance aux pannes (Fault Tolerance)

Lorsqu'une erreur survient dans le système (panne matérielle, perte de communication, etc.), les exigences ne sont plus satisfaites et le système n'est plus considéré comme disponible. La tolérance aux pannes garantit le respect des exigences même en cas de défaillance. L'objectif est d'éviter les défaillances catastrophiques causées par un point de défaillance unique (Single Point of Failure) et d'assurer la continuité d'exploitation.

La tolérance aux pannes est intégrée dans la conception du système et couvre uniquement les erreurs envisagées lors de la conception. En règle générale, la tolérance aux pannes est conçue de manière à prendre en charge plusieurs erreurs, même simultanées (p. ex. panne de l'alimentation électrique ou d'un chemin de communication).

I.4 Redondance (Redundance)

La redondance fournit des ressources supplémentaires (matérielles ou logicielles) non nécessaires à la satisfaction des exigences. En cas de dérangement, elles sont activées afin de garantir la continuité d'exploitation. Les ressources supplémentaires sont généralement des sous-systèmes dupliqués. Les désignations courantes sont « 1:1 » lorsqu'une ressource de réserve est prévue pour chaque ressource, et « 1:n » lorsqu'une seule ressource de réserve couvre n ressources.

I.5 Hot-standby

La ressource de réserve est entièrement synchronisée avec la ressource active afin de permettre une reprise immédiate de l'exploitation. La ressource de réserve satisfait immédiatement aux exigences, sans nécessiter de synchronisation avec les systèmes connectés (hit-less »). En général, un moniteur indépendant surveille les ressources et

déclenche le basculement (« switch-over »). Dans les architectures simples, les ressources se surveillent mutuellement et gèrent elles-mêmes le basculement.

I.6 Cold-standby

La ressource de réserve reste inactive jusqu'à la survenue d'une panne. Une fois activée, elle doit d'abord se synchroniser avec les systèmes connectés. Durant cette phase de synchronisation, la ressource de réserve ne satisfait pas encore aux exigences et le basculement est visible pour les systèmes périphériques (non hit-less »). L'établissement d'une nouvelle connexion ou un redémarrage intégral des transactions est souvent nécessaire. La ressource de réserve doit être déclenchée par une impulsion externe, car ni la ressource défaillante ni la ressource de réserve passive ne sont en mesure de le faire de manière fiable. Une intervention manuelle est souvent requise.

I.7 Sauvegarde des données et du système (Backup)

La sauvegarde des données et du système crée un instantané de l'état du système à un moment déterminé. Cet instantané peut restaurer les données ou les systèmes à l'état de la sauvegarde. Les erreurs de manipulation ou survenues dans l'application de traitement des données peuvent ainsi être annulées. Toutes les modifications intervenues depuis la dernière sauvegarde sont toutefois perdues et doivent à nouveau être saisies. Outre cette réinitialisation, une sauvegarde système permet également d'effectuer une restauration sur un autre matériel. La sauvegarde système constitue ainsi également un mécanisme de protection contre les pannes matérielles, mais implique toutefois une importante perte de données et une indisponibilité prolongée.

Un archivage permet, via des mécanismes similaires, de conserver des données et des états système sur de longues périodes. La priorité n'est ici pas la restauration. L'archivage permet notamment, à la suite d'incidents (p. ex. en criminalistique), d'effectuer une reconstitution ou de démontrer la traçabilité complète d'un journal d'audit (audit trail).

I.8 Disaster-Recovery

Après une panne complète, l'état d'exploitation est rétabli conformément aux processus et aux plans de redémarrage (incluant l'ordre de priorité précis des systèmes).

II Redondances

La redondance vise à augmenter la disponibilité et la maintenabilité d'un système, en l'occurrence les « systèmes de gestion et de commande des équipements d'exploitation et de sécurité » sur les routes nationales.

La disponibilité globale est augmentée grâce au choix d'un réseau approprié (voir directive ASTRA 13040) et à une architecture système adaptée, certaines parties du système pouvant tomber en panne sans provoquer un arrêt complet. Tout comme l'architecture du système, l'architecture de communication constitue un élément essentiel pour augmenter la disponibilité.

La liste suivante se limite à l'augmentation de la disponibilité des ordinateurs OTTR, des AR et des AS.

La disponibilité des moyens de communication, des applications et des données doit en principe être augmentée par un environnement redondant à haute disponibilité (matériel, logiciel et gestion des éléments).

La redondance peut être obtenue à différents niveaux, mais dépend des possibilités prises en charge par les fabricants et doit être vérifiée en conséquence :

- Redondance logicielle : application, base de données, virtualisation des applications, du bureau et/ou du serveur au moyen d'un hyperviseur (variable selon le fabricant) ;
- Fonctions supplémentaires de l'hyperviseur : High Availability (grâce au partage des ressources sur l'hyperviseur, une panne matérielle peut être surmontée de manière transparente), Fault Tolerance (le système miroir fonctionne de manière synchrone), répartition automatisée de la charge, etc. ;
- Redondance matérielle : cluster matériel ou association de 2 unités ou plus avec différentes possibilités de réalisation : actif/passif (hot-standby ou cold-standby), actif/actif (synchrone ou hot-standby).

II.1 Redondance applicative

Les applications utilisées disposent souvent de leur propre possibilité de redondance. Le cas échéant, cette possibilité de redondance peut être utilisée.

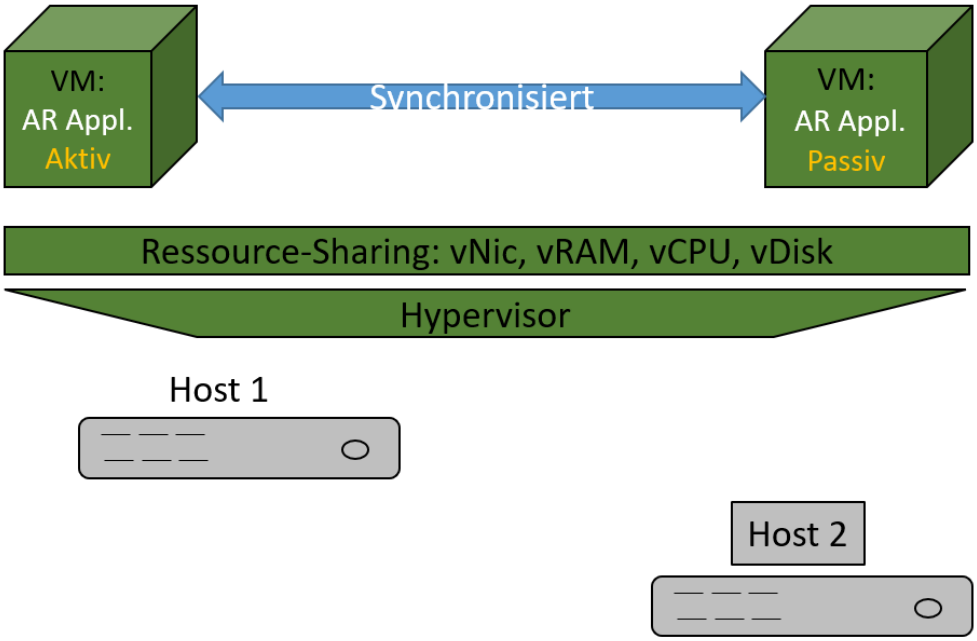


Figure II.1 : Redondance d'application AR

La Figure II.1 présente une solution d'application. Voici une description (simplifiée) du principe :

- Les deux hôtes (1 et 2) sont actifs (AR 1-1 et AR 1-2) ;
- Un guest (VM application AR sur VM AR 1-1) est actif, l'autre est passif (application AR sur VM AR 1-2) ;
- Les applications AR sur les guests synchronisent leurs données entre elles et se surveillent mutuellement ;
- En cas de panne de l'application active, l'application passive devient « immédiatement » active.

L'avantage est le recours à une solution de redondance éprouvée, fonctionnelle et prise en charge par le fabricant. Le principal inconvénient réside dans l'utilisation. Le niveau gestion doit savoir quel AR est actif et contrôler l'accès en conséquence. Du point de vue de la communication, cette solution ne pose aucun problème compte tenu du doublement possible des lignes de communication (partie intégrante de OPC UA ; Profinet Multi Controller, Multi Device ; Modbus TCP Multi Client, Multi Server).

L'hôte doit être surveillé séparément et fonctionne de manière indépendante (VM AR 1-1 indépendante de VM AR 1-2).

