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 2016 V1.70*
*ASTRA 13031*

# Impressum

**Auteurs / groupe de travail**

| | |
|---|---|
| Roth Felix | (OFROU N-ST, président) |
| Schnetz Jean-Paul | (OFROU N-ST) |
| Dedes Carolin | (AWK Group AG, Zürich) |
| Münger Rolf | (AWK Group AG, Zürich) |
| Mirolo Mario | (IM Maggia Engineering SA) |
| Mutti Christian | (IM Maggia Engineering SA) |

**Groupe d'accompagnement**

| | |
|---|---|
| Joseph Cédric | (OFROU N-SFS) |
| Fuchs Eugen | (OFROU N-ST) |
| Glanzmann Markus | (OFROU N-ST) |
| Eisenlohr Markus | (OFROU I-FU) |
| Hofer Günter | (OFROU I-FU) |
| Maltese Paolo | (OFROU I-FU) |
| Schneider Thomas | (OFROU I-F4) |
| Wyss Martin | (OFROU I-B) |

**Traduction** (version originale en allemand)
Services linguistiques OFROU (traduction française et traduction italienne)

**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.astra.admin.ch.

© ASTRA 2016
Reproduction à usage non commercial autorisée avec indication de la source.

# Avant-propos

Les équipements d'exploitation et de sécurité (EES) contribuent considérablement à la sécurité des tunnels et des tronçons à ciel ouvert du réseau suisse des routes nationales. Ils jouent également un rôle important dans la gestion du trafic, en tentant de préserver un trafic aussi fluide que possible.

Afin qu'ils puissent être exploités efficacement, ces équipements disposent d'un système de gestion et de commande permettant le pilotage et la surveillance à distance, indépendamment de leur emplacement.

La présente directive décrit la structure pour un système de gestion et de commande des EES, uniforme et cohérent, pour l'ensemble du territoire suisse. Elle forme une base solide et modulaire qui permet à l'OFROU de poursuivre l'extension des EES, mais aussi de réaliser de nouvelles solutions dans le domaine de la gestion du trafic ou de la connectivité entre les véhicules et les infrastructures routières.

**Office fédéral des routes**

Jürg Röthlisberger
Directeur

# Table des matières

**Impressum** ..... **2**
**Avant-propos** ..... **3**

**1 Introduction** ..... **7**
1.1 Objectif de la directive ..... 7
1.2 Champ d'application ..... 7
1.3 Destinataires ..... 7
1.4 Entrée en vigueur et modifications ..... 7

**2 Principes de base** ..... **8**
2.1 Objectifs de l'architecture ..... 8
2.2 Aperçu général ..... 8
2.2.1 Niveau gestion ..... 9
2.2.2 Réseau de communication des équipements d'exploitation et de sécurité des routes nationales ..... 9
2.2.3 Niveau des systèmes de tronçons ..... 9
2.2.4 Groupes d'utilisateurs ..... 9
2.2.5 Systèmes périphériques de la Confédération ..... 9
2.2.6 Systèmes périphériques de tiers ..... 10
2.3 Exigences générales posées à l'architecture système ..... 10
2.4 Périmètre d'influence ..... 10
2.4.1 Niveau gestion ..... 10
2.4.2 Région EES ..... 10
2.4.3 Section EES ..... 11
2.5 Migration ..... 12

**3 Architecture du niveau gestion** ..... **13**
3.1 Aperçu ..... 13
3.2 Interfaces utilisateurs ..... 13
3.3 Applications métiers (FA) ..... 14
3.4 Services ..... 14
3.4.1 Services métiers ..... 15
3.4.2 Services de base ..... 15
3.5 Collecte et administration des données ..... 15
3.6 Représentation d'état (image-situation) ..... 15
3.7 Communication entre le niveau gestion et les systèmes de tronçons ..... 15
3.8 Exigences du niveau gestion ..... 16
3.8.1 Rôles ..... 16
3.8.2 Services (services métiers et services de base) ..... 16
3.8.3 Collecte et administration des données ..... 16
3.8.4 Journalisation ..... 16
3.8.5 Connexion de systèmes externes ..... 16
3.8.6 Surveillance et commande d'installations ..... 17
3.8.7 Infrastructure IT ..... 17

**4 Réseau de communication des EES** ..... **18**

**5 Architecture du niveau des systèmes de tronçons** ..... **19**
5.1 Aperçu des systèmes de tronçons ..... 19
5.1.1 Vue fonctionnelle du niveau des systèmes de tronçons ..... 19
5.1.2 Niveau région EES ..... 19
5.1.3 Niveau section EES ..... 20
5.1.4 Niveau installation ..... 20
5.1.5 Interdomaines ..... 20

5.2 Exigences générales des systèmes de tronçons ... 21
5.2.1 Autonomie ... 21
5.2.2 Interdomaines et liaisons entre installations ... 21
5.2.3 Visualisation / possibilité de commandes ... 21
5.2.4 Protocoles de communication / interfaces ... 22
5.3 Constitution des systèmes de tronçons ... 23
5.3.1 Niveau région EES ... 23
5.3.2 Niveau section EES ... 25
5.3.3 Fonctionnalités du système de gestion AR ... 26
5.3.4 Fonctionnalités des commandes d'installation (AS) et des commandes locales (LS). 26
5.4 Gestion des données ... 27
5.5 Modes d'exploitation et de fonctionnement ... 27
5.6 Echange de données ... 28
5.6.1 Les systèmes au niveau région EES ... 28
5.6.2 Serveur de gestion section ... 28
5.6.3 Commande d'installation / commande locale ... 29

**6 Disponibilité ... 30**
6.1 Eléments de base ... 30
6.2 Exigences posées aux valeurs MTBF ... 30

**7 Migration ... 32**

**Annexes ... 33**

**Glossaire ... 39**
**Bibliographie ... 42**
**Liste des modifications ... 43**

# 1 Introduction

## 1.1 Objectif de la directive

Cette directive standardise la mise en place du système de gestion des équipements d'exploitation et de sécurité (EES) sur les routes nationales, et définit les normes pour leur planification, leur conception et leur réalisation.

Elle décrit la mise en œuvre des systèmes de gestion et de leurs interfaces.

## 1.2 Champ d'application

La directive a un caractère contraignant pour la planification, la conception, la réalisation et l'exploitation des systèmes de gestion de tous les équipements d'exploitation et de sécurité (EES) des routes nationales.

## 1.3 Destinataires

La directive s'adresse :

- aux chefs de projets de l'OFROU ;
- aux spécialistes EES de l'OFROU ;
- aux spécialistes EES des unités territoriales ;
- aux bureaux d'ingénieurs et aux entreprises ;
- aux planificateurs/projeteurs, constructeur et exploitants opérant dans les domaines de l'entretien courant, de la maintenance et du suivi des EES.

## 1.4 Entrée en vigueur et modifications

Ce document entre en vigueur le 01.01.2015. La « Liste des modifications » se trouve à la page 43.

# 2 Principes de base

L'architecture système décrit les systèmes de gestion et de commande des installations (hardware et software), les systèmes de tronçons (voir chap. 2.2.3) et le niveau gestion (voir chap. 2.2.1). Elle représente un modèle qui décrit les interdépendances entre les différents éléments ainsi que leurs propriétés et leurs fonctions.

Le présent chapitre expose les objectifs de l'architecture système, les exigences générales associées, et en donne un aperçu général. Par la suite, il définit les différents éléments de l'architecture système ainsi que d'autres systèmes périphériques attenants, et introduit les notions générales.

## 2.1 Objectifs de l'architecture

L'architecture système vise les objectifs suivants :

- L'architecture système possède une structure modulaire ;
- Les systèmes de gestion existants et décentralisés seront remplacés par un système de gestion unique ;
- Elle met à disposition des services centralisés, et utilise les services de l'Administration fédérale existants ;
- La communication entre les systèmes de tronçons et le niveau gestion s'effectue selon des standards usuels ;
- La connectivité à l'échelon suisse est garantie par un réseau de communication uniforme ;
- Les systèmes de gestion et de commande des EES ont une structure homogène pour l'ensemble du pays, c'est-à-dire que leur structure et, plus particulièrement, leurs interfaces obéissent à des conditions et à des règles uniformes ;
- Les systèmes périphériques de tiers[1] (hors du domaine de validité de l'architecture système) sont reliés par des interfaces standardisées ;
- L'architecture système est ouverte à l'intégration et à l'utilisation de nouvelles technologies ;
- Les systèmes de gestion et de commande des EES sont spécifiés de manière à ce qu'il puisse y avoir concurrence entre différents fournisseurs.

## 2.2 Aperçu général

L'architecture système est récapitulée à la fig. 2.1. La fig. 2.2 présente sa topologie ainsi qu'un niveau plus détaillé des systèmes de tronçons. Ce chapitre propose une présentation succincte des différents éléments : les détails figurent aux chap. 3 et 4.

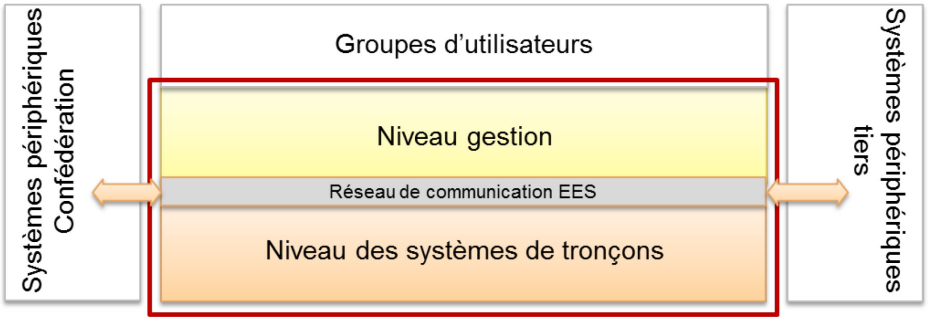


*Fig. 2.1 Aperçu général de l'architecture des systèmes de gestion et de commande EES (dans le cadre rouge), y.c. systèmes périphériques et groupes d'utilisateurs.*

[1] cantonaux, etc., voir aussi chapitre 2.2.6.

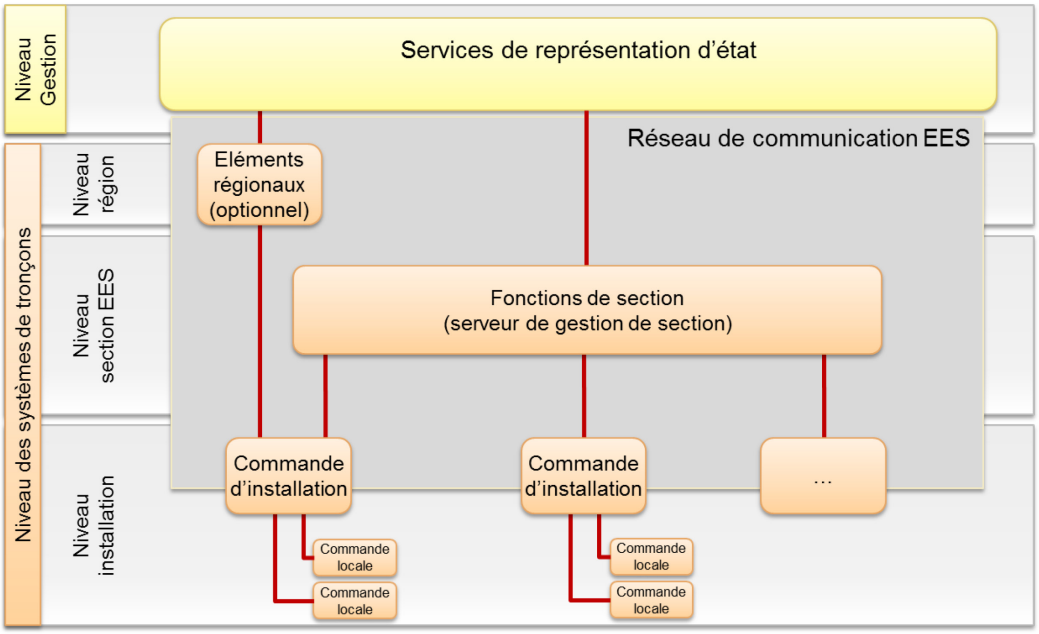


*Fig. 2.2 Topologie de l'architecture des systèmes de gestion et de commande EES*

### 2.2.1 Niveau gestion

Le niveau gestion est le niveau qui englobe les fonctionnalités des anciens systèmes de gestion (UeLS), les applications de la centrale de gestion du trafic (VMZ-CH) ainsi que d'autres applications (comme GEWI TIC, FA BM). Les utilisateurs reçoivent chacun une application métier spécifique pour les rôles « gestion du trafic », « police », « exploitation et entretien » et « gestion des chantiers ». Il existe en Suisse un niveau gestion pour l'ensemble des EES.

### 2.2.2 Réseau de communication des équipements d'exploitation et de sécurité des routes nationales

Le réseau de communication des EES prend en charge la communication entre les systèmes de tronçons et le niveau gestion. Il supporte la transmission des données, des signaux vidéo et de la voix. Les réseaux destinés à la communication à l'intérieur des systèmes de tronçons sont réalisés sous la forme de sous-réseaux.

### 2.2.3 Niveau des systèmes de tronçons

Le niveau des systèmes de tronçons (STS) décrit les contraintes des installations avec leurs systèmes locaux de commande (niveaux processus et terrain) ainsi que leurs connexions au réseau de communication.

