Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral des routes OFROU

DIRECTIVE

OT SECURITY

Édition 2024 V2.00
ASTRA 13030

Impressum

Auteurs / Groupe de travail

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

Groupe d'accompagnement

Bruno Frey	OFROU DS-État-major IT/OT Gouvernance
Wolfgang Hoffmann	OFROU DS-État-major IT/OT Gouvernance
Crausaz Bernard	OFROU DS-UARS
Markus Eisenlohr	OFROU I-FU
Patrick Fuhrer	OFROU F3
Peter Baur	OFROU F4
Ivo Perseghini	OFROU F5
Daniel Sägesser	UT I
Pascal Roth	UT VIII
Fabio Caspani	UT VIII
Ludovic Roulet	UT IX
Ivo Achermann	UT X
Patrik Imhof	UT XI
Luca Hunziker	IM Maggia Engineering SA
Alain Gatti	ingegna SA
Markus Schlup	Amstein + Walthert Progress AG

Traduction
CSI Consulting AG, la version originale en allemand fait foi.

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

Source
Le document peut être téléchargé gratuitement sur www.ofrou.admin.ch.

Préface

Les progrès rapides de la technique et les exigences sans cesse croissantes posées à l'infrastructure routière exigent des directives uniformes en matière de sécurité d'exploitation. La sécurité routière sur le réseau routier actuel est aujourd'hui assurée dans une large mesure par les équipements d'exploitation et de sécurité (EES).

La présente directive définit les grandes lignes d'une architecture de sécurité uniforme pour les équipements d'exploitation et de sécurité de l'OFROU. Elle a été déduite des directives sur la gouvernance de la sécurité OT de l'OFROU, des directives de la Confédération, des besoins en matière de sécurité (besoin de protection) avec les exigences en matière de protection des informations et des données ainsi que de l'analyse des risques avec l'exigence de garantir autant de sécurité que nécessaire et non pas autant de sécurité que possible.

La présente directive vise à jeter les bases d'un niveau de sécurité OT uniforme pour les équipements d'exploitation et de sécurité de l'OFROU.

La présente version 2.00 a été remaniée et adaptée à l'état de la technique et à la nouvelle cyberstratégie de la Confédération. Une attention particulière a été accordée aux nombreuses particularités de l'environnement EES/OT.

Office fédéral des routes

Jürg Röthlisberger
Directeur

Table des matières

1 Introduction

1.1 But de la directive

La sécurité désigne un état dans lequel les risques résiduels sont considérés comme acceptables. La présente directive fixe des exigences et des mesures pour la protection des éléments des équipements d'exploitation et de sécurité (EES) à l'aide de moyens OT afin de garantir la sécurité dans une mesure suffisante.

1.2 Champ d'application

Etant donné que la sécurité IT et la sécurité OT présentent des points communs, mais aussi de grandes différences, les deux thèmes de sécurité sont traités séparément et gérés par des directives distinctes. La présente directive ne traite que du domaine de la sécurité OT.

La directive s'applique obligatoirement à la planification, à l'étude de projet, à la réalisation et à l'exploitation des systèmes de communication, de commande et de contrôle (systèmes OT) de tous les équipements d'exploitation et de sécurité (EES) des routes nationales.

1.3 Destinataires

La directive s'adresse aux :

- Spécialistes et planificateurs d'entretien EES de l'OFROU ;
- Spécialistes EES des unités territoriales ;
- Chef de projet SA-CH de l'OFROU ;
- Chef de projet de l'OFROU (pour les projets avec technique de commande et de contrôle) ;
- Planificateurs et entreprises qui exécutent des activités pour le compte de l'OFROU aux EES.

1.4 Entrée en vigueur et modifications

La présente directive entre en vigueur le 01.03.2016. La « liste des modifications » est documentée en page 29.