II.2 Augmentation supplémentaire de la redondance

La redondance des applications peut être accrue en utilisant des mécanismes internes supplémentaires des plateformes de virtualisation. Les mécanismes de redondance peuvent être combinés en configurant l'application AR ou le guest correspondant (VM), ainsi que la même application AR (VM), en tant que services indépendants. Une panne du service sur l'hôte entraîne le redémarrage du même service sur un autre hôte ou son transfert vers celui-ci. L'application AR sur l'hôte détecte simultanément la panne de l'autre application AR sur l'autre hôte et s'active ainsi à son tour.

II.3 Cluster à haute disponibilité (cluster HA)

Les clusters à haute disponibilité permettent de relier entre eux 2 ou plusieurs ordinateurs de sorte qu'un seul ordinateur soit visible de l'« extérieur ». En cas de panne sur l'un des systèmes, l'autre peut ainsi prendre le relais afin de maintenir la disponibilité du service ou de l'application.

Si une erreur se produit sur l'ordinateur du cluster, les services fonctionnant sur cet ordinateur sont migrés vers un autre ordinateur (de manière automatisée ou manuelle). Tous les éléments critiques (RAM, cartes réseau, processeurs, disques, alimentations sont au moins dédoublés. Tous les ordinateurs accèdent à la même base de données.

Cette solution est prise en charge par les principaux hyperviseurs (modules supplémentaires pour vSphere, Hyper-V Server, etc.) et peut être utilisée comme possibilité de redondance.

Contrairement à la redondance applicative, le cluster HA est une solution informatique classique et non une solution d'application. La solution cluster HA nécessite davantage de ressources matérielles (2 ordinateurs, plusieurs réseaux par ordinateur) et un effort de configuration supplémentaire (détermination des services et des ressources pour la surveillance). En revanche, la solution HA est indépendante du fabricant en ce qui concerne l'application AR et constitue une solution courante et répandue dans les environnements informatiques.

II.4 Cluster haute disponibilité (Failover Cluster)

Le système d'exploitation HOST étendu permet de réaliser des clusters haute disponibilité, également appelés « Failover Clusters ». Le Failover Cluster présente une grande résistance aux pannes grâce à la redondance.

Dans un cluster haute disponibilité, les composants critiques sont réalisés de manière redondante. Si un composant tombe en panne dans un serveur, le composant redondant de l'autre serveur prend le relais. Selon la configuration, il est possible, dans les clusters haute disponibilité, que les deux serveurs (nœuds), le primaire et le secondaire, soient actifs et répartissent la charge. Il se peut toutefois également que seul un des deux soit actif et que l'autre soit passif et en veille.

Ces clusters sont visibles comme un seul et même serveur de l'« extérieur », avec au moins une machine virtuelle AR.

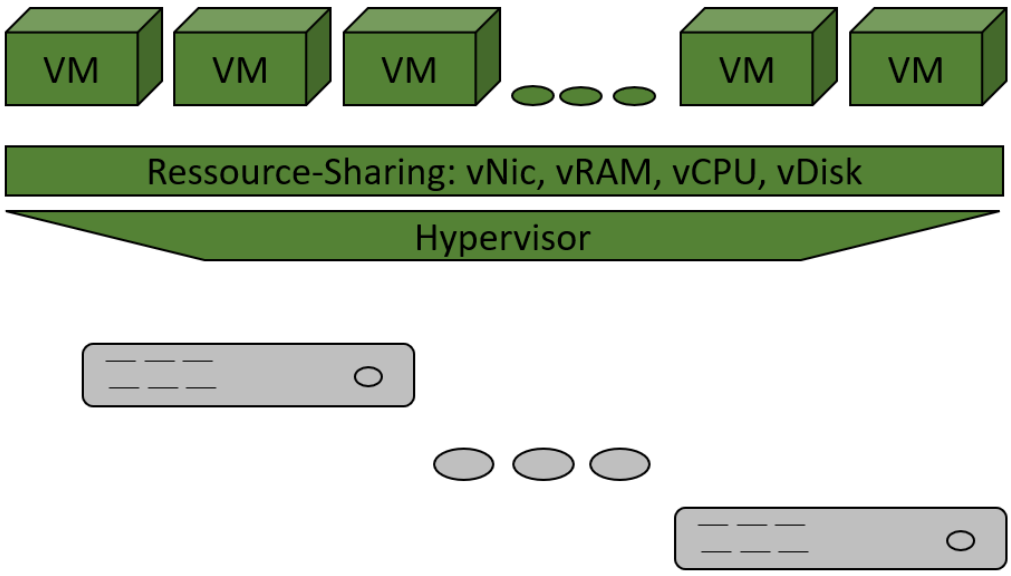


Figure II.2 : Failover Cluster

Dans le cas du Failover Cluster, les machines virtuelles sont exploitées à l'intérieur du cluster, et ne sont donc visibles de l'« extérieur » que sous la forme d'un serveur. Le Failover Cluster prend en charge la gestion totale de la redondance.

II.5 Cluster avec SAN virtuel (Storage Area Network)

Dans cette configuration, le stockage de données existant est partagé entre tous les ordinateurs (VSAN).

Le principe (largement simplifié) est le suivant :

- Un élément est toujours actif (par exemple une interface de communication) ;
- Chaque nœud surveille ses services et son matériel spécifiques ;
- Les 2 hôtes échangent généralement ces données d'état via un réseau dédié ;
- En cas d'irrégularités, l'autre nœud prend en charge les services nécessaires et met le matériel nécessaire à disposition ;
- Les disques durs de l'ordinateur 1 et de l'ordinateur 2 sont regroupés logiquement (virtuellement) en « un seul disque ».

II.6 Cluster Fault Tolerance (FT)

Dans le cas du cluster Fault Tolerance, les ressources matérielles sont mises en miroir sur deux serveurs et tous les ordres sont exécutés de manière redondante sur le serveur miroir. Si le serveur maître tombe en panne, l'esclave prend en charge poursuite du traitement des applications en cours, en temps réel.

II.6.1 Comparaison de la redondance AR

La redondance d'application, le cluster HA et la redondance mixte sont autorisés. Le tableau suivant n'est pas exhaustif et ne fournit que des bases décisionnelles sommaires.

Tableau II.3 : Comparaison de la redondance AR

Exigence / Disponibilité	Redondance d'application	Cluster HA	Redondance mixte	Remarque
Configuration du réseau	Faible	Normale	Élevée	
Exploitation du réseau	Faible	Faible	Faible	
Personnel d'entretien	Faible	Faible	Élevé	Situation initiale, la composition du personnel peut varier au fil du temps
Support OT	Faible	Élevée	Élevée	
Distribution OT	Très faible	Très élevée	Très faible	Connaissances sur le « marché »
Coûts du matériel	Moyens	Élevés	Élevés	
Coûts des logiciels du système	Élevés	Élevés	Très élevés	
Disponibilité	Élevée	Très élevée	Très élevée	
Sauvegarde / Restauration	Normale	Faible	Normale	
Conservation des données	Normale	Normale	Normale	
Mise à jour du système d'exploitation (sécurité)	Élevée	Faible	Très élevée	

Charge de travail pour le remplacement	Élevée	Faible	Très élevée	
Disponibilité sur le marché	Élevée	Très élevée	Élevée	
Connaissances SCADA	Moyennes	Élevées	Moyenne	1)

1) Pour fonctionner de manière fluide, le cluster HA doit savoir exactement quels services / processus doivent être surveillés et de quelle manière . Souvent, les fournisseurs ne disposent pas de ces informations, car ils utilisent des logiciels « clés en main » qu'ils ont soit achetés, soit développés en interne. Cet aspect doit être clarifié au cas par cas lors de la mise en œuvre.

Une redondance conforme aux chapitres ci-dessus est exigée. Les caractéristiques sont laissées à l'appréciation de l'unité territoriale et n'ont pas d'impact significatif sur l'intégration dans le niveau de gestion régional si sur la connexion au niveau de l'installation.

III Bases de la virtualisation

III.1 Plateforme de virtualisation

La virtualisation neutralise le lien avec le matériel. Le matériel est ainsi émulé au moyen d'une couche logicielle intermédiaire (hyperviseur). La virtualisation permet à la fois d'améliorer la compatibilité de l'ordinateur virtualisé avec les différents fabricants de matériel serveur, tout en simplifiant la maintenance. Grâce à la connexion virtuelle via l'hyperviseur, les ressources physiques existantes sont regroupées et mises à la disposition des « machines virtuelles ».