### 2.2.4 Groupes d'utilisateurs

Un groupe d'utilisateurs se compose de plusieurs utilisateurs ayant le même rôle (voir [2]). Le niveau gestion met à disposition des utilisateurs des applications dotées d'interfaces utilisateurs. Pour chaque rôle principal, il existe une application dédiée appelée « application métier ». Elle garantit aux utilisateurs, en fonction du rôle attribué, des droits d'accès définis aux différentes ressources des EES (données, états d'installations, ordres de commande).

### 2.2.5 Systèmes périphériques de la Confédération

L'architecture système prévoit des interfaces avec lesquelles des systèmes périphériques internes de la Confédération peuvent être reliés aux EES.

### 2.2.6 Systèmes périphériques de tiers

Des systèmes périphériques externes (p. ex. systèmes de tronçons ou systèmes de gestion tiers) peuvent être reliés via les interfaces prévues dans l'architecture système. L'architecture autorise la liaison de systèmes périphériques externes, en particulier :

- liaison de systèmes de tronçons cantonaux au niveau gestion de l'OFROU ;
- transmission de données des systèmes de tronçons de l'OFROU à un système de gestion cantonal.

## 2.3 Exigences générales posées à l'architecture système

Ce chapitre définit les exigences générales pour l'architecture.

- Il existe un niveau gestion central uniforme. Il permet de piloter ou de surveiller tous les systèmes de tronçons à partir d'applications métiers ;
- La surveillance de tous les éléments (hardware et software du niveau gestion ainsi que tous les éléments des systèmes de tronçons) est possible via une infrastructure de surveillance centrale ;
- Pour relier les systèmes de tronçons de l'OFROU au niveau gestion, il est indispensable que les interfaces respectent les prescriptions et les critères uniformes des documents applicables et que les outils mis à disposition soient utilisés pour valider la solution implémentée ;
- L'autonomie des différents niveaux doit être garantie (pas de dépendance vis-à-vis de niveaux supérieurs) ;
- L'architecture système ainsi que les éléments des systèmes de gestion et de commande des EES sont conçus de telle sorte qu'ils puissent être réalisés par plusieurs fournisseurs.
- Le mode d'affichage utilisé sur les postes de travail est calqué sur le navigateur afin qu'il ne soit pas nécessaire de développer, d'exploiter et d'entretenir un logiciel client (client software) spécifique ;
- Les accès aux EES se font exclusivement par des accès sécurisés, bien définis.
- Un accès à distance doit être possible à tous les niveaux à des fins de support et d'entretien ;
- Il faut tenir compte des périmètres des unités territoriales pour régler les attributions concernant l'exploitation des installations.

## 2.4 Périmètre d'influence

Les paragraphes suivants décrivent les principes applicables aux périmètres d'influence géographiques du niveau gestion ainsi que ceux des systèmes de tronçons (sections EES et régions EES).

### 2.4.1 Niveau gestion

Le niveau gestion est le niveau supérieur de gestion centralisé, pour l'ensemble de la Suisse. Dans les applications métiers, un périmètre d'influence géographique défini, peut être assigné à certains utilisateurs, compte tenu de leurs rôles.

### 2.4.2 Région EES

Certaines fonctions (p. ex. harmonisation des vitesses) concernent plusieurs sections. Elles sont alors réunies en une région EES dépassant le cadre d'une section (description des éléments régionaux, voir fig. 2.3 et la tab. 5.3). La taille de la région EES varie suivant le type d'installation (voir fig. 2.3) et est fixée au moment de la conception de cette installation (chap. 5.3.1).

### 2.4.3 Section EES

Une section EES est un segment de route nationale qui forme une unité fonctionnellement fermée pour un équipement d'exploitation et de sécurité donné. Le serveur de gestion section prend en charge la surveillance et la gestion générale de la section EES ainsi que la liaison avec le niveau gestion. La section EES ne coïncide pas obligatoirement avec une section UPlaNS. En revanche, elle est identique pour toutes les installations (voir aussi fig. 2.3).

Les exceptions possibles (p. ex. signalisation) sont décrites au chapitre 5.3. Le périmètre d'une installation de signalisation peut couvrir plus d'une section EES.

La constitution de sections doit obéir aux règles suivantes :

- Une section EES est définie par la présence des EES (voir chap. 0). Elles disposent toujours d'un serveur de gestion section ;
- Un tunnel équipé de son propre serveur de gestion section, en vertu du processus décrit au chapitre 0, constitue une section EES propre (y. c. ses abords et d'éventuels tronçons à ciel ouvert) ;
- Un tunnel qui n'est pas équipé de son propre serveur de gestion section est attribué à une section EES et il est géré par le serveur de celle-ci. Cela peut aussi être le serveur de gestion section d'un autre tunnel (chevauchement d'installations) ;
- Un tronçon à ciel ouvert comportant des EES (p. ex. réaffectation de la bande d'arrêt d'urgence) peut également constituer une section EES :
- La longueur d'une section EES est dépendante des EES qui en font partie ;
- Certains actionneurs ou capteurs éloignés (p. ex. des signaux) n'entrent pas dans la détermination de l'étendue de la section EES. Comme tous les autres, ces actionneurs/capteurs sont reliés aux commandes de la section à laquelle ils sont rattachés, mais ils se trouvent ou peuvent se trouver géographiquement dans le périmètre d'une section voisine ;
- Une section EES peut être subdivisée en sous-section. Cela est particulièrement judicieux dans le cas des tunnels. Dans le cas d'installations dotées de commandes locales, tous les agrégats d'une sous-section sont commandés par une seule commande locale ;
- Ces sous-sections sont calquées sur les limites du périmètre de fourniture de l'énergie. Débranchements et pannes dans l'alimentation basse tension doivent soit toucher la sous-section entière où l'épargner complètement.

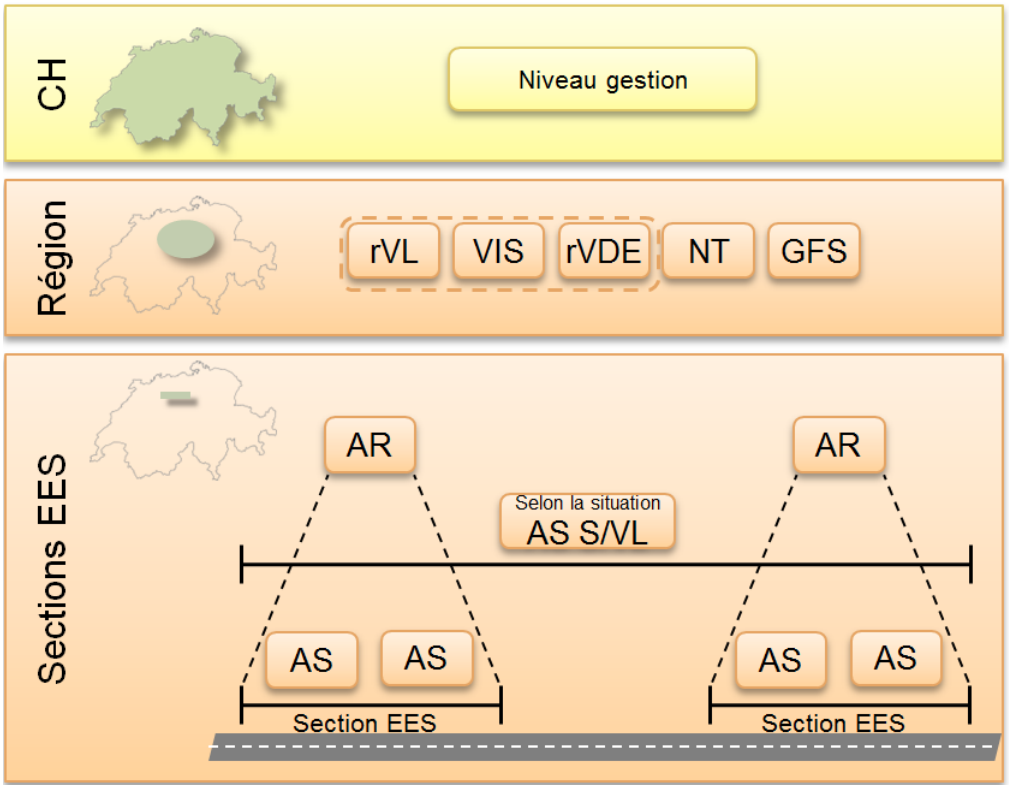


*Fig. 2.3 Etendue géographique des éléments de l'architecture système*

*Légende :*

*rVL Gestion régionale du trafic ;*
*VIS Système d'information trafic ;*
*rVDE Acquisition régionale de données de trafic ;*
*NT Installation des téléphones de secours ;*
*GFS Installation de surveillance et d'alarmes météo ;*
*AR Serveur de gestion section ;*
*AS Commande d'installation (hors installation signalisation) ;*
*AS S/VL Commande d'installation signalisation / calculateur trafic.*

Ces notions sont décrites au chapitre 5.3.

## 2.5 Migration

Le passage de l'architecture existante à la nouvelle architecture décrite est nommé migration. Cette transition nécessite une architecture, des procédures et des règles de migration. L'architecture de migration est exposée au chapitre 7. Le concept de migration décrit les démarches et les phases de la migration. 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.

# 3 Architecture du niveau gestion

## 3.1 Aperçu

Le niveau gestion contient tous les éléments nécessaires pour le déroulement des processus opérationnels de la gestion et de la sécurité du trafic, de l'exploitation et de l'entretien des EES ainsi que de la gestion des chantiers. Il réunit les applications métiers ainsi que tous les services indispensables au bon déroulement des tâches et au support des utilisateurs. Le niveau gestion est réalisé sous la forme d'une architecture orientée services (SOA). Il se subdivise en plusieurs couches, à savoir (voir fig. 3.1 et chap. 2.2.1) :

- les interfaces utilisateurs : uniformisation des interfaces homme – machine ;
- les applications métiers : cette couche contient les applications spécifiques aux rôles (comme soutien des processus opérationnels) ;
- les services métiers : composants représentant la logique métier ;
- les services de base : composants dotés de fonctionnalités de base nécessaires au fonctionnement des applications métiers ;
- la collecte et l'administration des données : collecte des données importantes des systèmes de tronçons sur une longue période ;
- la représentation d'état : composants servant à visualiser l'état réel actuel des systèmes de tronçons ;
- Communication : sert à l'échange des données entre le niveau gestion et le niveau des systèmes de tronçons.

Les chapitres suivants expliquent les fonctions principales des différentes couches.

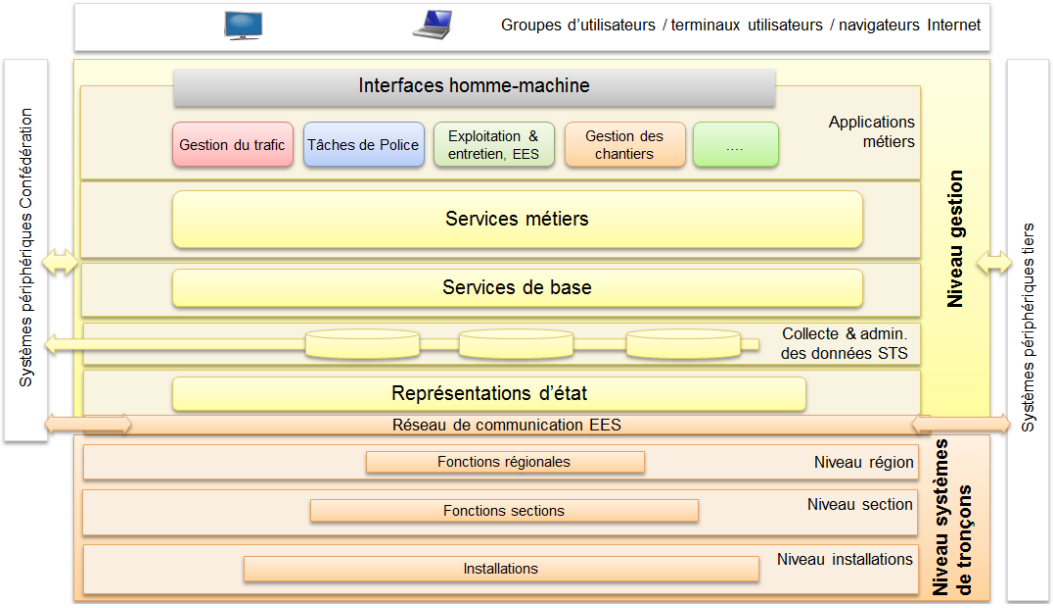


*Fig. 3.1 Eléments du niveau gestion*

## 3.2 Interfaces utilisateurs

Les interfaces utilisateurs des applications métiers doivent être élaborées conformément aux chartes IHM [5], [6] et aux instructions OFROU 73002 ([2]).

Elles doivent être réalisées de manière à ce que certaines parties puissent être réutilisées au besoin dans d'autres installations sans devoir les réimplémenter.

## 3.3 Applications métiers (FA)

Les applications métiers se situent au niveau supérieur de l'architecture. Elles supportent les processus opérationnels pour tous les utilisateurs impliqués. Pour cette raison, chaque application métier dispose d'une interface utilisateur et de la logique de commande qui en fait partie et qui active les services métiers ou services de base. Chaque utilisateur et chaque groupe d'utilisateurs ont des vues différentes dans une application métier, en fonction de leurs rôles et de leurs droits d'accès.

- Application métier Gestion du trafic (VM)

Cette application métier supporte la diffusion de l'information et la gestion de la circulation de manière à ce que le trafic soit aussi fluide que possible sur le réseau des routes nationales (transport de personnes et trafic lourd). Elle prend en considération la gestion d'événements, de chantiers, de manifestations, etc.