2 Termes

Les termes spécifiques suivants sont utilisés dans la présente directive :

- **Système de gestion de la sécurité (SMS) :** un système de gestion de la sécurité (SMS) définit les règles et les méthodes permettant d'assurer la sécurité au sein d'une organisation ou d'un secteur ;
- **Niveau de sécurité :** par niveau de sécurité, on entend le degré de sécurité exigé ou existant ;
- L'**équipement d'exploitation et de sécurité (EES)** comprend les installations électromécaniques ainsi que les installations de commande et de gestion qui servent à l'exploitation et à la sécurité des routes nationales ;
- **OT et système OT (OT System)** : OT signifie Operational Technology et désigne l'utilisation de matériel et de logiciels pour la surveillance et la commande de processus physiques, d'appareils et d'infrastructures. L'OT comprend donc la technique de commande et de contrôle des EES, l'infrastructure nécessaire (p. ex. réseau IP EES), les systèmes OT ainsi que les applications et les services. Les systèmes OT et les agrégats sont des EES ;
- **Zone de réseau (zone)** : Une zone est une association logique de systèmes OT qui se caractérisent par des tâches communes et sont soumis à la même politique de zone. L'accès au réseau d'une zone s'effectue par le biais de composants réseau, tandis que l'application des règles de la politique de zone s'effectue par le biais d'éléments de sécurité ;
- **Éléments de sécurité / Policy Enforcement Point (PEP) :** les éléments de sécurité servent à appliquer des règles (de politiques) à un Policy Enforcement Point (point de transition entre deux zones). Les éléments de sécurité ont différentes formes et fonctions, comme par exemple les pare-feu, les filtres de paquets dynamiques, les passerelles de protocole d'application, les serveurs proxy ou les serveurs proxy inversés.

3 Système de gestion de la sécurité OT (OT-SMS)

Le système de gestion de la sécurité OT (OT-SMS) définit les règles et les méthodes permettant de garantir la sécurité au sein de l'OFROU. Le système OT-SMS est inscrit dans les instructions de l'OFROU concernant la gouvernance de la sécurité OT et est décrit plus en détail dans la présente directive.

Avec l'OT-SMS, l'OFROU s'assure que :

- un niveau de sécurité OT uniforme soit atteint ;
- une architecture de sécurité uniforme soit respectée ;
- en tenant compte de l'état de la menace et des scénarios de risque qui en découlent, on assure autant de sécurité que nécessaire et non pas autant que possible.

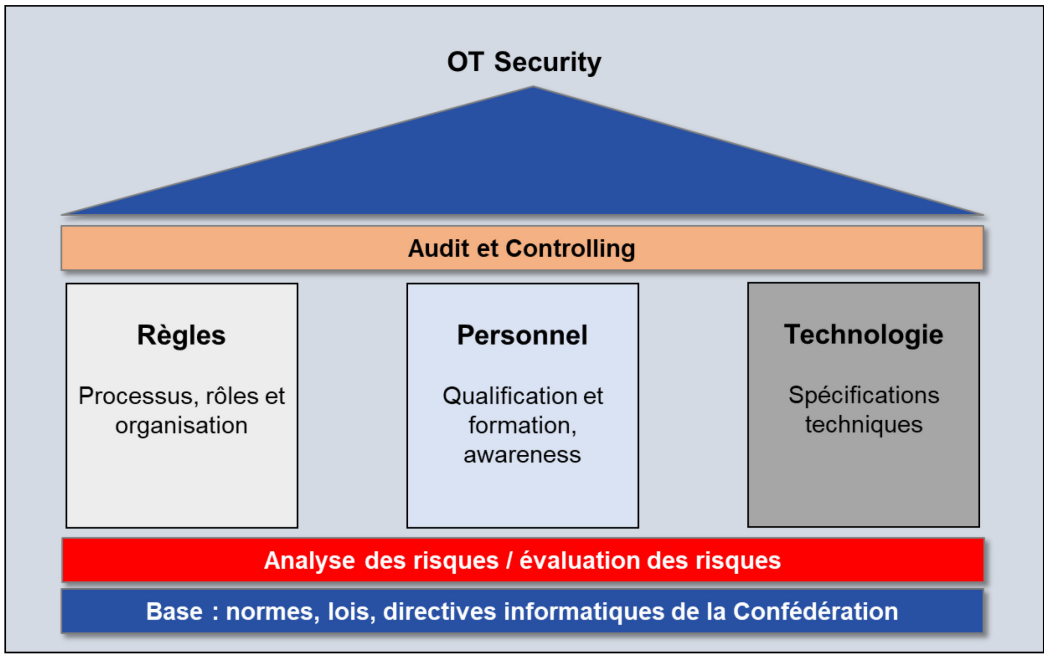

Fig. 3.1 Système de gestion de la sécurité OT (OT-SMS) des routes nationales

Les chapitres suivants présentent les scénarios de risques et expliquent les règles et les méthodes des trois éléments de base que sont les règles, les personnes et la technologie du système OT-SMS :

- Le chap. 4 présente les menaces, les besoins et les objectifs de protection ;
- Le chap. 5 décrit les processus en mettant l'accent sur l'organisation de la sécurité OT, les rôles et l'organisation ;
- Le chapitre 6 décrit les directives et les dispositions relatives à la qualification et à la formation des collaborateurs et à la sensibilisation dans le domaine de la sécurité OT ;
- Le chapitre 7 décrit les directives et les dispositions relatives aux systèmes techniques et à l'utilisation des systèmes OT.