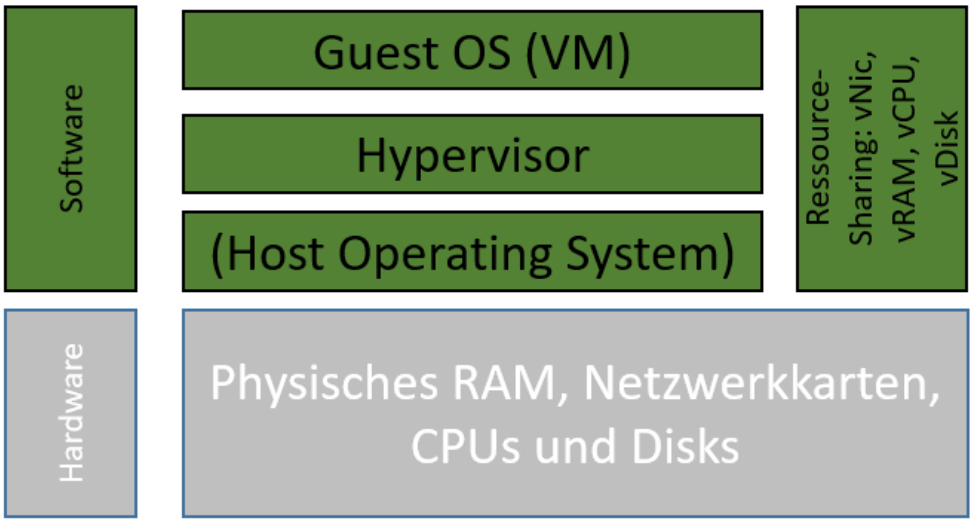


Figure III.4 : Structure de la plateforme de virtualisation (représentation schématique)

Les fonctions les plus importantes sont les suivantes :

- Utilisation efficace de toutes ressources existantes ;
- Indépendance vis-à-vis du fabricant de serveurs ;
- La maintenance du matériel et des logiciels est simplifiée et peut être effectuée pendant l'exploitation ;
- La sauvegarde et la récupération après sinistre sont plus faciles à réaliser (voir chapitre suivant).

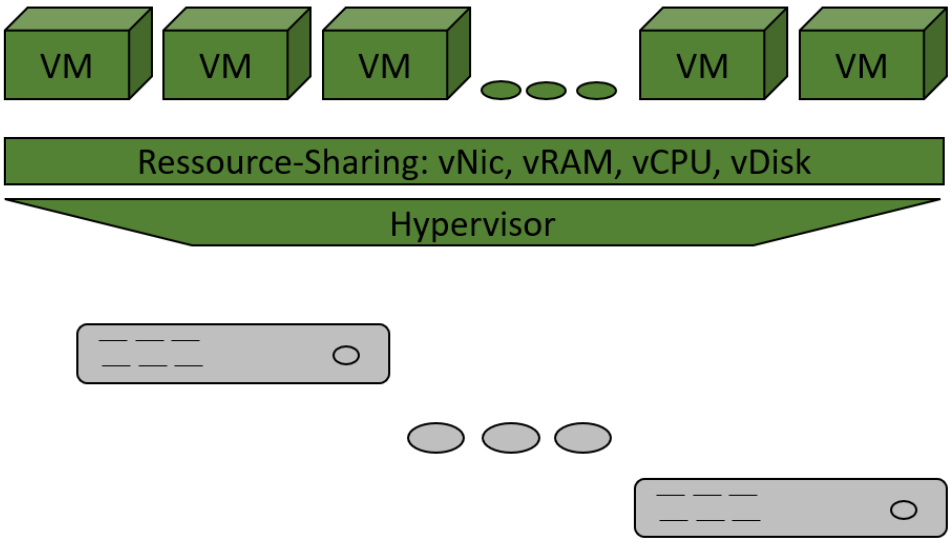


Figure III.5 : Représentation schématique de la plateforme de virtualisation

Chaque plateforme de virtualisation se compose de plusieurs ensembles de matériel informatique (selon Figure III.5), soit :

- Plateforme de virtualisation dans le local technique OT (OTTR) et la centrale technique : au moins 3 ensembles de matériel informatique chacun ;
- Plateforme de virtualisation dans les locaux techniques ou les petits objets (par exemple un tunnel de moins de 600 m) : au moins 2 ensembles de matériel informatique chacun.

Deux types de virtualisation sont admis :

- Virtualisation au moyen du système d'exploitation hôte et/ou logiciel de virtualisation séparés. Exemple : Microsoft Hyper-V avec Microsoft Windows Server ;
- Virtualisation au moyen du système d'exploitation hôte et/ou logiciel de virtualisation regroupés. Exemple : VMware vSphere.

IV Architecture système Suisse (SA-CH)

IV.1 Architecture SA- CH

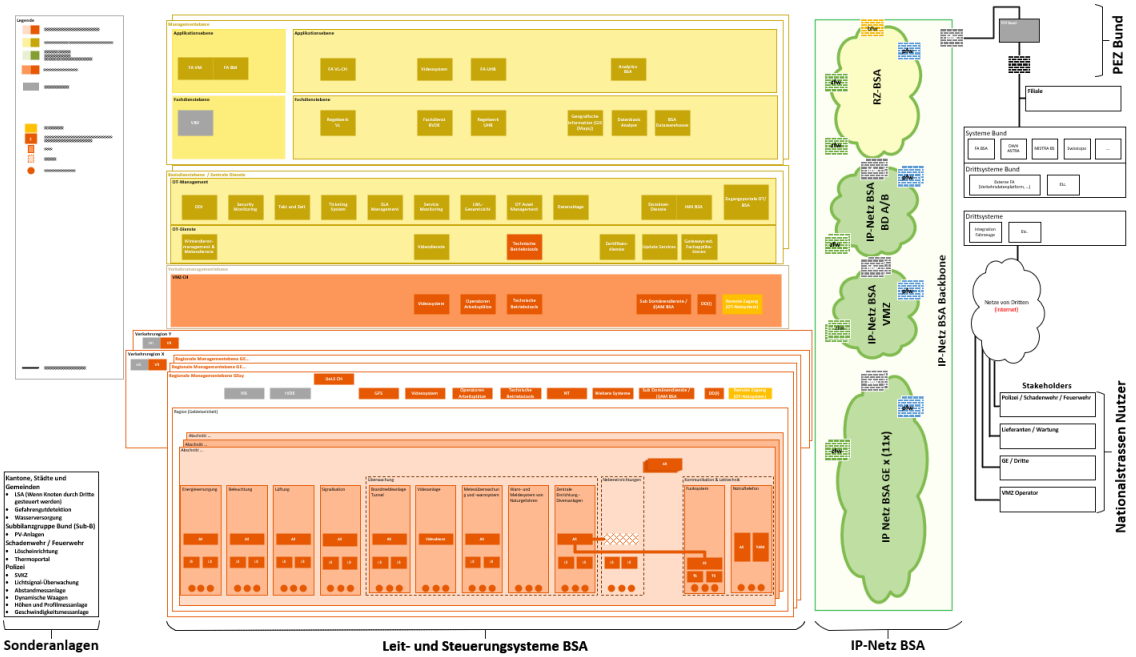


Figure IV.6: Architecture SA-CH (Présentation de la section : nombre maximal d'installations dans le tunnel)

IV.2 Architecture SA- CH : mise en œuvre SA-CH GUI/MMI

L'aperçu ci-dessous présente à la fois les interfaces utilisateur GUI (GUI) et MMI (MMI). Comme expliqué dans le chapitre 5.2.3, les implémentations MMI doivent impérativement respecter les guides de style de l'OFROU pour toutes les applications métier. Les composants et outils standard, tels que NMS, peuvent être mis en œuvre l'interface graphique standard.