- Application métier Tâches de police (POL)

L'application métier FA POL supporte l'exécution de tâches de police sur le périmètre des routes nationales dans le cadre de l'alarme (engagement des services sanitaires et des pompiers) et de la première intervention (p. ex. fermeture d'un tunnel) lors d'événements. Elle supporte également la surveillance et la coordination des activités pendant la gestion des événements.

- Application métier Entretien et exploitation (UHB)

L'application métier FA UHB assiste les unités territoriales (UT) dans l'exploitation opérationnelle et l'entretien des EES. De même, elle permet aux UT de seconder les services d'urgences dans le traitement d'événements, via le pilotage des installations correspondantes.

- Application métier Gestion des chantiers (BM)

La gestion des chantiers assure une vision globale actualisée en permanence de tous les chantiers prévus ou en activité sur les routes nationales. Elle comporte des informations sur la durée d'un chantier ainsi que sur les restrictions de circulation sur le tronçon routier concerné. Elle met à disposition du service hivernal des informations météorologiques, des images vidéo et l'état du trafic.

Les applications métiers (FA POL, FA UHB, FA VM, FA BM) mettent à disposition les fonctions de commande et de surveillance des EES nécessaires pour accomplir ces tâches et assumer les responsabilités liées.

Les nouvelles applications métiers à élaborer doivent utiliser les services de base et métiers déjà développés et donc existants.

## 3.4 Services

« Service » est un terme générique qui s'applique tant aux services métiers qu'aux services de base. Un service est une unité fonctionnelle encapsulée comportant des interfaces définies. Celles-ci implémentent la logique d'accès et d'exploitation, mais ne disposent pas d'une interface utilisateur. L'OFROU administre ces services qui doivent être obligatoirement utilisés lors de nouveaux développements. En aucun cas ils ne doivent être dupliqués.

Les services sont groupés en domaines d'après leur appartenance fonctionnelle. S'ils sont utilisés entre différents domaines, ils doivent être activés via l'interface web-service.

### 3.4.1 Services métiers

Des fonctions du niveau gestion des EES spécifiques à l'OFROU sont réalisées dans les services métiers, p. ex. les prévisions de trafic ou des fonctions météorologiques.

Les fonctions et les données mises à disposition dans les services métiers couvrent en principe l'ensemble de la Suisse et doivent être disponibles pour toutes les applications métiers.

Les prévisions du trafic, la météo ou les interventions calendaires sont des exemples de domaines métiers.

### 3.4.2 Services de base

Les services de base mettent à disposition des fonctions générales, non spécifiques à l'OFROU, telles que la sauvegarde des données, la gestion des documents et la sécurité informatique.

## 3.5 Collecte et administration des données

Les services de la couche « collecte et administration des données » stockent les données de la représentation d'état, à long terme et comme historique, dans une base de données.

Le Tab. 3.2 met en évidence les types de données archivés dans le niveau gestion.

*Tab. 3.2 Archivage dans le niveau gestion*

| Type de donnée | Archivage dans le niveau gestion |
|---|---|
| Points de données | |
| Etat de l'installation et valeurs de mesure | Archivage de points de données sélectionnés |
| Etat du trafic | Archivage complet pendant une période limitée |
| Données de trafic | Archivage complet pendant une période limitée |
| Etat de la signalisation | Archivage d'un état résumé de la signalisation pendant une période limitée |
| Messages | Archivage de messages de haute priorité (alarmes) et de dérangements regroupés (journal) |
| Voix | - |
| Vidéo | - |
| Log-files | Archivage de log-files sélectionnés dans le niveau gestion |
| Sauvegarde des données (backup) | Le backup se fait sur l'infrastructure centrale comme partie du niveau gestion |

## 3.6 Représentation d'état (image-situation)

La couche « représentation d'état » du niveau gestion comprend les données des états actuels, obtenus via interface, de tous les systèmes de tronçons importants pour le niveau gestion (états du trafic, de la signalisation, valeurs de mesure des installations, notifications d'alarme et de dérangements, etc.).

Chaque service métier peut s'abonner à la représentation d'état pour obtenir une certaine quantité de données ; il reçoit au fur et à mesure les valeurs actuelles et assure ainsi l'actualisation des interfaces utilisateurs du niveau gestion.

## 3.7 Communication entre le niveau gestion et les systèmes de tronçons

Au niveau gestion on retrouve l'OPC-UA client. Il communique avec l'OPC-UA serveur du serveur de gestion section, de la rVL et de la VL au niveau tronçon.

Cette interface de points de données transmet les états et les commandes entre les niveaux.

## 3.8 Exigences du niveau gestion

Le niveau gestion doit assumer les exigences suivantes :

### 3.8.1 Rôles

- Il doit être possible de répartir les tâches de manière flexible entre les groupes d'utilisateurs en fonction du rôle, du mandat / de la tâche et du périmètre de compétences (géographique) (voir [2]). Le périmètre de compétences doit être défini par rapport aux limites d'une ou de plusieurs sections EES.
- Le périmètre de compétences géographique des applications métiers est configurable par groupe d'utilisateurs. Ces configurations, fixées préalablement, doivent être modifiables rapidement (p. ex. pour la commutation entre service de jour et service de nuit, pour la réalisation de redondances géographiques, etc.).
- Lors de changements d'ordre organisationnel (p. ex. changements dans la compétence territoriale de la police, concentration de plusieurs polices cantonales dans une seule centrale), la nouvelle répartition des rôles doit être rapidement adaptable, ceci en relation avec les limites d'une ou de plusieurs sections EES.

### 3.8.2 Services (services métiers et services de base)

- Les services, les composants technologiques prédéterminés par les services et les fonctionnalités mises à disposition doivent être obligatoirement intégrés dans le développement des applications et ne doivent en aucun cas, être remplacés par d'autres composants analogues (p. ex. service de signature électronique local) ou dupliqués. Les processus/sous-processus identiques des divers groupes d'utilisateurs sont supportés par les mêmes services métiers. Les applications métiers accèdent à des services métiers ou de base pour couvrir l'ensemble des tâches des groupes d'utilisateurs.
- Les interfaces de services sont à concevoir de manière à ce que plusieurs versions (suite à des modifications) des services puissent être exploitées parallèlement.

### 3.8.3 Collecte et administration des données

- Les données de base, les données archivées et les données variables sont centralisées, en dehors des applications métiers, et mis à disposition sous forme de services de données.
- L'architecture offre une solution de sauvegarde centralisée (backup) uniforme destinée à sécuriser et à archiver toutes les données EES propres à l'OFROU.
- Toutes les données doivent être horodatées.

### 3.8.4 Journalisation

- Pour assurer la traçabilité, toutes les données doivent être enregistrées. De plus amples détails figurent dans la directive ASTRA 13030 « Sécurité IT des systèmes de gestion et de commande des équipements d'exploitation et de sécurité ».

### 3.8.5 Connexion de systèmes externes

- Des installations externes peuvent être connectées aux applications métiers propres à l'OFROU, et, inversement, des installations de l'OFROU peuvent être connectées à des systèmes de gestion et de commande externes. A cet effet, l'interface définie dans l'architecture entre les systèmes de tronçons et le niveau gestion est à utiliser.
- L'architecture met à disposition des mécanismes qui permettent aux services de base ou métiers d'utiliser des services externes à l'architecture système (p. ex. Météosuisse ou Viasuisse) ou d'acquérir des données en provenance de sources externes.

### 3.8.6 Surveillance et commande d'installations

- Les applications métiers peuvent piloter les installations uniquement par le serveur de gestion section ou par les éléments régionaux et uniquement via l'interface des points de données. La logique de commande des installations est exclusivement implantée sur les commandes d'installations.
- Les interventions directes sur les installations peuvent être exécutées à partir du niveau gestion via l'interface utilisateur du serveur de gestion section.
- Le niveau gestion détermine au démarrage, quels sont les messages (dérangements, alarmes, etc.) dont il a besoin. La couche de transport garantit la livraison postérieure permanente.
- Les messages arrivant dans le cadre de la surveillance des installations ou du serveur de gestion section (dérangements, alarmes, valeurs de mesure, etc.) sont traités de manière appropriée par le niveau gestion et affichés chez l'utilisateur, conformément à son rôle. Le niveau gestion met à disposition des fonctions appropriées en vue du traitement des messages (quittance, archivage, etc.)

### 3.8.7 Infrastructure IT

- Un environnement de production, d'intégration et de formation doit être mis en place.
- Toutes les fonctionnalités des applications métiers doivent être disponibles pour l'instruction et les tests. Cependant, leur activation ne doit pas avoir d'effets sur les installations physiques (blocage des ordres de commande à partir du niveau gestion).
- L'infrastructure du niveau gestion est surveillée par le biais d'un monitorage. Le protocole prédéfini (SNMP) doit être utilisé.
- Le réseau de communication des EES doit être surveillé séparément.
- Les procédures de sécurité et l'IAM (identity and access management) définies sont à utiliser au niveau national selon la directive ASTRA 13030 « Sécurité IT des systèmes de gestion et de commande des équipements d'exploitation et de sécurité » ([3]).

# 4 Réseau de communication des EES

Le réseau de communication des EES constitue la couche de communication reliant les systèmes de tronçons entre eux et avec le niveau gestion.

Il contient des composants de réseau actifs pour l'ensemble des liaisons de communication suivantes :

- AR – niveau gestion, de façon similaire, rVL, VIS, rVDE, NT, GFS – niveau gestion ;
- AR – AS ;
- selon l'installation, AS – LS ;
- selon l'installation, les agrégats AS/LS ;
- la liaison aux installations externes s'effectue via une interface réseau définie.

Le réseau de communication des EES est envisagé comme un réseau ouvert qui comprend le réseau backbone suisse de la confédération ainsi que les réseaux locaux des unités territoriales. Ceux-ci forment un réseau commun global dans lequel, en principe, chaque composant actif peut communiquer avec les autres composants (des restrictions sous forme de sous-réseaux peuvent être configurées). Le réseau de communication de la section EES est toujours réalisé sous la forme d'un sous-réseau.

En principe, pour leur communication interne, les différentes installations ne disposent pas d'un réseau de communication propre, mais utilisent à cet effet les sous-réseaux. La ventilation et l'alarme incendie tunnel (BMT) peuvent être dotées chacune de leur propre réseau dans la section, compte tenu de leurs fonctions de sécurité.

# 5 Architecture du niveau des systèmes de tronçons

Ce chapitre décrit l'architecture de gestion et de commande des EES, au niveau des systèmes de tronçons.

## 5.1 Aperçu des systèmes de tronçons

Le niveau des systèmes de tronçons (voir fig. 5.1) comporte :

- niveau de la région EES ;
- niveau de la section EES ;
- niveau des installations jusqu'au niveau du terrain.

### 5.1.1 Vue fonctionnelle du niveau des systèmes de tronçons

L'architecture définit les systèmes de gestion et de commande des installations complètes ou partielles suivantes (selon la directive 13013 Structure et désignation des équipements d'exploitation et de sécurité (AKS-CH) [1]) :

- distribution d'énergie (E) ;
- éclairage (B) ;
- ventilation (L) ;
- signalisation y c. guidage du trafic (S / VL) et les fonctions régionales :
  - gestion régionale de trafic (rVL) ;
  - acquisition régionale de données de trafic (rVDE) ;
  - système d'informations trafic (VIS) ;
- installation de surveillance (U) :
  - installation de détection incendie tunnel (BMT) ;
  - installation vidéo (VTV) ;
  - système régional de l'installation de surveillance et d'alarmes météo (GFS) ;
  - système de gestion - installation Divers. (DI) ;
- communication et systèmes de gestion (KL) :
  - système de radiocommunication (FE) ;
  - Intercalation OUC/DAB+
  - téléphone de secours (NT) ;
- Installation auxiliaire (N).

  Elle définit également les systèmes de gestion et de commande du serveur de gestion section.

### 5.1.2 Niveau région EES

Le niveau de la région EES contient les systèmes nécessaires pour l'exécution des fonctions régionales et donc dépassant le cadre d'une section (plus de détails au chapitre 5.3.1).

- Commandes régionales pour les installations qui englobent plusieurs sections EES : emprise régionale. En font partie le guidage du trafic (rVL), l'acquisition régionale de données de trafic (rVDE), le système d'informations trafic (VIS), etc. (voir tab. 5.3). Ces installations servent, soit à exécuter des fonctions de coordination dans la région, soit à commander certains EES (p. ex. VDE ou PMV) qui ne sont attribués à aucune commande d'installation.

### 5.1.3 Niveau section EES

Le niveau section EES contient le serveur de gestion section (AR).

- Le serveur de gestion section est le trait d'union entre les installations et le niveau gestion pour la visualisation et la commande des EES. Il assume également le traitement des réflexes interdomaines des installations.

### 5.1.4 Niveau installation

Le niveau installation contient les commandes d'installation et les commandes locales :

- **La commande d'installation** : elle peut surveiller et commander des installations dans la section EES. Sur l'ensemble de la section EES, il est nécessaire de différencier les installations uniques aux tunnels (alarme incendie, ventilations, etc.) de celles se trouvent dans l'ensemble de la section EES (y c. tronçon à ciel ouvert).
- **La commande locale** sert à surveiller/piloter une partie d'une installation. Dans ce cas, il s'agit soit d'une zone (p. ex. commande d'une sous-section d'un tunnel) ou d'une fonction particulière (commande d'une fonction partielle des installations) ou des deux.