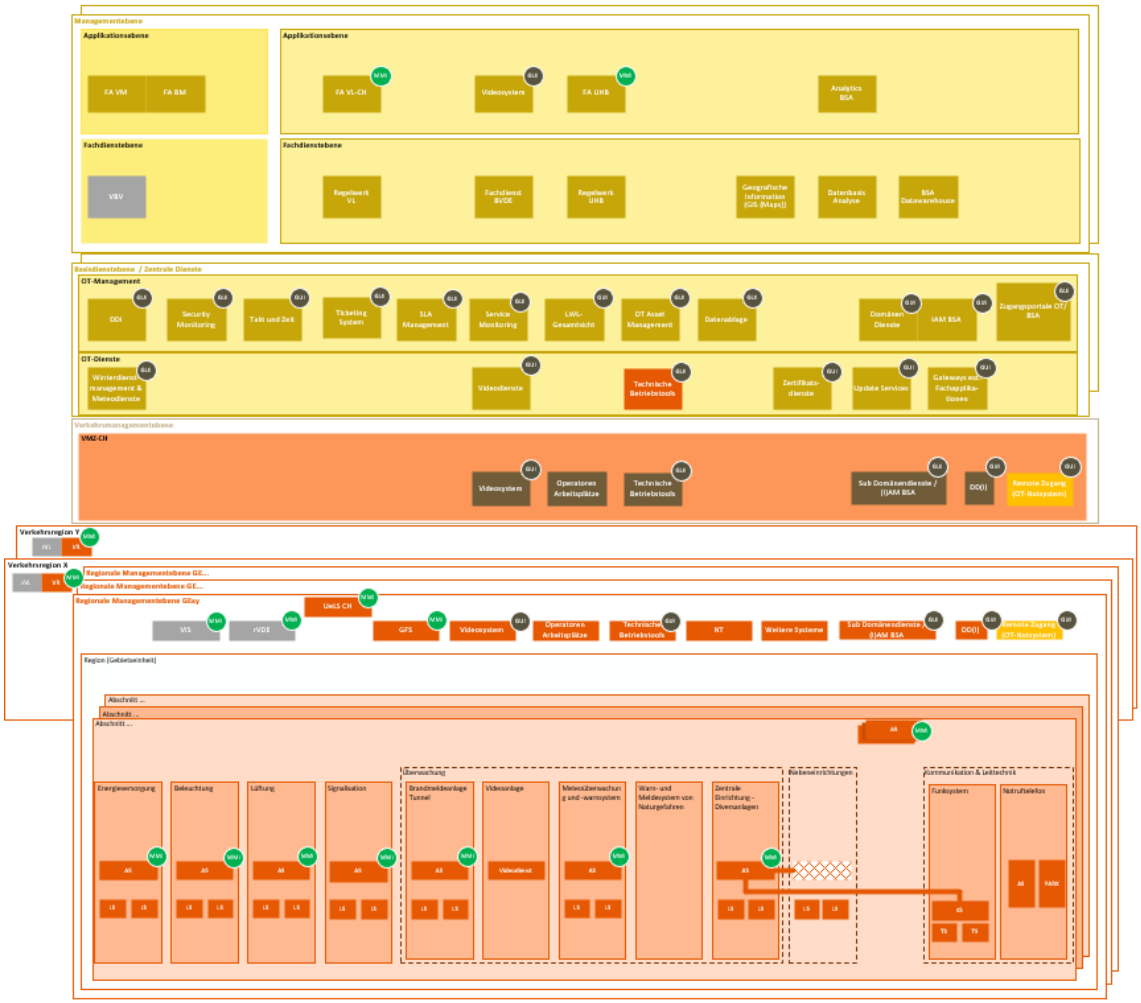


Figure IV.7: Architecture SA-CH avec MMI/GUI

V Applications technologiques

V.1 Applications technologiques pour un tube

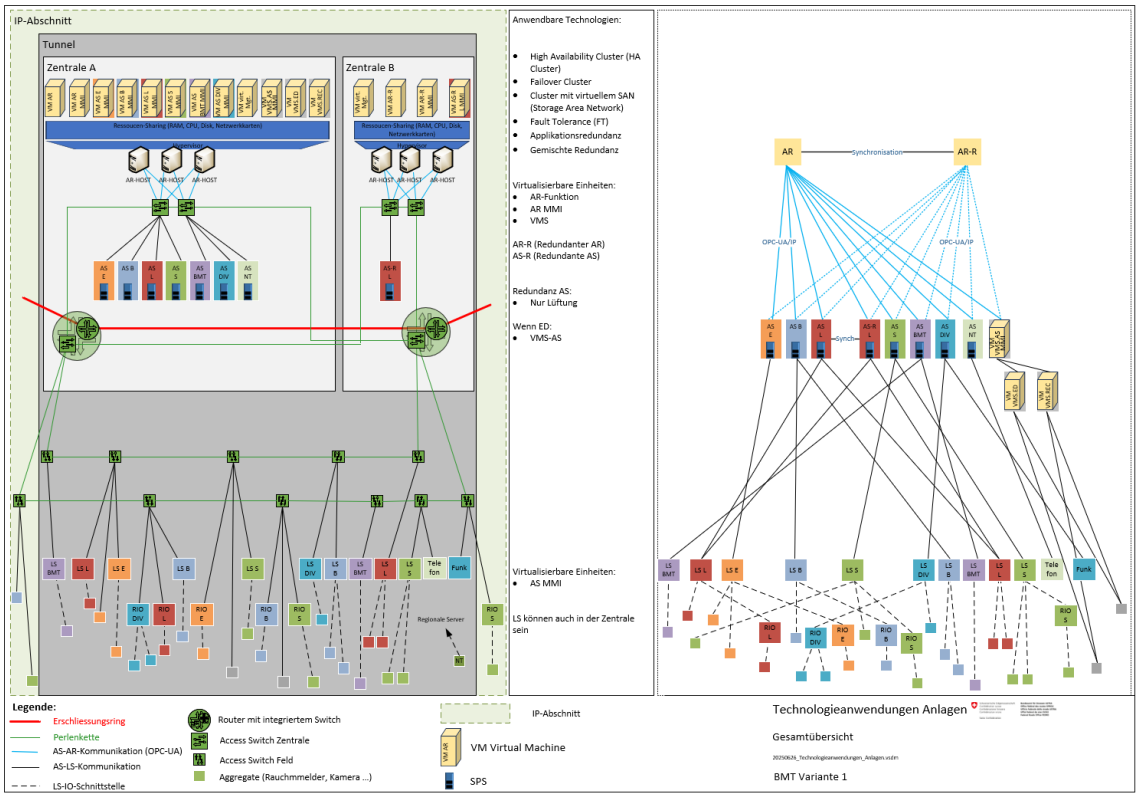


Figure V.8 : Vue d'ensemble - applications technologiques pour un tube - variante 1

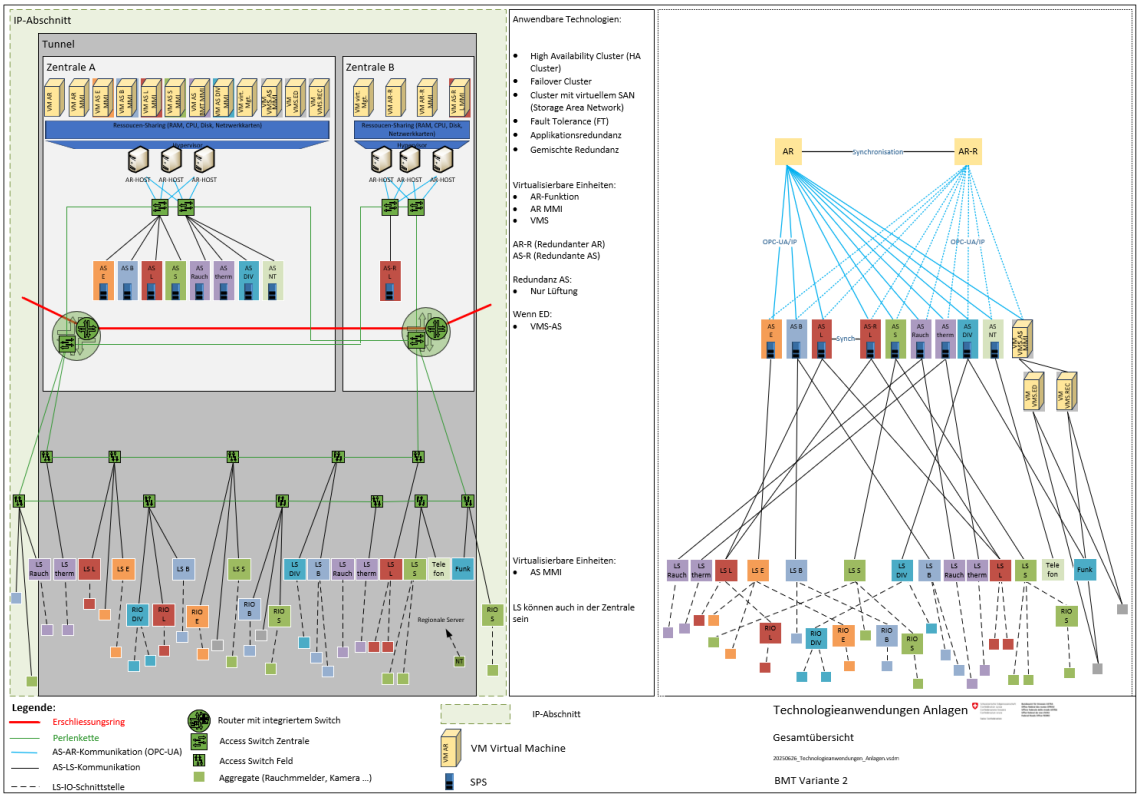


Figure V.9 : Vue d'ensemble - applications technologiques pour un tube - variante 2

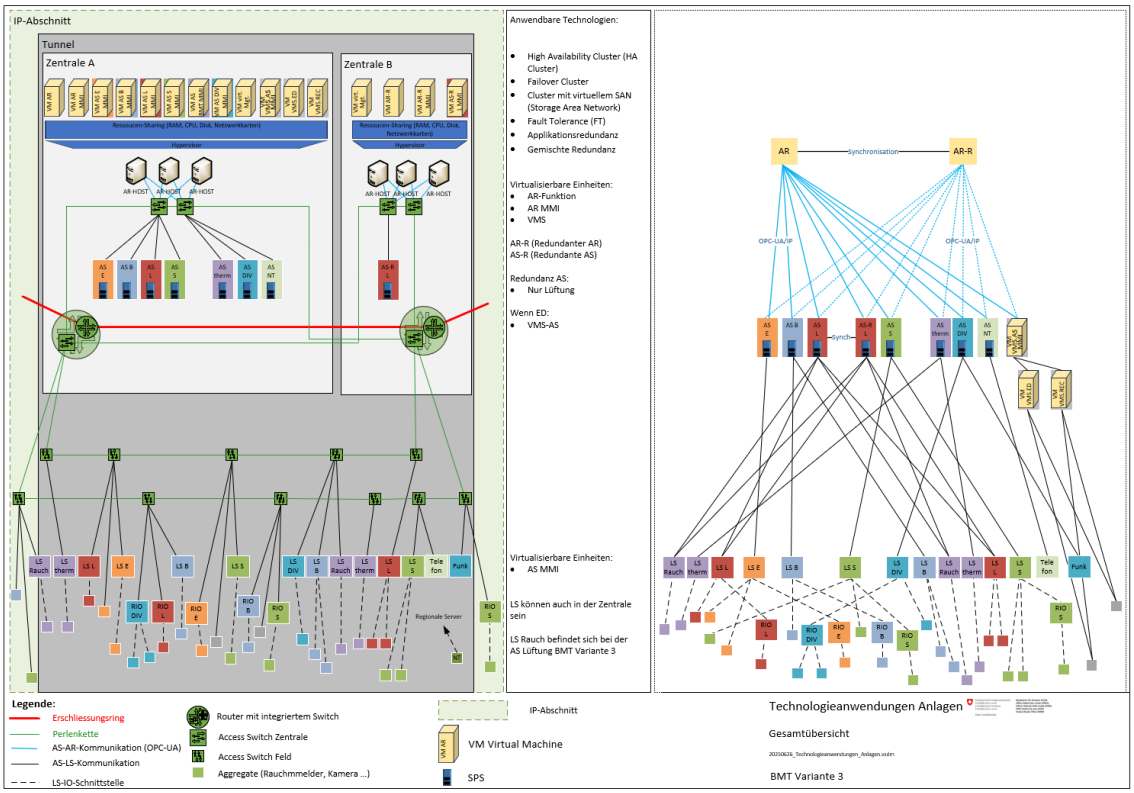


Figure V.10 : Vue d'ensemble - applications technologiques pour un tube - variante 3

V.2 Applications technologiques pour deux tubes

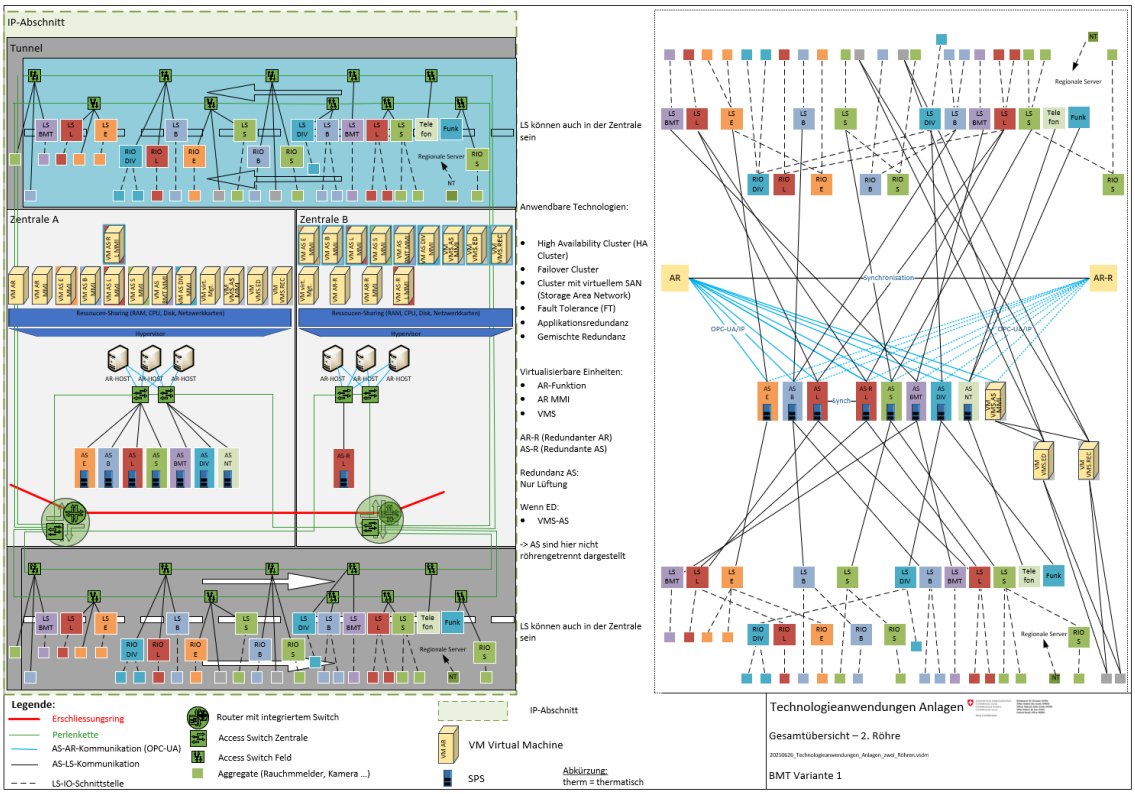


Figure V.11 : Vue d'ensemble - applications technologiques pour deux tubes - variante 1

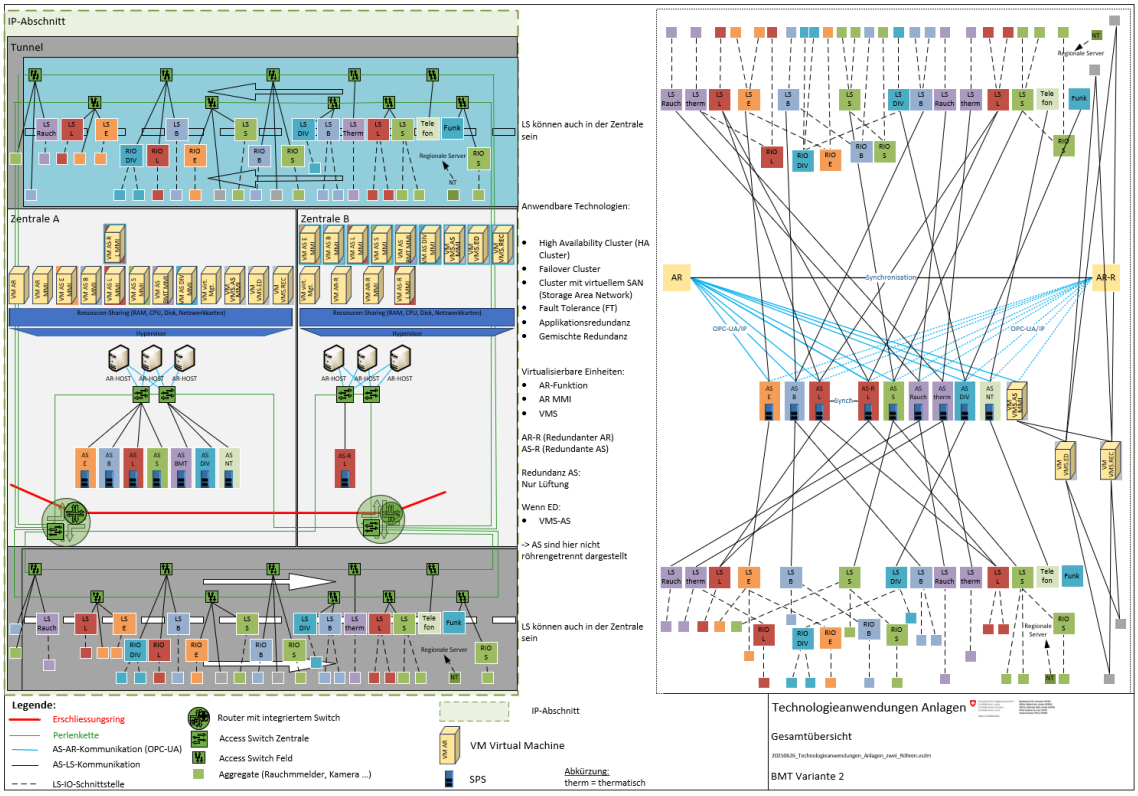


Figure V.12 : Vue d'ensemble - applications technologiques pour deux tubes - variante 2