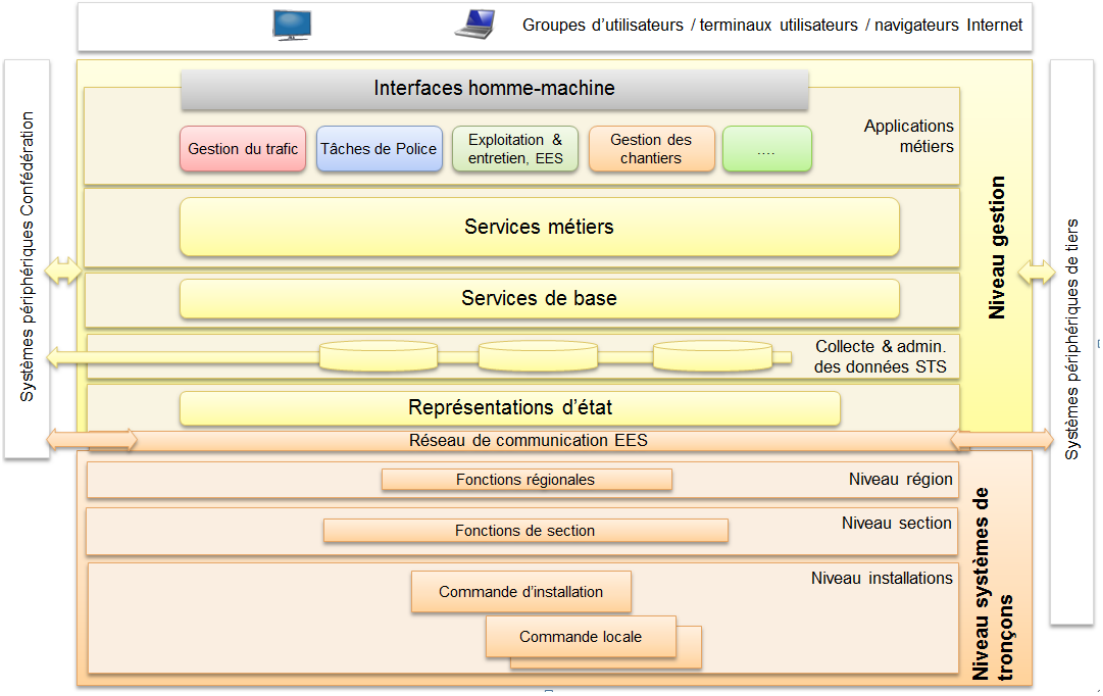


*Fig. 5.1 Eléments du niveau des systèmes de tronçons. Les actionneurs et les capteurs du niveau de terrain ne sont pas représentés dans la figure ni traités dans cette RiLi.*

### 5.1.5 Interdomaines

Deux types d'interdomaines sont utilisés. Il s'agit d'interdomaines automatiques, exécutés sans intervention manuelle.

- Type 1 : interdomaine critique pour la sécurité

Le type 1 est mis en œuvre lorsque l'interdomaine a la priorité la plus élevée et qu'il doit aussi fonctionner en cas de panne d'une liaison de communication et/ou d'un élément supérieur tel que l'AR.

- Type 2 : interdomaine non critique pour la sécurité

Le type 2 entre en jeu lorsque l'interdomaine n'est pas classé « type 1 critique pour la sécurité ».

## 5.2 Exigences générales des systèmes de tronçons

### 5.2.1 Autonomie

- Autonomie au niveau de chaque installation : les installations doivent être conçues pour fonctionner de manière autonome.
- Autonomie au niveau d'une section EES : la fonctionnalité des installations dans la section EES, commandes comprises, doit être entièrement assurée en cas de coupure du réseau de communication général (réseau de communication EES), de coupure ou de défaillance d'autres éléments et/ou fonctions en dehors de la section.

### 5.2.2 Interdomaines et liaisons entre installations

- Les interdomaines critiques pour la sécurité (interdomaines de type 1) sont transmis de manière redondante par des chemins différents. Une première voie de communication est physiquement câblée entre les AS de deux installations L'autre voie de communication transite par le serveur de gestion section. Du fait de la transmission redondante, l'autonomie est ainsi mieux assurée dans le tunnel (réalisation d'un état sûr) en cas de panne du serveur de gestion section AR.
- Les interdomaines non critiques pour la sécurité (interdomaines de type 2) passent par le serveur de gestion section, c'est-à-dire que la commande d'installation émettrice communique avec les commandes d'installation réceptrices via l'AR.
- Tous les interdomaines doivent pouvoir être inhibés pour les cas d'entretien et de tests. L'utilisateur doit pouvoir constater l'inhibition des interdomaines sur son interface.

### 5.2.3 Visualisation / possibilité de commandes

- La visualisation locale d'une section EES s'effectue sur le serveur de gestion section (AR). Toutes les représentations détaillées des installations sont générées et mémorisées sur l'AR. Les représentations des installations du calculateur trafic (VL ou rVL ou AS VL) sont générées et mémorisées sur le VL ou rVL.
- Les diverses installations possèdent une interface de commande locale (p. ex. Touch Panel) par laquelle les principales fonctions peuvent être commandées sur place (AS, LS).
- Les systèmes AR et VL doivent être accessibles pour chaque utilisateur autorisé, à partir de chaque emplacement central (centrale de tunnel, BLZ).
- Le système de gestion signalisation (VL) est relié à l'AR mais aussi directement au niveau gestion. La visualisation de l'installation (vue processus VL) s'obtient sur le VL et non pas sur l'AR.
- Un environnement de test doit permettre l'intégration de diverses installations sans déclenchement des interdomaines. Le mode test doit être indiqué à l'utilisateur.
- En mode de fonctionnement « Manuel » (voir 5.5), divers composants peuvent être directement pilotés, pour autant que la structure de l'installation le prévoie.
- Il est possible de prévoir un accès direct pour l'entretien à distance (voir directive ASTRA 13030 « Sécurité IT des systèmes de gestion et de commande des équipements d'exploitation et de sécurité »).
- Afin d'économiser ou de simplifier le remplacement du matériel, il est en principe possible de travailler avec des systèmes virtuels. Cependant, toutes les exigences doivent être respectées, en particulier pour l'autonomie.

### 5.2.4 Protocoles de communication / interfaces

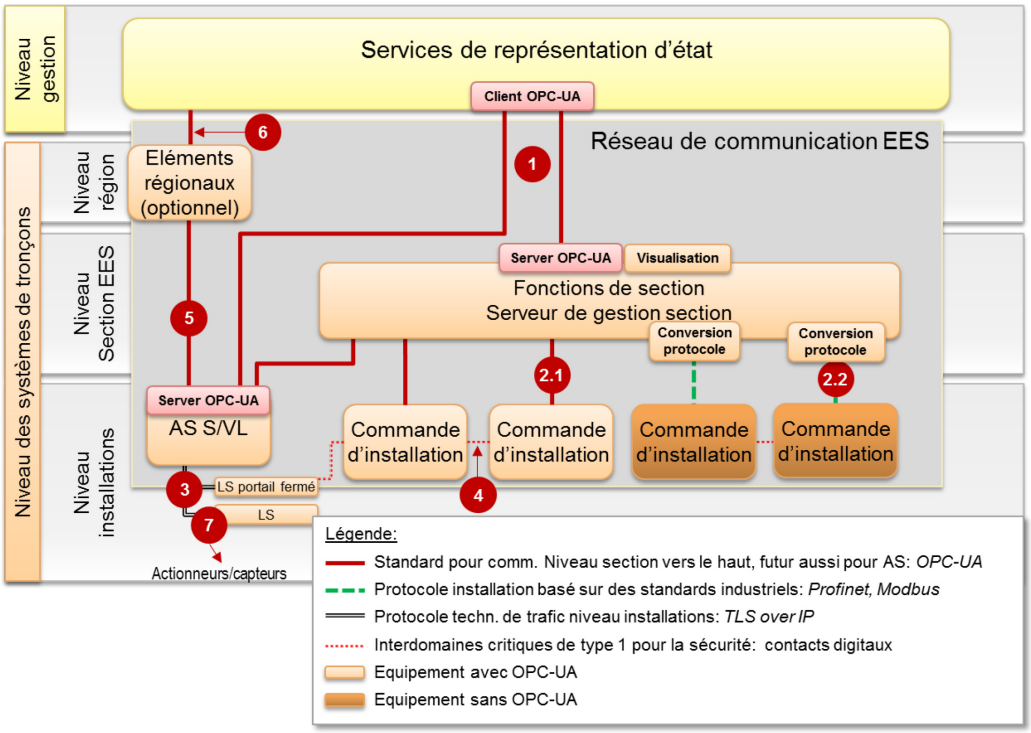


*Fig. 5.2 Vue d'ensemble des standards de protocoles entre les différents éléments*

**Principe de base**

La communication entre le niveau gestion et les éléments régionaux, entre le niveau gestion et les serveurs de gestion section ainsi qu'entre les serveurs de gestion section et les commandes d'installations est standardisée.

**Les standards de communication**

- Entre le niveau gestion et le niveau section EES (1), ainsi qu'entre le niveau gestion et les éléments régionaux (6), le protocole de communication OPC-UA est à utiliser.
- Le protocole OPC-UA est prévu, prioritairement, pour la communication de données entre le niveau section EES et le niveau des installations (2.1). Il en va de même pour la communication entre les éléments régionaux et le niveau des installations (5). Les protocoles de communication Profinet et Modbus TCP (2.2) sont également autorisés.
- Communication entre les commandes d'installation :
  - Interdomaine Type 1 : pour les interdomaines critiques pour la sécurité, il existe une voie de communication supplémentaire directe via contacts digitaux (4). Ce câblage physique peut se faire soit par câble, soit par bus. Les bus doivent pouvoir se surveiller eux-mêmes. Exemple : les valeurs sont échangées directement entre l'AS BMT et l'AS ventilation ;
  - Interdomnaine type 2 : la communication entre deux commandes d'installation transite par le serveur de gestion section au moyen de l'un des protocoles de communication cités ci-dessus.
- Pour les systèmes de tronçons de la signalisation, le TLS over IP (3) est utilisé depuis le VL jusqu'au niveau LS (voir [8]).
- Le mode de communication entre la commande d'installation et les commandes locales ainsi que la communication avec les actionneurs et les capteurs au niveau du terrain (7) n'est pas prescrit (communication interne de l'installation).
- Pour les données vidéo, les protocoles selon la directive ASTRA 13005 sont à appliquer.

## 5.3 Constitution des systèmes de tronçons

Ce chapitre propose une description plus précise des niveaux des systèmes de tronçons (hors niveau terrain) et de leur mise en œuvre.

### 5.3.1 Niveau région EES

Toutes les fonctions qui dépassent l'étendue d'une section EES mais qui sont limitées géographiquement à une région EES bien précise se trouvent au niveau de la région EES (fonctions de processus pour des installations dont l'étendue dépasse le cadre d'une section EES et qui, par conséquent, ont une emprise régionale).

Dans une région EES, les commandes régionales (voir *Fig. I.1*) ont une interface avec les éléments du niveau des installations qui leur sont subordonnées, de même qu'avec le niveau gestion.

Les éléments suivants sont prévus au niveau de la région EES :

- Gestion régionale de trafic (rVL)

Elle prend en charge la coordination de la gestion sur toute la section des AS S/VL subordonnée, lorsque de telles fonctions techniques de gestion du trafic sont nécessaires dans la région EES (p. ex. plans de feux à grande échelle ou harmonisation de la vitesse sur un espace plus vaste qu'une section ; elles sont généralement nécessaires dans les régions EES relativement complexes sur le plan de la gestion du trafic).

  - Coordination et commande des VL subordonnées (en particulier en cas de chevauchements et d'interdépendances) ;
  - Commutation de plans de feux combinés (standards) au moyen de la vue état final/état actuel ;
  - Réalisation d'interdépendances entre sections (signalisation de dangers).
  - Régime de vitesse avec programmation horaire en cas de panne de la saisie des données du trafic ;
  - Plans de feux généraux (80 km/h, risque de chaussée glissante, etc.).

- Système d'information trafic (VIS)

*Le système d'information sur le trafic commande et coordonne les PMV (panneaux à messages variables) et les WWW (panneaux de direction à indications variables) présents dans les sections EES sans calculateurs de trafic (VR).*

- Acquisition régionale de données de trafic (rVDE)

L'acquisition régionale de données de trafic rassemble et traite les données d'installations de saisie des données de trafic (VDE) que l'on trouve dans des sections EES sans calculateurs trafic (VR). Les installations VDE qui se trouvent dans le périmètre d'un calculateur trafic doivent être raccordées à celui-ci.

- Installation des téléphones de secours (NT)

L'installation centralisée de téléphone de secours dessert les téléphones de secours dans les différentes sections EES de la région.

- Le système de surveillance et d'alarmes météo (GFS)

Ce système analyse les données des différentes stations de mesure GFS d'une région EES.

Pour le niveau région des EES, les exigences suivantes s'appliquent :

- Les fonctions régionales de trafic (p. ex. gestion du trafic, saisie des données du trafic, commande des PMV) ne doivent pas obligatoirement être installées sur leur propre Hardware, mais peuvent être rassemblées dans un ordinateur.
- L'autonomie de ces systèmes doit être assurée.
- Les installations régionales disposent de leur propre visualisation / possibilité de commande.