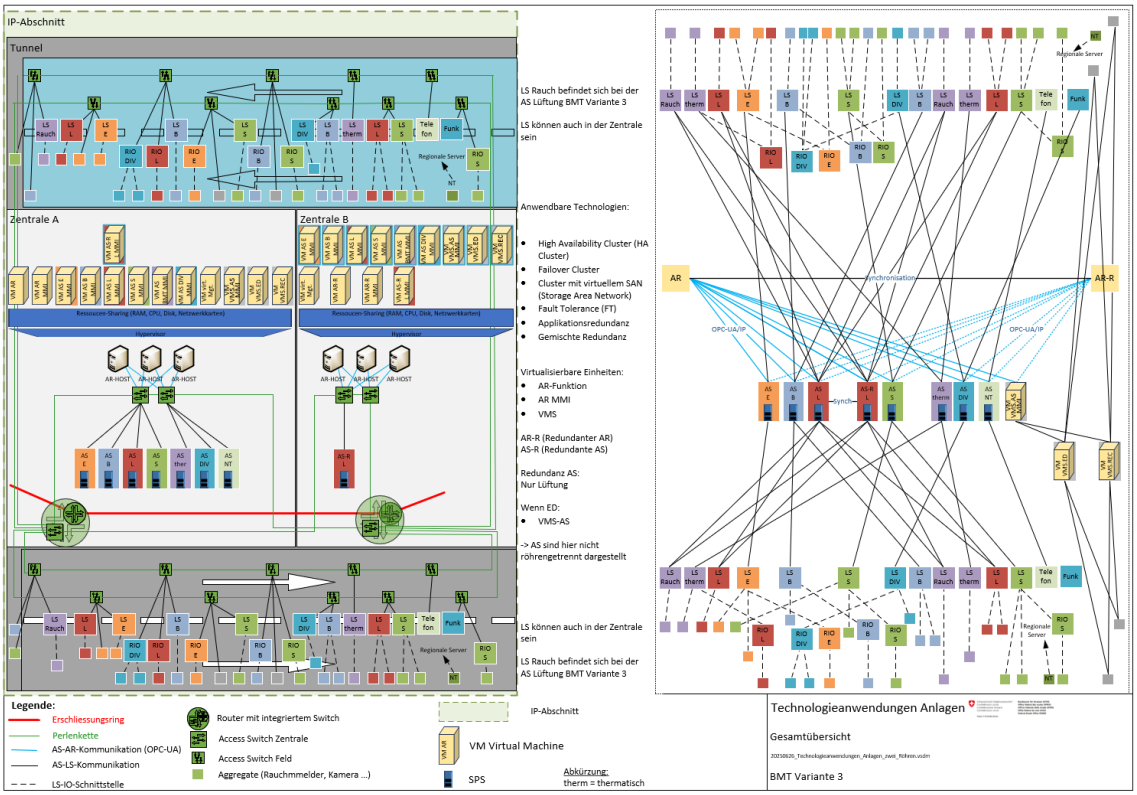


Figure V.13 : Vue d'ensemble - applications technologiques pour deux tubes - variante 3

V.3 Exemple de calcul des ressources matérielles

V.3.1 Matériel hôte (serveur)

Le dimensionnement du matériel informatique dépend de l'utilisation effective. Le choix du matériel informatique doit être adapté aux besoins spécifiques de chaque site, qu'il s'agisse de locaux techniques OT ou de centrales techniques. Les principales ressources matérielles sont indiquées ci-après (liste non exhaustive) :

- Processeurs (attention, impact possible sur la licence logicielle) ;
- Mémoire de travail (RAM) ;
- Disques durs ;
- Cartes réseau.

Deux unités doivent en principe être disponibles dans chaque cas. Ce chiffre peut être multiplié selon l'usage prévu.

Les exigences minimales sont communiquées par les fabricants des systèmes d'exploitation ainsi que par les éditeurs d'applications ou de bases de données.

Exemple

Pour définir les exigences relatives au matériel informatique, les données suivantes peuvent être appliquées comme base approximative :

1. Collecter les besoins de toutes les VM ;
2. Ajouter une réserve de 50 % pour les VM supplémentaires ou les pics de charge ponctuels ;
3. Totaliser les besoins au niveau du matériel HOST ;
4. Soustraire 25 % des capacités théoriquement disponibles pour obtenir une indication approximative de la ressource effectivement utilisable.

Exemple de RAM

Tableau V.14 : Exemple de RAM

Besoin	**RAM [Go]**	
Système d'exploitation HOST	24	
VM 1	24	
VM 2	48	
VM 3	48	
VM 3	96	
Total	240	
Réserve 50 %	120	
Total avec réserve	360	Par matériel HOST
Plus 25 %	90	Majoration afin d'atteindre la capacité effectivement utilisable
Besoin total corrigé	**450**	Par matériel informatique (valeur de commande)
Moins 25 %	**-90**	Déduction des pertes système
Capacité effective totale	**360**	Valeur effective utilisable

Exemple avec des clusters de 2 et 3 HOSTS

Tableau V.15 : Exemple avec des clusters de 2 et 3 HOSTS

Calcul RAM [Go]	**Total**	**Total cluster de 2**	**Total cluster de 3**
Système d'exploitation HOST	16	32	48
Système d'exploitation Guest (VM 1)	16	32	48
Système d'exploitation Guest (VM 2)	16	32	48
Système d'exploitation Guest (VM 3)	16	32	48
Application (VM 1)	32	64	96
Application (VM 2)	24	48	72
Base de données (VM 3)	64	128	192
Total	184	368	552
Réserve (défaillance d'un serveur matériel)		368	552
Réserve (maintenance d'un serveur matériel)		368	552
Total pour la couverture en cas de panne d'un serveur		**736**	**1104**
Total pour la couverture en cas de maintenance d'un serveur		**736**	**1104**
Total pour la couverture en cas de panne d'un serveur et de maintenance de l'autre			**1656**

Ce tableau ne tient pas compte du tableau V.164. Une majoration de 25 % doit ainsi être ajoutée pour la valeur de commande effective.

V.3.2 Infrastructure de stockage des données (storage)

Le dimensionnement du matériel de stockage des données dépend de l'utilisation effective. Le choix du matériel de stockage doit être adapté aux besoins spécifiques de chaque site (locaux OT, locaux techniques, etc.). Les principales bases de calcul sont indiquées ci-après (liste non exhaustive) :

- Disques durs ;
- Cartes réseau.

La capacité effectivement utilisable d'un disque dur ou d'un support de stockage se calcule (approximativement) comme suit.

Tableau V.17 : Capacité effectivement utilisable d'un disque dur ou d'un support de stockage

Exemple de calcul du stockage [Go]	**Total par disque dur**	**Total avec 3 disques durs**	**Remarque**
Capacité brute	300	900	
Capacité brute (env. 90 %) (utilisation propre du système déduite)	270	810	

Les gains de capacité liés à l'utilisation de la déduplication et de la compression dépendent du fabricant.

À partir de la capacité brute	Capacité utilisable :	
Nette en RAID 0	810	Aucune tolérance aux défaillances
Nette en RAID 1	270	Tolérance à 2 disques défectueux
Nette en RAID 5	540	Tolérance à 1 disque défectueux
Nette en RAID 10 et en RAID 6 et 60	-	Au moins 4 disques

Glossaire

Begriff/Abkürzung	Terme/abréviation	Signification
(BSA) Abschnitt	section (EES)	Section logique pour les EES, pas le tronçon physique
(Netzwerk-) Segment	segment (de réseau)	Segments selon ASTRA 83040 (généralement réalisés par des VLAN)
(Netzwerk-)Zone	zone (de réseau)	selon la NSP de la Confédération Si003 (séparées par la PEZ)
(Teil-)Anlage	(partie d')installation	Limité au sens strict des définitions de l'AKS
Access-Bereich	niveau accès	Structure L2, mettant à disposition les interfaces d'accès (Userport) aux équipements terminaux
ABX	ABX	Abréviation d'Abraxas
AD	AD	Active Directory
AI	AI	Intelligence artificielle (en anglais : *Artificial Intelligence*)
AKS-CH	AKS-CH	Structure et désignation des équipements d'exploitation et de sécurité
AR	AR	Serveur de gestion section
AS	AS	Commande d'installation
Ausrüstung/Gerät	équipement	Toute sorte d'équipement actif dans un contexte large des EES (même sans connexion au réseau IP EES)
AWL	liste d'instructions	Liste d'instructions
B	B	Éclairage
Backbone/BB	backbone/BB	Interconnexion nationale de tous les réseaux partiels mise à disposition par la Confédération (L3 par l'OFIT, transmission par la BAC), dorsale
BD (Basisdienste)	BD (services de base)	Services de base pour le réseau (outil IPAM, DNS, sources d'horloge/temps, …) pour l'ensemble du réseau IP EES
BIT/ KdoCy	OFIT/ cdmt Cyber	Office fédéral de l'informatique et de la télécommunication / commandement Cyber
BLI	BLI	Clignotant
BLZ	BLZ	Centre de contrôle d'exploitation
BM	BM	Gestion de chantier
BMT	BMT	Installation de détection incendie tunnel (BMT)
BSA	EES	Équipements d'exploitation et de sécurité
BSA-Abschnitt	section EES	Section de route nationale gérée par un serveur de gestion de section
BSA-Region	région EES	Région définie de façon spécifique pour l'installation, dans laquelle il existe une commande régionale supérieure
BVDE	BVDE	Acquisition des données d'exploitation et de trafic
CA	CA	Organisme de certification (de l'anglais « *Certificate Authority* »)
CAB	CAB	Change Advisory Board
KAM	KAM	Caméra
Client/Host	client/hôte	Termes génériques TIC, sans signification particulière pour les EES, utilisation dans le contexte des protocoles standardisés
DDI	DDI	Outil de gestion DNS, DHCP et adresses IP
DHCP	DHCP	Dynamic Host Configuration Protocol
Dienst	service	Terme générique qui s'applique tant aux services métier qu'aux services de base. Les services implémentent les logiques d'accès et de traitement, mais ne disposent pas d'une interface utilisateur.
DIV	DIV	Système de gestion installation diverses
DNS	DNS	Le « système de noms de domaine » (de l'anglais « *Domain Name System* ») est l'un des services les plus importants pour

Begriff/Abkürzung	Terme/abréviation	Signification
		de nombreux réseaux IP. Sa tâche principale est de répondre à des requêtes de résolution de noms. Il fonctionne comme un service de renseignement téléphonique.
Domäne	domaine	Le domaine sert à organiser ou à regrouper des éléments. Ses utilisations à l'OFROU sont les suivantes : Espace de noms : espace dans lequel les identités sont univoques, c'est-à-dire que chaque ressource possède sa propre identité. Domaine de fonctions : regroupement de différentes fonctions. Domaine métier : regroupement de différents services métier. Domaine de processus : regroupement de différents processus.
DWH	DWH	Datawarehouse
DWW	SVI	Signalisation variable des itinéraires
E	E	Approvisionnement en énergie
ELZ	ELZ	Centrale d'intervention (de la police).
Endgerät	équipement terminal	Toute sorte d'équipement connecté à un Userport du réseau IP EES
F/Filiale	F/filiale	Filiale (cinq structures régionales de l'OFROU)
FA	AM	Application métier
FAT	FAT	Factory Acceptance Test
FBS	bloc fonctionnel	Bloc fonctionnel
FE	FE	Installation radio
Firewall	firewall/pare-feu	Un pare-feu est un système de sécurité qui protège un réseau informatique ou un équipement individuel contre les accès indésirables au réseau.
FIT	FIT	Factory Integration Test
FT	FT	Fault Tolerance
FUB	FUB	La Base d'aide au commandement s'appelle désormais commandement Cyber
G	G	Signal de vitesse
GE	UT	Unité territoriale (11 structures supracantonales, exploitant leur réseau IP EES UT)
GFS	GFS	Installation de surveillance et d'alarmes météo (également appelée système de détection du verglas)
GHGW	HV-AD	harmonisation des vitesses et avertissement de danger
GIS	GIS	Système d'information géographique
GS	GS	Signal de danger
GUI	GUI	Interface utilisateur graphique (de l'anglais « *Graphical User Interface* »), ici équivalente à l'interface MMI, mais sans adaptations spécifiques à l'OFROU, soit conforme au standard du fabricant)
HA Cluster	HA Cluster	Hight Availability Cluster
HCI	HCI	Hyperconverged Infrastructure
IAM BSA	IAM BSA	Identity Management System BSA
IKT	IKT	Technologies de l'information et de la communication
IP	IP	Internet Protocol (protocole internet)
IP-Abschnitt	IP-section	Section logique pour les cascades
IPAM	IPAM	IP Address Management
IPC	IPC	Ordinateur industriel
IP-Netz BSA GE GE Abschnitt BD VMZ Backbone	réseau IP EES UT UT section BD VMZ Backbone	Le réseau IP pour les équipements d'exploitation et de sécurité des routes nationales comprenant les éléments suivants (réseaux partiels) : - 11 réseaux IP EES UT - la dorsale nationale (réseau IP EES Backbone) - le réseau de la VMZ-CH

Begriff/Abkürzung	Terme/abréviation	Signification
		- les connexions aux centres de calcul EES) - les connexions aux BD (services de base du réseau IP EES)
ISBO	ISBO	Délégué à la sécurité informatique de l'unité organisationnelle
ISO	ISO	Information Security Officer
KoP	schéma à contacts	Schéma des contacts
L	L	Ventilation
LDAP	LDAP	Lightweight Directory Access Protocol
Leitebene	niveau gestion	Voir niveau processus
Leitsystem	système de gestion	Sert aux opérateurs pour la surveillance et la commande des installations
Leittechnik	système de commande/gestion	Fonctions et composants servant à la surveillance et à la commande des installations.
LS	LS	Commande locale (abréviation de l'allemand « *Lokalsteuerung* »)
LWL	LWL	Fibre optique
Management-Ebene (auch Mgmt-Ebene oder ME)	niveau management (ou ME)	Niveau gestion central supérieur
MDT	MDT	Temps moyen d'indisponibilité (en anglais : *mean down time*)
MMI	MMI	Man Machine Interface (avec toutefois des adaptations spéficiques à l'OFROU)
Monitoring	monitoring	Surveillance et visualisation des fonctions techniques des installations et des systèmes.
MTTR	MTTR	Temps moyen de réparation (en anglais : *mean time to repair*)
N	N	Installation auxiliaire
NCSC -> BACS	NCSC -> BACS	National Cyber Security Centre (Centre national pour la cybersécurité)-> Office fédéral de la cybersécurité
NMS	NMS	Network Management System
NT	NT	Téléphone de secours
NTP	NTP	Network Time Protocol
OBNB	OBNB	Réseau optique des autorités fédérales
OPC UA	OPC UA	Open Platform Communications Unified Architecture
OPC	OPC	Open Platform Communications
OT	OT	Operational Technology (OT)
OTTR	OTTR	Local technique OT (Operational Technology)
PEP	PEP	Éléments de sécurité / Point d'application des règles (Policy Enforcement Point)
PEZ	PEZ	zone de sécurité située en amont qui permet l'accès de l'extérieur dans des conditions moins rigoureuses que les zones intérieures situées en aval avec des exigences de protection plus élevées (de l'anglais « *Policy Enforcement Zone* »). En dehors de l'administration fédérale, cela correspond à une DMZ (zone démilitarisée).
PKI	PKI	Infrastructure à clé publique (de l'anglais « *Public Key Infrastructure* ». Système permettant l'émission, la gestion et la vérification de certificats numériques, utilisés pour la communication sécurisée et l'authentification sur Internet. La PKI sert à chiffrer des données, à créer des signatures numériques et à vérifier l'identité des utilisateurs, appareils ou services.
Portalrot	Feu rouge au portail	Feu rouge à l'entrée d'un tunnel (portail)
Prozessleitebene	niveau processus	Terme issu de la technique de contrôle-commande : à ce niveau, la surveillance et l'utilisation de toutes les commandes de l'installation et la commande supérieure (interdomaines du tunnel) ont lieu à l'intérieur d'une section au moyen d'un AR.
PUN	R-BAU	Réaffectation de la bande d'arrêt d'urgence