Le tableau et la figure ci-après décrivent les types d'installations sur l'étendue de la région EES :

*Tab. 5.3 Les types d'installations au niveau de la région*

| Type d'installation | Eléments régionaux | Etendue de la région EES |
|---|---|---|
| Gestion régionale de trafic (rVL) | Guidage du trafic de la région EES | Territoire cohérent sous l'angle de la gestion du trafic. |
| Acquisition régionale des données de trafic (rVDE) | Saisie des données de trafic de la région EES | Unité territoriale |
| Système d'information trafic (VIS) | Panneaux à message variable (PMV) dans la région EES | Unité territoriale |
| Installation de surveillance et d'alarme météo (GFS) | Installations de surveillance et d'alarmes météo | Unité territoriale |
| Téléphones de secours (NT) | Installation centrale NT | Unité territoriale |

La figure suivante montre l'étendue possible des régions EES à titre d'exemple :

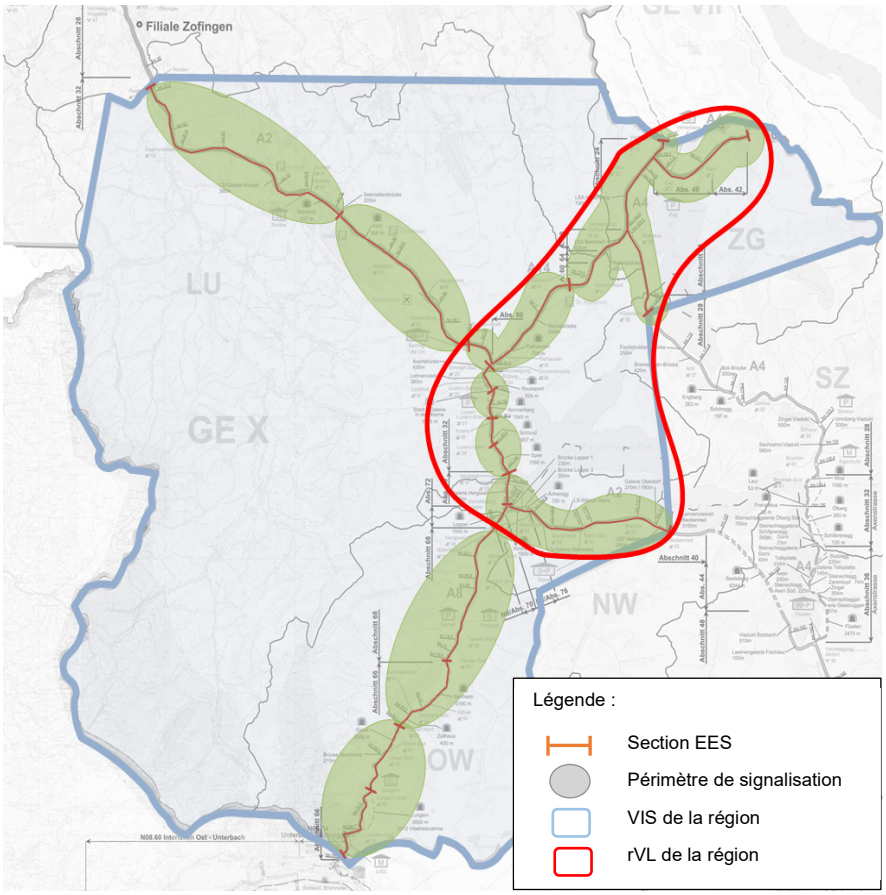


*Fig. 5.4 Représentation schématique du niveau de la région, de la zone d'influence de la signalisation et des sections EES à l'exemple de l'UT X*

### 5.3.2 Niveau section EES

L'architecture du niveau section EES est mise en évidence à la *Fig. I.1.* Le serveur de gestion section (AR) est positionné à ce niveau. Il dispose, d'une part, d'interfaces avec la totalité des commandes d'installation (AS) de la même section EES, et d'autre part, d'interfaces avec le niveau gestion. Il a donc en principe pour fonction de relier le niveau des installations à celui de gestion, de visualiser la section EES, et de mettre à disposition des vues des processus des installations.

Le niveau d'équipements dans un tunnel détermine la présence ou non d'un serveur de gestion section. Lorsque les EES d'un tunnel sont assainis, renouvelés (augmentation ou réduction), la procédure suivante s'applique (voir Fig. 5.5)

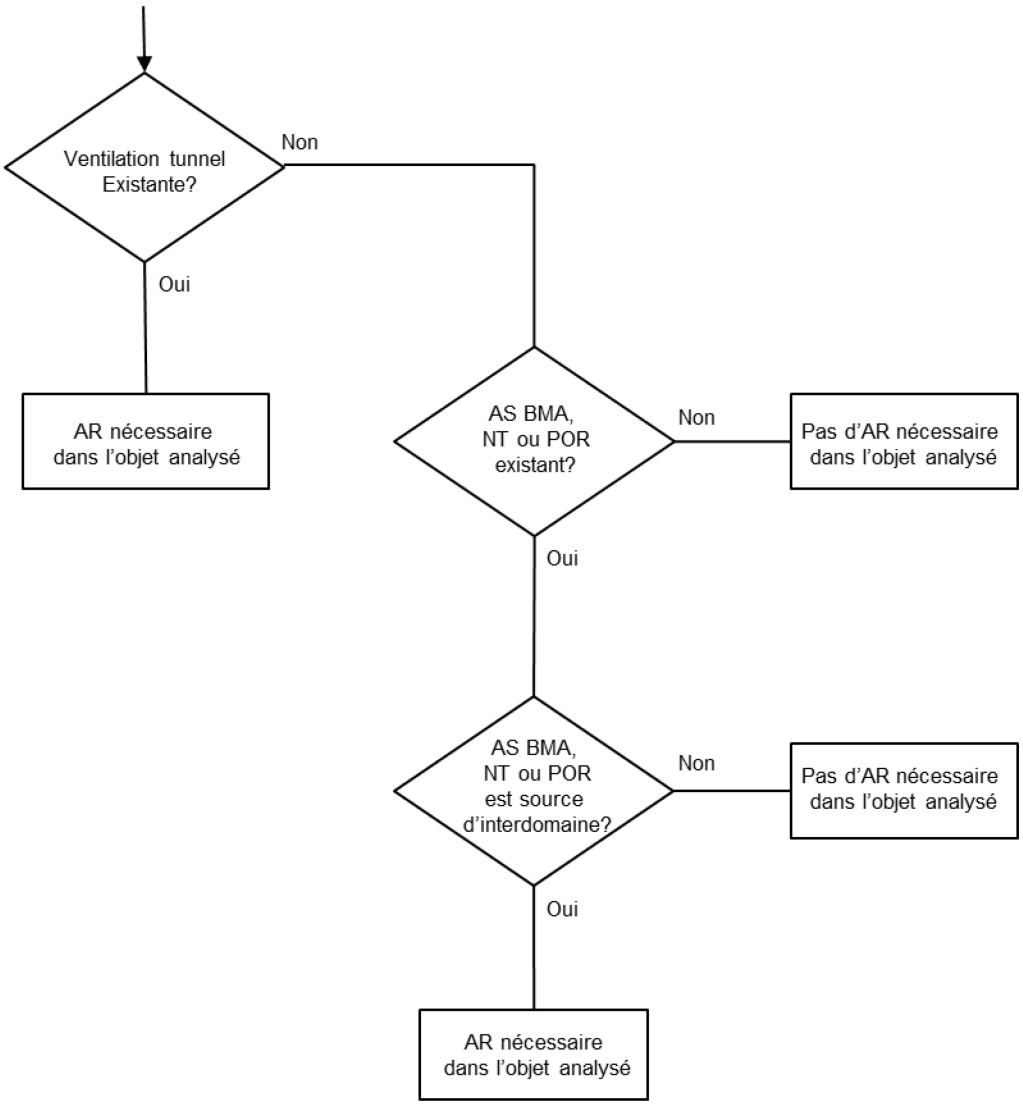


*Fig. 5.5 Diagramme de processus : décision relative à la nécessité d'un AR. Pour la définition des sources d'interdomaines, voir la matrice des interdomaines de l'OFROU*

### 5.3.3 Fonctionnalités du système de gestion AR

Le serveur de gestion section (AR) doit répondre aux exigences du chapitre 5.2 et aux exigences suivantes :

- Le serveur de gestion section doit visualiser et commander les installations de manière autonome[2] via une interface graphique ;
- Il assure la communication avec le niveau supérieur, en l'occurrence le niveau gestion, par une interface standardisée ;
- Il assure la communication avec les commandes des installations.
- Il traite les données des systèmes de tronçons (en revanche, les fonctions sont traitées dans les commandes des installations AS) ;
- Il traite des interdomaines de la section.

### 5.3.4 Fonctionnalités des commandes d'installation (AS) et des commandes locales (LS)

La commande d'installation (AS) met à disposition la logique de processus d'une installation. Elle contient les fonctions de commande principales de l'installation.

Les AS communiquent avec le serveur de gestion section ainsi qu'avec leurs propres commandes locales (LS).

Les principales fonctions d'une AS sont :

- contient la logique de l'installation (logique de processus) ;
- met à disposition une interface standardisée comportant les points de données prédéterminés pour la communication avec le serveur de gestion section (AR) ;
- génère des messages individuels ;
- communique avec les commandes locales (LS) ;
- communique avec les autres commandes d'installations (AS – AS) via l'AR, exception faite des interdomaines de type 1.

Les exigences suivantes s'appliquent aux AS et LS :

- Les commandes d'installation sont réalisées à l'aide d'automates programmables industriels (API) usuels du marché. Les API suivants sont admis :
  - API disposant d'un système d'exploitation propriétaire / firmware spécifique ;
  - API contenant un système d'exploitation répandu tel que Linux ou embedded-Windows, pour autant que ce dernier ne soit pas accessible via l'interface réseau. Les accès systèmes sur les API (p. ex. actualisation de la version du système d'exploitation / firmware) ne doivent être possibles que via des interfaces firmware propriétaires de l'API.
  - Les VL et les AS VTV peuvent aussi être réalisés sous la forme de PC industriels.
- Les commandes locales (LS) de la signalisation peuvent être réalisées sous la forme de modules de commande SM (Steuermodul) et de modules EAK (Eingabe-, Ausgabekonzentrator) conformément au standard TLS.
- Plusieurs unités fonctionnelles d'une installation (selon liste dans 5.1.1) peuvent fonctioner sur le même matériel (API) – une AS peut, par exemple, prendre en charge les fonctions d'une LS) – mais elles doivent être séparées sur le plan logique.
- L'indépendance fonctionnelle des installations et des parties d'installations entre elles doit être garantie (exemple : renouvellement d'installations dans le trafic sans effets négatifs sur la disponibilité du tunnel, sur l'entretien ou sur la défaillance d'une installation).
- Il est possible de regrouper plusieurs sections partielles d'une installation, si cela est techniquement judicieux (p. ex. BMT). Les limites extérieures de ces groupements doivent coïncider avec les limites de sections EES ou celles des sections partielles.

---

[2] Autonome : sans liaison avec les niveaux supérieurs.

- Pour les tunnels à deux tubes, il existe une AS par installation pour les deux tubes. Les commandes locales et les agrégats au-dessous du niveau de la commande d'installation sont exécutés séparément pour chaque tube.
- Au niveau logique, la commande d'installation doit prendre en compte une séparation des tubes par directions.

## 5.4 Gestion des données

Toutes les données des installations, à l'exception du rVL/VL, sont stockées sur le serveur de gestion section AR.

Les états de signalisation, les plans de feux, les informations sur la situation du trafic, les valeurs de mesure de la VDE, etc. sont stockés sur le rVL/VL.

Le tab. 5.6 montre quels types de données existants sont archivés au niveau des systèmes de tronçons.

*Tab. 5.6 Archivage au niveau des systèmes de tronçons*

| Type de donnée | Archivage serveur de gestion section | Archivage niveau commande d'installation |
|---|---|---|
| Points de données | | |
| Etat des installations et valeurs de mesure | Archivage des données des installations pendant 13 mois | Archivage selon directives spécifiques aux installations |
| Etat du trafic | - | - |
| Données du trafic | - | - |
| Etat de la signalisation | - | - |
| Notifications | Archivage de toutes les notifications pendant 13 mois (journal) | - |
| Voix (téléphone de secours) | - | - |
| Log-files | Archivage de tous les log-files pendant un mois | Archivage de tous les log-files pendant un mois |
| Sauvegarde des données (backup) | - | - |

## 5.5 Modes d'exploitation et de fonctionnement

On distingue les modes d'exploitation suivants :

- « distant » : dans ce mode d'exploitation, les données d'exploitation actuelles sont transmises au niveau immédiatement supérieur, les ordres sont reçus du niveau immédiatement supérieur. C'est le mode d'exploitation normal ;
- « local » : dans ce mode, les données d'exploitation actuelles sont transmises au niveau immédiatement supérieur, mais aucun ordre n'est reçu de ce niveau ;
- « entretien » : dans ce mode, aucune donnée d'exploitation actuelle n'est transmise au niveau immédiatement supérieur, et aucun ordre n'est reçu de ce niveau supérieur. ;
- « test » : ce mode correspond au mode « distant », mais les messages sont transmis à des utilisateurs tests spécifiques et non pas aux utilisateurs standards. Cela permet de déclencher et de faire des essais d'alarme dans le cadre de tests de tunnels sans déranger le personnel régulier.

On distingue les modes de fonctionnement suivants :

- « automatique » (commandé par la logique de processus de l'installation)
- « manuel » (commandé par l'utilisateur)

## 5.6 Echange de données

Ce chapitre résume l'échange de données entre les différents éléments de l'architecture système.

### 5.6.1 Les systèmes au niveau région EES

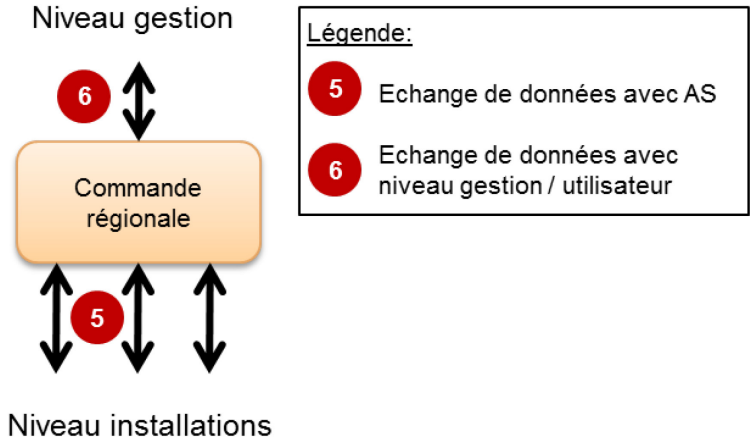


*Fig. 5.7 Par exemple : rVL - échange de données*

**Echange de données avec le niveau gestion / utilisateur (6) :**

L'élément régional met à disposition du niveau gestion et de l'utilisateur les points de données sélectionnés (voir Typicals).

**Echange de données avec AS S (5) :**

Cette interface permet à la rVL de commander et de surveiller l'installation subordonnée AS-S.

### 5.6.2 Serveur de gestion section

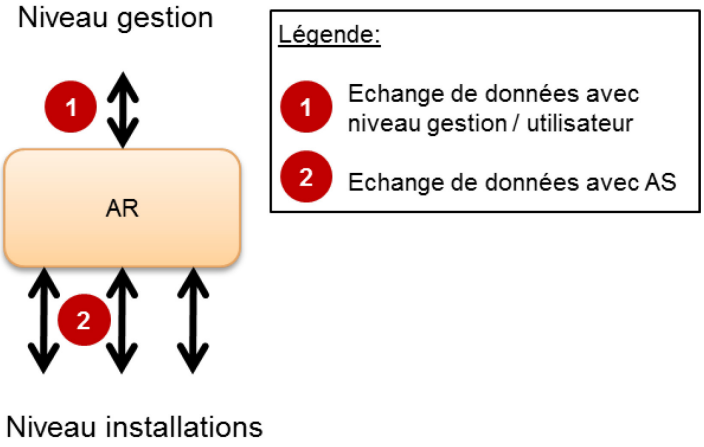


*Fig. 5.8 AR - échange de données*

**Echange de données avec le niveau gestion / utilisateur (1) :**

L'AR met à disposition du niveau gestion et de l'utilisateur des points de données sélectionnés.

**Echange de données avec l'AS (2) :**

Cette interface permet à l'AR de commander et de surveiller les installations.

### 5.6.3 Commande d'installation / commande locale

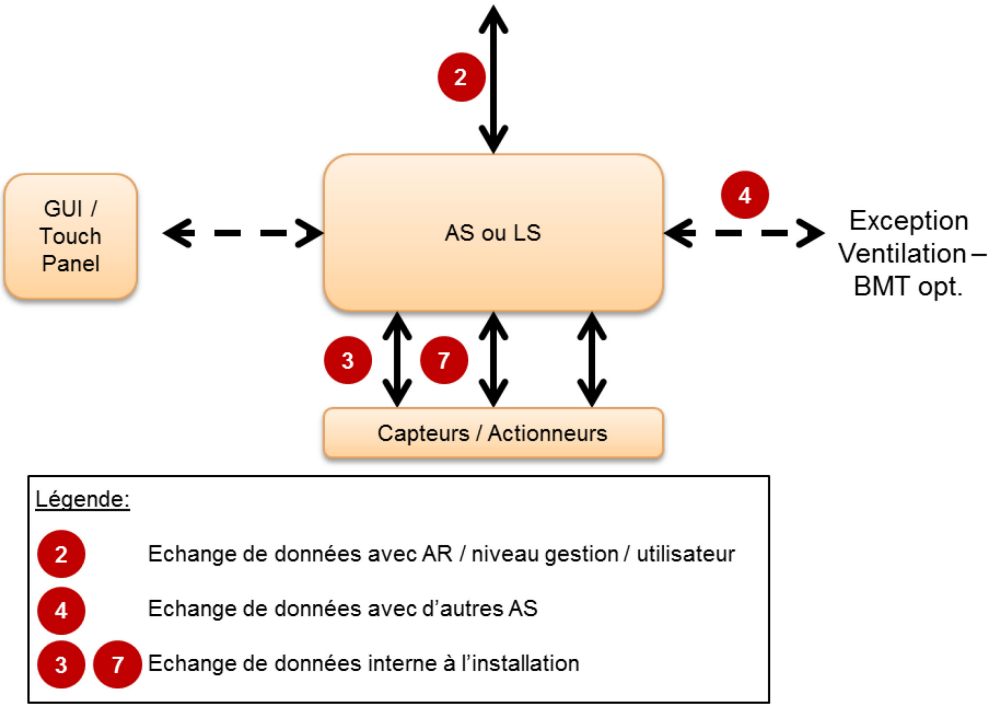


*Fig. 5.9 Echange de données générique AS/LS*

**Echange de données avec AR / niveau gestion / utilisateur (2) :**

L'AS envoie des messages / informations à l'AR et reçoit les commandes de l'AR.

**Echange de données interne à l'installation (3), (7) :**
L'AS échange des données et des commandes avec les LS et leurs capteurs et actionneurs.

**Communication Type 1 (4) :**

La communication entre commandes d'installations (AS <–> AS) se fait via l'AR. Pour les interdomaines de type 1, une liaison directe AS <-> AS (4) supplémentaire est prévue.

**GUI / Touchpanel :**

L'installation peut être aussi pilotée localement.

# 6 Disponibilité

Ce chapitre détermine les exigences relatives au temps moyen entre deux pannes (MTBF) et à la disponibilité des différents éléments.

## 6.1 Eléments de base

La disponibilité A est exprimée mathématiquement par une valeur sans dimension comprise entre 0 et 1, qui décrit le rapport entre la durée totale (MTBF = MTTF + MDT) et la durée moyenne d'indisponibilité (MDT). Dans cette directive, la disponibilité est représentée par un pourcentage, avec A=1 ⇔ 100%, soit :

$$A = 1 - \frac{MDT}{MTBF} = \frac{MTBF - MDT}{MTBF}$$

Pour obtenir une disponibilité élevée, le temps moyen qui s'écoule entre deux pannes (MTBF) doit être long, la durée moyenne d'indisponibilité (MDT) doit être courte, dans le cas où le système concerné tolère la défaillance de différents éléments.

La MDT est la somme du temps moyen de réparation (MTTR), du temps consacré à l'identification de la panne, appelé aussi temps de détection, et du temps de réaction jusqu'à ce que l'on puisse commencer à réparer la panne. Le temps de réaction comprend la mobilisation des personnes responsables et leur déplacement sur le site ou, à distance, sur le lieu où elles peuvent œuvrer à l'élimination de la panne ou de l'erreur.

Par exemple, avec deux éléments redondants ($A_1$, $A_2$), on calcule le MTBF et le MDT du système global (Atot) comme suit :

$A_{tot} = 1-(1-A_1) \times (1-A_2)$

Si les deux éléments sont identiques :

$$A_{tot} = 2A - A^2$$

## 6.2 Exigences posées aux valeurs MTBF

La Fig. 6.1 précise les exigences posées aux valeurs MTBF ainsi que les disponibilités arrondies qui en résultent. Ces disponibilités ont été calculées compte tenu de l'hypothèse selon laquelle la durée d'une défaillance par événement est égale à la durée de la remise en état (cf. [4]).

Par « temps de réparation » (MTTR), on entend le temps écoulé entre le début des travaux de réparation et la reprise de l'exploitation.

MTBF et MTTR sont des valeurs qui sont affectées aux caractéristiques d'un produit. La valeur MDT est une exigence issue des processus d'entretien et d'exploitation des EES.

| | | Défaillance complète (hardware et software) | | | | | |
|---|---|---|---|---|---|---|---|
| | | Produit | | Exploitation | | | |
| **Système / Elément** | **Technologie** | **MTBF en année** | **MTTR** | **Durée de panne par événement, MDT** | **Durée cumulée de pannes par an : (1-A)x8760** | **A tot*** ** | **A classe ** ** |
| **Niveau gestion y compris FA** | **Servercluster , Software, etc.** | **0.2 an** | ***** | **≤ 4h** | **≤ 22h** | **≥ 99.75%** | **2** |
| **Backbone 1)** | | **6 an** | ***** | **≤ 16h** | **≤ 2.5h** | **≥ 99.97%** | **1** |
| **Sous-réseau local EES 2)** | | **12 an** | ***** | **≤ 8h** | **≤ 0.7h** | **≥ 99.99%** | **1** |
| **rVL / VL / AS-S autres éléments régionnaux** | **IPC** | **1 an** | **4h** | **≤ 72h [4]** | **≤ 72h** | **≥ 99.2%** | **2** |
| **Serveur de gestion section (redondant) 3)** | **IPC** | **3 ans** | **4h** | **≤ 72h [4]** | **≤ 22h** | **≥ 99.75%** | **2** |
| **Commande d'installation (systèmes standards)** | **API** | **5 ans** | **4h** | **≤ 504h [4]** | **≤ 100h** | **≥ 98.8%** | **3** |
| **Commande d'installation (systèmes critiques pour la sécurité - BMT, ventil. Selon [4])** | **API** | **5 ans** | **4h** | **≤ 72h [4]** | **≤ 14h** | **≥ 99.8%** | **2** |
| **Commande locale (systèmes standards [4])** | **API** | **40 ans** | **4h** | **≤ 504h [4]** | **≤ 13h** | **≥ 99.9%** | **2** |
| **Commande locale (systèmes critiques pour la sécurité - BMT, ventilation, signalisation [4])** | **API** | **40 ans** | **4h** | **≤ 72h [4]** | **≤ 2h** | **≥ 99.98%** | **1** |

* Réparation par les fournisseurs, donc seul est considéré le temps de panne total par événement.
**Classe 1: 99.9% ≤ A tot ≤100%
Classe 2: 99.0% ≤ A tot < 99.9%
Classe 3: A tot < 99.0%
*** A tot calculé et arrondi

**Références:**

[4] Office fédéral des routes, Exigences minimales en matière d'exploitation des tunnels routiers, OFROU 86053, V0.98, 2013

1) Exigences au backbone de la confédération
2) Selon directive 13040 Réseaux IP EES UT

*Tab. 6.1 Aperçu des exigences posées aux valeurs MTBF par système*

3) Dans le cas d'un **système redondant**, la défaillance complète désigne la panne simultanée de tous les éléments redondants à tel point que le système global ne peut plus remplir sa fonction. En l'occurrence, il n'est pas important de savoir si la panne est due à des défauts matériels (hardware) ou logiciels (software).

Conformément aux réflexions et en référence à [4], il est possible, sans redondance, d'atteindre une disponibilité suffisante, pour autant que la remise en état (principalement sur le temps de réaction) se produit en quelques jours.

Pour les systèmes à disponibilité élevée, les redondances sont obligatoires et permettent de fixer des exigences acceptables à la réparation (en particulier le temps de réaction).

Pour maximiser la disponibilité d'un système redondant, il faut que les deux éléments soient aussi indépendants l'un de l'autre que possible (p. ex. séparation locale, raccordement à des réseaux électriques différents, raccordement à des switches différents). De la sorte, il est possible de minimiser les pannes dues à des causes communes.

# 7 Migration

Ce document définit l'état idéal final de l'architecture système. Le remplacement des EES existants sera traité en détail dans une documentation séparée. Les étapes de la migration sont sommairement présentées dans ce chapitre. La Fig.7.1 donne un aperçu de l'architecture de migration.

Les nouveaux systèmes de tronçons sont reliés aux systèmes de gestion généraux décentralisés actuels par un adaptateur de services (service-Adapter SA), alors que les systèmes de tronçons existants sont reliés au nouveau niveau gestion par un intégrateur de services (service-Integrator SI).

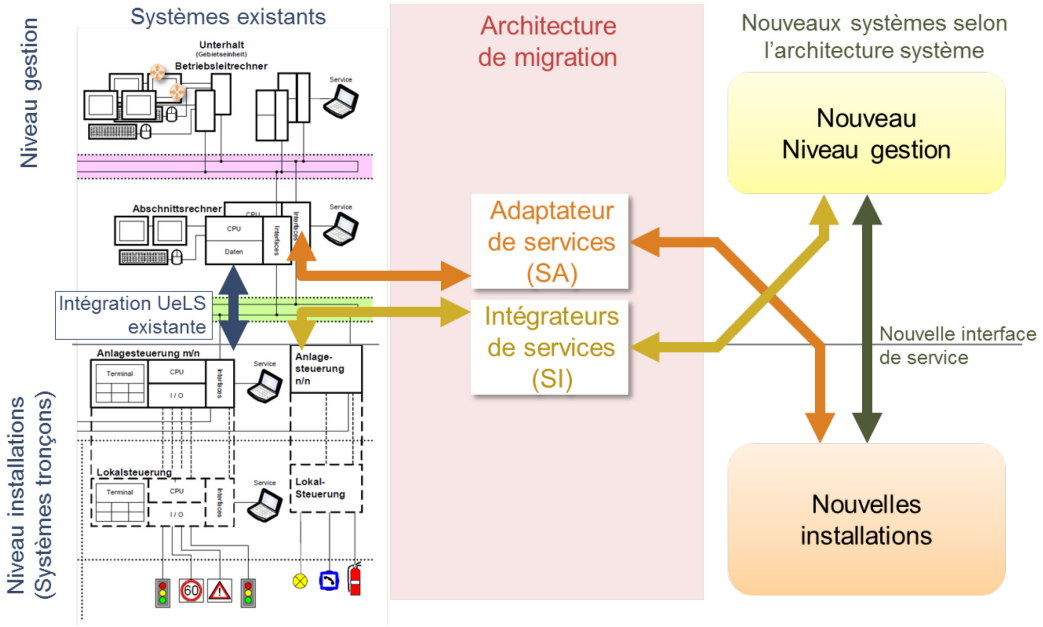


*Fig. 7.1 Aperçu de l'architecture de migration*

Le processus de migration est conduit comme un projet commun des divisions N et I.