Begriff/Abkürzung	Terme/abréviation	Signification
RaDo	DoRa	Dosage de rampe
RTSP	RTSP	Real-Time Streaming Protocol
rVDE	rVDE	Acquisition régionale des données de trafic
rVL	rVL	Gestion régionale du trafic
RZ(-BSA)	RZ(-BSA)	Centre de calcul EES
S	S	Signalisation
SA-CH	SA-CH	Architecture système Suisse
SAN	SAN	Storage Area Network
SAP	SAP	Service Access Point : dans le réseau IP EES, les « points d'accès au service » sont en général des ports physiques d'un commutateur ou d'un routeur.
SAT	SAT	Site Acceptance Test – Réception sur le site d'installation final, c'est-à-dire chez le client
Server	serveur	Termes génériques TIC, sans signification particulière pour les EES), utilisation dans le contexte des protocoles standardisés
Service	service	Voir Service
SISTO	SISTO	Galeries de sécurité
SIT	SIT	Site Integration Test
SLA	SLA	BSA (Accord de niveau de service)
SMS	SMS	Security Management System
SNMP	SNMP	Simple Network Management Protocol
SOC	SOC	Security Operation Center
SPS	SPS	Automate programmable industriel
SSO	SSO	Single Sign On (authentification unique)
ST	ST	Texte structuré
SVM	GTL	Gestion du trafic lourd
U	U	Installations de surveillance
UeLS-CH	UeLS-CH	Système de gestion générale suisse (ancien BL)
UHB	UHB	Entretien et exploitation
ÜV-LW		Interdiction de dépassement pour les poids lourds
VBV	VBV	Vehicle-By-Vehicle
VDV	VDV	Le centre de données trafic désigne le réseau de communication destiné au transport des données de gestion du trafic
VIS	VIS	Système d'information routière
VL	VL	Gestion du trafic
VL-CH	VL-CH	Gestion du trafic suisse
Videosystem	Système vidéo	Système de traitement des informations vidéo
Videodienst	Service vidéo	Service de traitement des informations vidéo
VM	VM	Machines virtuelles
VM AP	VM AP	Application de machines virtuelles
VMS.AS	VMS.AS	Toutes les consignes envoyées par l'AR, y compris les fonctions et les commandes de contrôle, sont exécutées dans VMS.AS.
VMS.ED	VMS.ED	Module d'analyse vidéo côté serveur et de détection d'événements pour installation vidéo
VMS.MGT GE	VMS.MGT GE	Composant central du VMS – stocke la configuration du système de surveillance et gère l'authentification des utilisateurs, les droits d'accès, les règles, etc.
VMS.OPA/ DEC	VMS.OPA/ DEC	Clients destinés aux utilisateurs du VMS
VMS.REC	VMS.REC	Le serveur d'enregistrement gère les communications, les enregistrements et les messages d'état des appareils connectés

Begriff/Abkürzung	Terme/abréviation	Signification
		(caméras, encodeurs vidéo et audio, modules E/S et sources de métadonnées)
VMS.MGT RZ/ARC/OPA	VMS.MGT RZ/ARC/OPA	Partie du système vidéo VIDEO-CH destinée à l'archivage de séquences d'images associées à des événements
VMS.MOS/MGT BD/AN/TCA/TCN/	VMS.MOS/MGT BD/AN/TCA/TCN/	Partie du système vidéo VIDEO-CH destinée à l'archivage de séquences d'images associées à des événements
VMS-M/TNN/TDSG	VMS-M/TNN/TDSG	Partie du système vidéo VIDEO-CH destinée à l'archivage de séquences d'images associées à des événements
VMZ-CH	VMZ-CH	Centrale nationale suisse de gestion du trafic
VR	VR	Calculateur de trafic, à la fois RM VM et solution intermédiaire IVM
VSAN	VSAN	Virtual Storage Area Network
WTA	PMV	Panneau à messages variables
WWW	WWW	Panneau de direction à indications variables
ZSC	ZSC	Contrôleur de comptage de trafic

Bibliographie

Instructions, directives et documentations de l'OFROU

[1] Office fédéral des routes OFROU, **« Pilotage des équipements d'exploitation et de sécurité : rôles, tâches et exigences pour les interfaces utilisateurs »**, *instructions ASTRA 73002*, www.astra.admin.ch.

[2] Office fédéral des routes OFROU, « **OT Security Governance** », *instructions ASTRA 73006*, www.astra.admin.ch.

[3] Office fédéral des routes OFROU, **« Installations vidéo »**, *directive ASTRA 13005,* www.astra.admin.ch.

[4] Office fédéral des routes OFROU, **« Centrales techniques EES »**, *directive ASTRA 13009,* www.astra.admin.ch.

[5] Office fédéral des routes OFROU, **« Contrôles et tests des EES »**, *directive ASTRA 13028*, www.astra.admin.ch.

[6] Office fédéral des routes OFROU, **« OT Security »**, *Richtlinie ASTRA 13030*, www.astra.admin.ch.

[7] Office fédéral des routes OFROU, **« Ingénierie des données EES »**, *directive ASTRA 13032*, www.astra.admin.ch.

[8] Office fédéral des routes OFROU, **« Définition OPC-UA »**, *directive ASTRA 13034*, www.astra.admin.ch.

[9] Office fédéral des routes OFROU, « **Réseau IP EES** », *directive ASTRA 13040*, www.astra.admin.ch.

[10] Office fédéral des routes OFROU, **« Gestion du trafic sur les routes nationales (directive-cadre VM-NS) »**, *directive 15003*, www.astra.admin.ch.

[11] Office fédéral des routes OFROU, **« Logique de régulation du trafic - Exigences fonctionnelles minimales pour la conception et l'exploitation des systèmes de gestion du trafic en vue de fluidifier le trafic »**, *directive ASTRA 15019*, www.astra.admin.ch.

[12] Office fédéral des routes OFROU, **« Network Security Policy Réseau IP EES (NSP Réseau IP EES) »**, *documentation ASTRA 83042*, www.astra.admin.ch.

[13] Office fédéral des routes OFROU, **« Distribution de temps et d'horloge dans le réseau IP EES »**, *directive ASTRA 83044*, www.astra.admin.ch.

[14] Office fédéral des routes OFROU, **« Style Guide EES – partie 0 : Bases générales »**, *documentation ASTRA 83050*, www.astra.admin.ch.

[15] Office fédéral des routes OFROU, **« Style Guide EES – partie 2 : Niveau systèmes de tronçons »**, *documentation ASTRA 83052*, www.astra.admin.ch.

[16] Office fédéral des routes OFROU, **« Style Guide EES – partie 3 : Bibliothèque des symboles »**, *documentation ASTRA 83053*, www.astra.admin.ch.

[17] Office fédéral des routes OFROU, **« Système de gestion générale (UeLS-CH) - Exigences de base »**, *directive ASTRA 83054*, www.astra.admin.ch.

[18] Office fédéral des routes OFROU, **« Système de gestion générale (UeLS-CH) - Guide d'utilisation de la documentation ASTRA 83054 pour la planification, la mise en soumission, l'exécution et l'intégration EES »**, *documentation ASTRA 83055*, www.astra.admin.ch.

[19] Office fédéral des routes OFROU, « **IAM BSA** », *documentation ASTRA 83056*, www.astra.admin.ch.

[20] Office fédéral des routes OFROU, **« Exigences minimales en matière d'exploitation - tronçon et tunnels »**, *documentation ASTRA 86053*, www.astra.admin.ch.

[21] Office fédéral des routes OFROU, **« Téléphone de secours »**, *manuel technique ASTRA 23001- 11650,* www.astra.admin.ch.

Liste des modifications

Édition	Version	Date	Modifications
2026	2.11	20.10.2026	• Modifications dans les chapitres 4.2.3, 4.12.5. • Diverses adaptations formelles, corrections mineures du texte. • Publication de la version française.
2026	2.10	20.01.2026	• Complément pour les installations de gestion du trafic. • Diverses adaptations formelles, corrections mineures du texte. • Bibliographie révisée.
2024	2.00	28.01.2025	• Entrée en vigueur de l'édition 2025 V2.00, version entièrement remaniée.
2016	1.70	01.11.2017	• Publication de la version française. • Harmonisation réalisée en parallèle de la traduction en français.
2016	1.60	01.01.2016	• Entrée en vigueur de l'édition 2016. • Document complet : Réseau d'infrastructure EES (ISN) remplacé par réseau de communication EES. • Document complet : Numérotation des exigences (Rx) supprimée. • Chapitre 2.5 Migration ajouté. • Légende de la figure 2.3 ajoutée. • Figures 3.1 et 5.1 simplifiées. • Chapitre 7 révisé. • Bibliographie révisée. • Diverses adaptations formelles, corrections rédactionnelles.
2015	1.50	01.10.2015	• Point de données du catalogue technique, annexe II, supprimé
2015	1.40	01.06.2015	• Point de données du catalogue technique, annexe II, ajouté • Diverses corrections apportées
2015	1.10	01.01.2015	• Entrée en vigueur de l'édition 2015