La migration et donc la mise en conformité des EES à la présente directive s'effectuent par étapes et en coordination avec l'avancement des projets EES.

Les étapes de migrations sont :

1. Respect de la topologie des systèmes de tronçons et des standards de communication ;
2. Respect des chartes IHM ;
3. Respect de la définition des points de données et des interfaces ;
4. Remplacement des UeLS-CH par le niveau gestion.

# Annexes

**I Modèles topologiques ..... 35**
I.1 Généralités ..... 35

# I Modèles topologiques

## I.1 Généralités

Les différents éléments individuels de l'architecture sont présentés dans les *Fig. I.1* à *Fig. I.3*.

Trois variantes fréquentes de l'architecture système sont présentées à savoir :

- *Fig. I.1* : vue fonctionnelle au niveau des systèmes de tronçons dans une section EES avec un tunnel et une partie à ciel ouvert, comportant un serveur de gestion section. Désignation des installations selon AKS-CH.
- *Fig. I.2* : vue fonctionnelle au niveau des systèmes de tronçons dans une section EES avec un grand, un petit tunnel et une partie à ciel ouvert, comportant un serveur de gestion section.
- *Fig. I.3* : vue fonctionnelle au niveau des systèmes de tronçons avec deux sections EES, comportant un serveur de gestion section par section :
  - pour la première avec un tunnel et une partie à ciel ouvert ;
  - pour la seconde avec uniquement un tunnel.

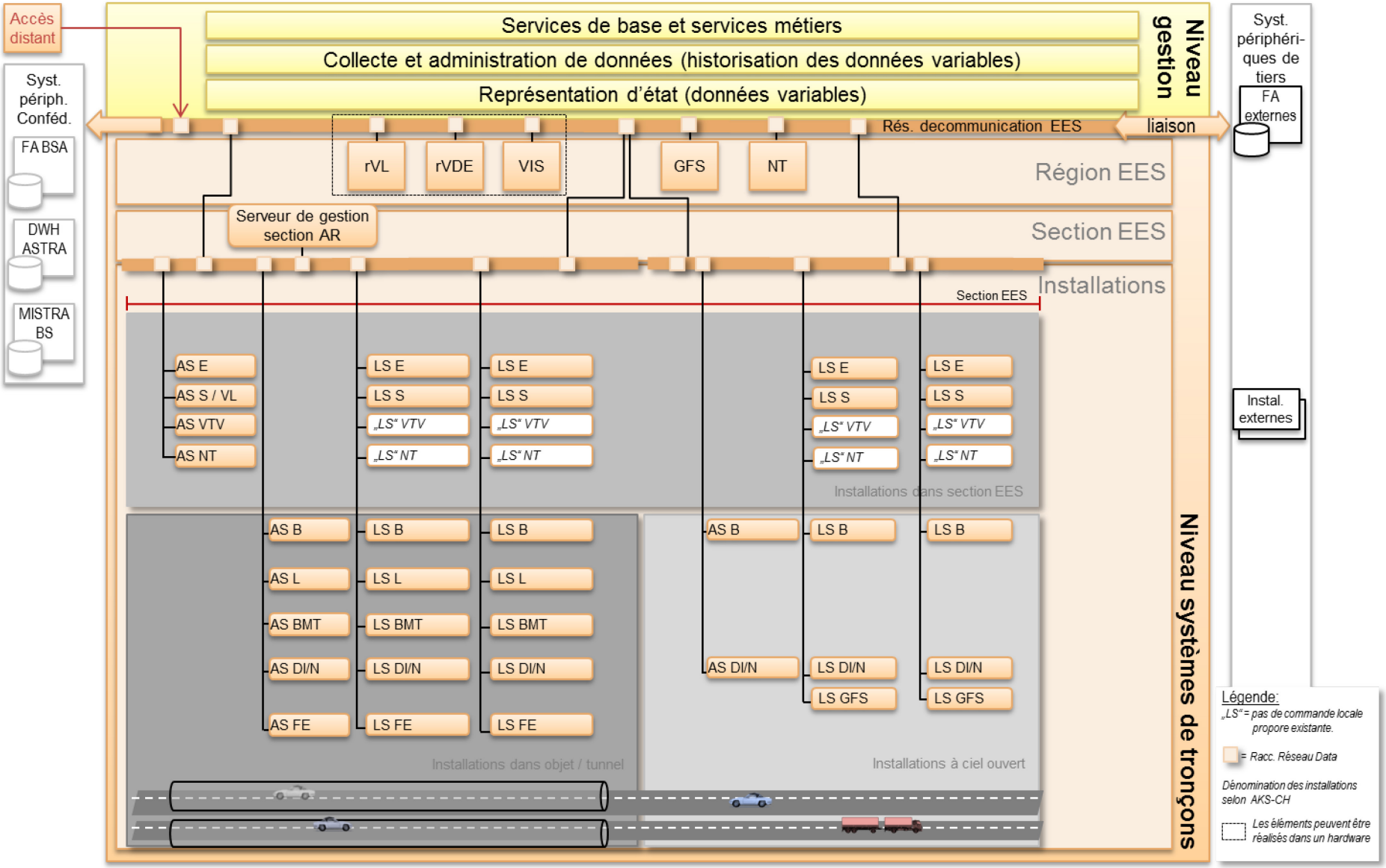


*Fig. I.1 Vue topologique au niveau des systèmes de tronçons (description, voir I.1).*

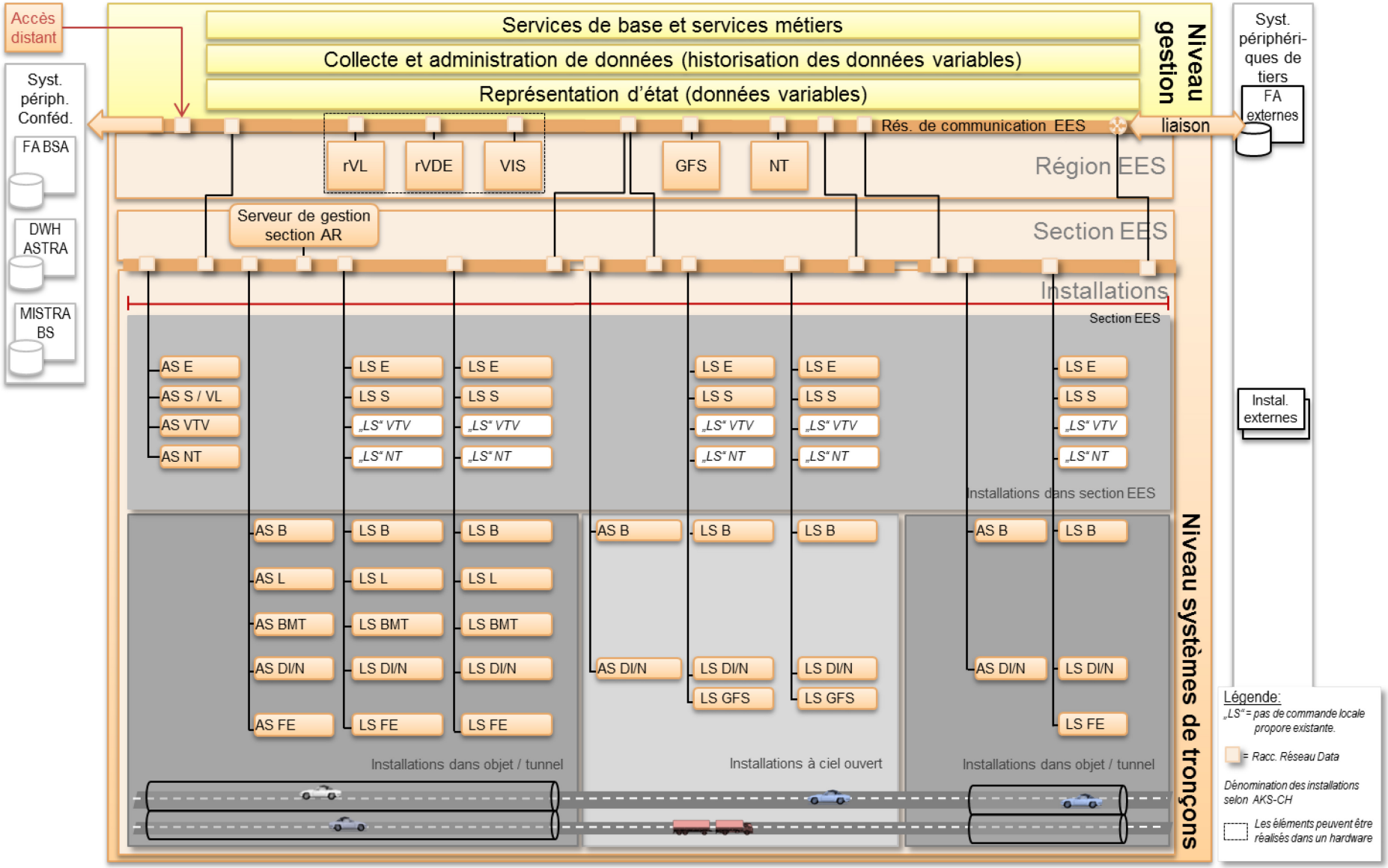


*Fig. I.2 Vue topologique au niveau des systèmes de tronçons (description, voir I.1).*

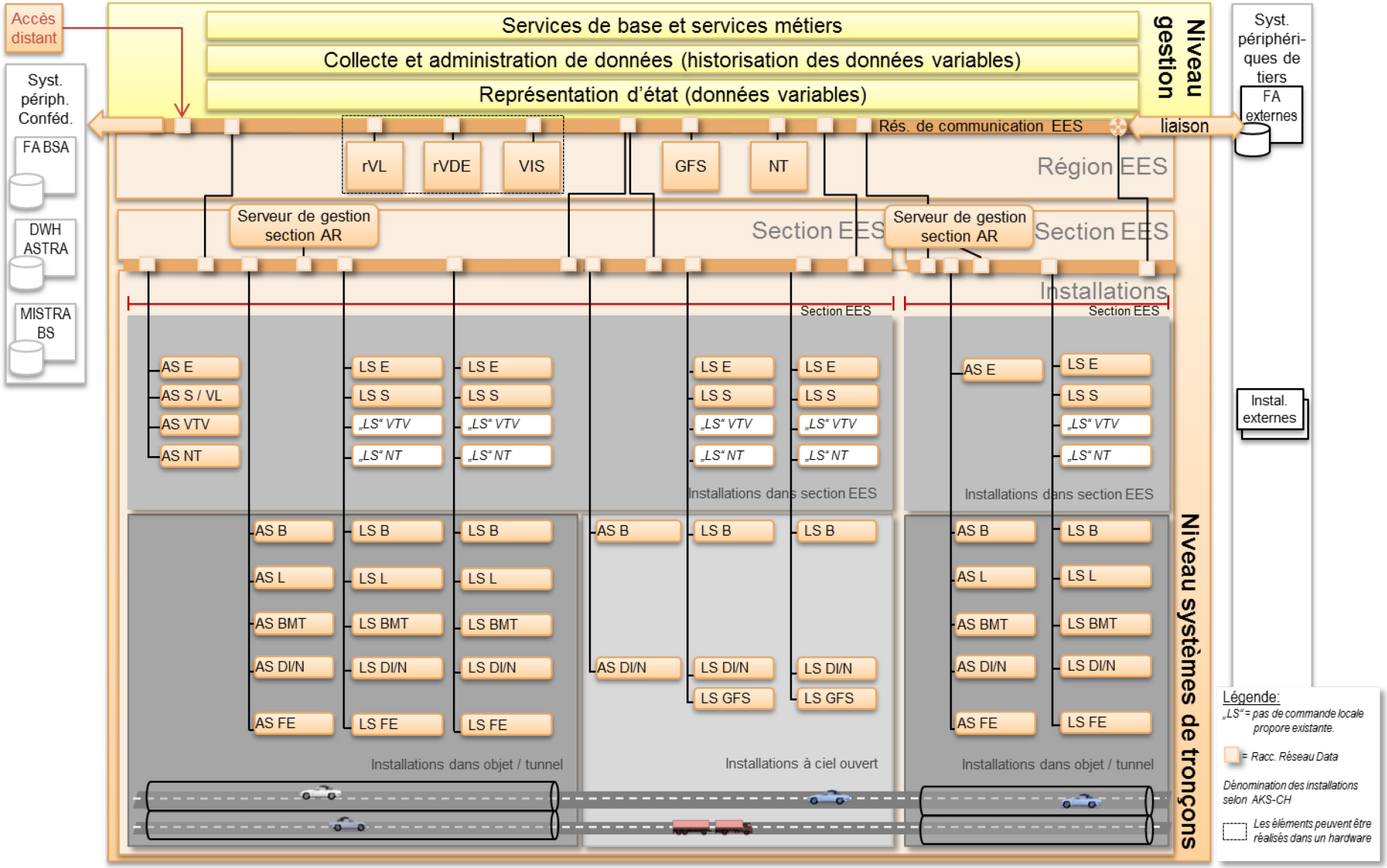


*Fig. I.3 Vue topologique au niveau des systèmes de tronçons (description, voir I.1)*

.

# Glossaire

| Terme | Définition |
|---|---|
| A | Availability : disponibilité (grandeur mathématique comprise entre 0 et 1) |
| AKS-CH | Structure et nomenclature des équipements d'exploitation et de sécurité (EES) |
| AR | Serveur de gestion section (abr. de « Abschnittsrechner ») |
| AS | Commande d'installation (abr. de « Anlagesteuerung ») |
| Autonomie | Indépendance par rapport aux niveaux supérieurs |
| Service de base<br>*Basisdienst* | Les services de base comportent des fonctions qui n'implémentent pas une logique métier, mais qui sont un prérequis pour les services métiers. Ils implémentent des fonctions d'infrastructure d'usage général ou nécessaires, mais sans caractère technique spécifique. |
| Modes d'exploitation<br>*Betriebsarten* | Les installations se trouvent dans un des quatre modes d'exploitation : « distant », « local », « entretien », « test ». |
| Niveau gestion<br>*Management-Ebene*<br>*Betriebsleitebene*<br>*Übergeordnete Leitsysteme (UeLS)* | Ce niveau gère la surveillance et la commande de toutes les installations d'un tronçon routier au moyen de serveurs de gestion générale, d'une part par la police pour ce qui concerne les événements et des aspects spécifiquement liés à l'exploitation, d'autre part, par le service d'entretien pour ce qui touche à la disponibilité fonctionnelle des installations. Les serveurs de gestion générale sont reliés aux serveurs de gestion de section par un réseau de communication.<br>Le terme allemand « Management-Ebene » contient la notion de niveau gestion centralisée sur le plan suisse. |
| BLZ | Centrale de commande d'exploitation (abrév. de « Betriebsleitzentrale ») |
| BMT | installation de détection incendie tunnel (abréviation de « Brandmeldeanlage Tunnel ») |
| EES<br>*BSA* | Equipements d'exploitation et de sécurité |
| Section EES<br>*BSA - Abschnitt* | Section de route nationale commandée par un serveur de gestion section |
| Région EES<br>*BSA – Region* | Région définie pour des installations spécifiques où il existe un système supérieur régional pour la commande. |
| PF<br>*BZ* | Un plan de feux (PF) ou « scénario de signalisation » est une combinaison préalablement définie et une succession d'enclenchements d'états d'un ou de plusieurs signaux. Chaque plan de feux se trouve dans l'un des états suivants :<br>« inactif » (déclenché), « en cours de mise en service », « actif » (enclenché), « en cours de démantèlement ».<br>Un plan de feux correspond toujours à un état final. Le processus de mise en place et de suppression d'un plan de feux, concerne toujours plusieurs signaux ou même plusieurs plans de feux indépendants les uns des autres. |
| Domaine<br>*Domäne* | Le domaine sert à organiser et à grouper des éléments. Au sein de l'OFROU, le domaine est utilisé pour :<br>- espace de noms : à l'intérieur d'un espace de noms, les identités sont univoques, c'est-à-dire que chaque ressource possède sa propre identité ;<br>- domaine de fonctions : regroupement de différentes fonctions ;<br>- domaine métier : regroupement de différents services métiers ;<br>- domaine de processus : regroupement de différents processus. |
| Service<br>*Dienst* | « Service » est un terme générique qui s'applique tant aux services métiers qu'aux services de base. Les services implémentent les logiques d'accès et de traitement, mais ne disposent pas d'une interface utilisateur. |
| DWH | Banque de données (abr. de « Data Warehouse »). |
| SAE<br>*ELS* | Système d'aide à l'engagement |
| FA | Application métier (abr. de « Fachapplikation »), application BSA. |
| FA BM | Application métier gestion des chantiers (BM = abr. de « Baustellenmanagement ») |
| FA POL | Application métier tâches de police |
| FA UHB | Application métier entretien et exploitation (UHB = abr. de « Unterhalt und Betrieb ») |
| FA VM | Application métier gestion du trafic (VM = abr. de « Verkehrsmanagement ») |
| Service métier<br>*Fachdienst* | Les services métiers sont des composants logiciels dans les EES, qui implémentent la logique métier. Ils sont groupés en domaines métiers d'après leur appartenance fonctionnelle. |

| Terme | Définition |
|---|---|
| Application métier<br>*Fachapplikation* | Les applications métiers servent à implémenter le support IT de processus métiers. Par conséquent, toute application métier dispose d'une interface utilisateur et de la logique de commande correspondante (navigation, flux de dialogue), qui active les services subordonnés. Chaque utilisateur et chaque groupe d'utilisateurs disposent de différentes vues et de différentes possibilités de commande suivant leur rôle et leurs droits d'accès. |
| UT<br>*GE* | Unité territoriale |
| GEWI TIC | Plateforme en ligne destinée à la saisie standardisée de messages; exploitée par Viasuisse |
| GFS | Installation de surveillance et d'alarmes météo (abr. de « Glatteisfrühwarnsystem »). |
| GUI | Interface utilisateur graphique (abr. de « Graphical User Interface »). |
| Bornes intelligentes<br>*Intelligente Klemmen* | Les bornes intelligentes permettent de transmettre plusieurs signaux numériques ou analogiques par un seul câble. |
| IPC | PC industriel. |
| Niveau gestion<br>*Leitebene* | Voir niveau processus |
| Système de gestion<br>*Leitsystem* | Sert aux opérateurs pour la surveillance et la commande des installations. |
| Système de commande/gestion<br>*Leittechnik* | Fonctions et composants servant à la surveillance et à la commande des installations. |
| LS | Commande locale (abr. de « Lokalsteuerung »). |
| ME | Niveau gestion (abr. de « Management-Ebene »). |
| MISTRA, MISTRA BS | Système d'information pour la gestion des routes et du trafic. BS = Système de base |
| Monitoring | Surveillance et visualisation des fonctions techniques des installations et des systèmes de commande. |
| MDT | Mean down time : durée moyenne d'indisponibilité (comprend le temps de réparation, la détection des erreurs, le temps de réaction, etc.). |
| MTBF | Mean time between failures : temps moyen entre deux pannes (y c. réparations). |
| MTTF | Mean time to failure : durée moyenne avant panne (pour le remplacement d'un système). |
| MTTR | Mean time to repair : durée moyenne de réparation. |
| NT | Installation téléphones de secours (abr. de « Notruftelefon »). |
| OPC-UA | OPC Unified Architecture (technologie d'interface indépendante de constructeurs, pour les processus et les systèmes de commande. |
| Niveau processus<br>*Prozessleitebene*<br>*Leitebene* | Terme utilisé dans les systèmes de gestion : à ce niveau s'effectuent la surveillance et la commande des installations et la gestion de la section (interdomaines de tunnels) au moyen d'un serveur de gestion section. |
| rVDE | Acquisition régionale de données de trafic (abr. de « regionale Verkehrsdatenerfassung »). |
| rVL | Gestion régionale du trafic (abr. de « regionale Verkehrslenkung ») |
| Adaptateur de services<br>*Service Adapter (SA)* | Pour intégrer des installations réalisées avec un serveur de gestion section en vertu des prescriptions de l'architecture système dans des systèmes de gestion générale (UeLS) encore existants, les données mises à disposition par l'AR doivent être converties dans une forme compréhensible par le système de gestion générale existant. Cette fonction est prise en charge par ce qu'on appelle un adaptateur de services. |
| Intégrateur de services<br>*Service Integrator (SI)* | Un intégrateur de services permet l'intégration d'une installation existante dans le niveau gestion de l'architecture système, par le fait que l'interface avec le niveau gestion est convertie dans une forme compréhensible par l'installation considérée. |
| Secteur<br>*Sektor* | Partie d'un territoire. Typiquement, un secteur sert à subdiviser la longueur des voies de circulation en vue de segmenter les installations. Un secteur peut avoir une longueur variant de quelques mètres à environ 5 km. |
| SNMP | protocole de gestion de réseau (abr. de « Simple Network Management Protocol »). |
| SOA | Architecture orientée services (abr. de « Service Oriented Architecture »). |
| API<br>*SPS* | Automate programmable (abr. de « Speicherprogrammierbare Steuerung »). |
| STS | Voir Système de tronçons (abr. de « Streckensystem »). |
| Systèmes de tronçons<br>*STS Streckensysteme* | Par systèmes de tronçons, on entend les installations et les systèmes implantés le long d'une route nationale et qui assurent l'exploitation et la sécurité de tous les EES d'un tronçon donné. Les composants se trouvent sur des niveaux d'automation différents |

| Terme | Définition |
|---|---|
| | (depuis les capteurs/actionneurs jusqu'aux éléments régionaux) tant sur des tronçons à ciel ouvert que dans des tunnels. |
| SA | Architecture système (abr. de « Systemarchitektur ») |
| Architecture technologique<br>*Technologiearchitektur* | Partie d'une architecture système qui traite de la construction et de l'exploitation d'une infrastructure IT. |
| TLS | Standard allemand définissant l'architecture et le protocole de communication pour les installations de signalisation (abr. de « Technische Lieferbedingungen für Streckenstationen »). |
| UeLS | Système de gestion général (abr. de « Übergeordnetes Leitsystem » |
| Systèmes périphériques<br>*Um–Systeme* | Les systèmes qui ne font pas partie des EES, mais qui communiquent avec ceux-ci, sont appelés systèmes périphériques dans ce document. |
| Section UPlaNS<br>*UPlaNS-Abschnitt* | Section entièrement assainie dans le cadre de la planification de l'entretien des routes nationales (abr. de « Unterhaltsplanung der Nationalstrassen »). |
| VIS | Système d'information trafic (abr. de « Verkehrsinformationssystem »). |
| VL | Système de gestion trafic, (correspond à la gestion des installations de signalisation AS S ; abr. de « Verkehrsleitsystem »). |
| VM-CH | Gestion du trafic Suisse (abr. de « Verkehrsmanagement Schweiz »). |
| VMZ-CH | Centrale suisse de gestion du trafic (abr. de « Verkehrsmanagementzentrale Schweiz ») |
| VTV | Installation vidéo (abr. de « Verkehrsfernsehen V-TV »). |
| PMV<br>*WTA* | Panneaux à messages variables. |
| WWW | panneau de direction à indications variables (abr. de « Wechselwegweisung »). |
| Représentation d'état<br>*Zustandsabbildung* | Situation actuelle réelle (état du trafic, de la signalisation, valeurs de mesure des installations, messages d'alarme et de dérangement, etc.) des systèmes de tronçons. |

# Bibliographie


**Directives, instructions et documentations de l'OFROU**

[1] Office fédéral des routes OFROU (2014), **« Structure et désignation des équipements d'exploitation et de sécurité (AKS-CH) »,** *Directive ASTRA 13013,* www.astra.admin.ch

[2] Office fédéral des routes OFROU (2013), **« Pilotage des EES : rôles, tâches et exigences pour les interfaces utilisateurs »**", *Instructions ASTRA 73002*, www.astra.admin.ch

[3] Office fédéral des routes OFROU, « **Sécurité informatique des systèmes de commande et de gestion des équipements d'exploitation et de sécurité »**, *Directive ASTRA 13030,* www.astra.admin.ch

**Documentations**

[4] Office fédéral des routes OFROU (2013), 86053 **« Exigences minimales en matière d'exploitation des tunnels routiers »**, www.astra.admin.ch

[5] Office fédéral des routes OFROU (2014), 83050 « **Style Guide EES**, **Partie 0 : Bases générales** », www.astra.admin.ch. (en allemand : version française en préparation)

[6] Office fédéral des routes OFROU (2014), 83052 « **Style Guide EES**, **Partie 2 : Niveau systèmes de tronçons** », www.astra.admin.ch. (en allemand : version française en préparation)

[7] Office fédéral des routes OFROU (2014), 83053 « **Style Guide EES**, **Partie 3 : Bibliothèque des symboles »**, www.astra.admin.ch. (en allemand : version française en préparation)

**Autres documents**

[8] Bundesministerium für Verkehr, Bau und Stadtentwicklung (2012), „**Technische Lieferbedingungen für Streckenstationen**", Edition 2012

# Liste des modifications

| Édition | Version | Date | Modifications |
|---|---|---|---|
| 2016 | 1.70 | 01.11.2017 | • Publication de la version française.<br>• Correspondance entre version française et version allemande. |
| 2016 | 1.60 | 01.01.2016 | • Entrée en vigueur de l'édition 2016 (version originale en allemand).<br>• Ensemble du document : remplacement de réseau des infrastructures EES (ISN) par réseau de communication des EES.<br>• Ensemble du document : suppression de la numérotation des exigences (Rx).<br>• Chapitre 2.5 Migration rajouté.<br>• Légende de la figure 2.3 rajoutée.<br>• Simplification des figures 3.1 et 5.1.<br>• Révision du chapitre 7.<br>• Correction de la bibliographie.<br>• Diverses corrections formelles et corrections de texte. |
| 2015 | 1.50 | 01.10.2015 | • Suppression de l'annexe II catalogue métiers points de donnée. |
| 2015 | 1.40 | 01.06.2015 | • Insertion de l'annexe II catalogue métiers points de donnée.<br>• Corrections diverses. |
| 2015 | 1.10 | 01.01.2015 | • Entrée en vigueur de l'édition 2015 (version originale en allemand). |