4 Menaces, besoins et objectifs de protection

Remarque préliminaire : au niveau de la Confédération, il n'existe pas encore de directives traitant du thème de la sécurité OT. Le sujet est en cours de traitement au niveau fédéral et sera intégré par l'OFROU dès que les directives seront disponibles.

4.1 Analyse des risques et des menaces

Dans la gestion des risques, l'analyse des risques est l'analyse des risques identifiés par l'identification des risques de différents faits et situations dangereuses. L'analyse des risques fait appel à différentes techniques d'analyse, telles que l'analyse qualitative et l'analyse quantitative. Le risque quantitatif résulte de la multiplication du montant des dommages par la probabilité d'occurrence ou le taux de danger. L'analyse des risques se concentre sur l'ampleur des dommages potentiels et leur coût pour l'OFROU.

L'analyse des menaces est une partie de la gestion des risques. L'analyse des menaces dans le contexte d'un système OT permet de recenser, de structurer et d'évaluer systématiquement les différentes menaces qui pèsent sur les systèmes et les processus OT. Les menaces identifiées et l'évaluation de la situation de danger permettent de déduire les différents risques pour la gestion des risques.

4.2 Menaces et scénarios de risques

Le tableau ci-dessous énumère et concrétise les dangers / menaces possibles pour l'infrastructure OT EES.

Tab. 4.1 Dangers/menaces

G-Nr.	Description
G1	Ingénierie sociale (hameçonnage, dumpster diving) / espionnage
G2	Introduction de logiciels malveillants via Internet, Intranet, supports de données amovibles ou matériel externe
G3	Infection par des logiciels malveillants via Internet, Intranet, supports de données amovibles ou matériel externe
G4	Intrusion non autorisée dans les systèmes OT (par ex. intrusion via des accès de maintenance)
G5	Abus d'autorisation (utilisation/administration non autorisée d'appareils et de systèmes)
G6	Composants de contrôle connectés à Internet
G7	Faille de sécurité dans le logiciel
G8	Défaillance ou perturbation des réseaux de communication
G9	Divulgation d'informations sensibles
G10	Panne / dysfonctionnement d'appareils ou de systèmes
G11	Panne de courant locale
G12	Absence / manque de personnel

Tab. 4.2 Dangers/menaces qui ne sont pas au centre de l'attention

G-Nr.	Description
G13	Terrorisme d'État
G14	Force majeure (panne d'électricité à grande échelle, catastrophes naturelles, pandémies), défaillance des fournisseurs, catastrophes techniques (explosions et incendies, effondrement de bâtiments, accidents de la circulation [accidents de voiture de masse, crashs d'avion, déraillement de train, naufrage, etc.], accidents radioactifs)
G15	Actes intentionnels tels que l'abus, le vol

Il en résulte différents scénarios de risque possibles dans l'environnement EES :

Tab. 4.3 Scénarios de risque

R-Nr.	Titre	Scénario de risque	Effets possibles
R1	Erreur de manipulation	• Déclenché par un être humain	• Circulation difficile sur les Routes nationales • Défaillance de composants EES • Danger pour les personnes
R2	Fausse alerte	• Le dysfonctionnement des systèmes d'alarme déclenche de fausses alarmes	• Perte de confiance dans l'organisation de l'alarme Dommages à l'image • Perte de temps des employés • Fenêtre de temps non surveillée pour les attaquants (car le personnel est occupé par les fausses alertes).
R3	Logiciels malveillants (malware)	• Malware ou ransomware sur le réseau IP EES • Les logiciels malveillants sont diffusés dans le réseau client de l'OFROU via le système OT • Le système OT est crypté • les configurations du système OT sont effacées (exécution automatique d'une réinitialisation)	• Panne totale à long terme de la fonctionnalité EES • Dans le pire des cas, une grande partie de l'OFROU sera touchée • Manipulation des installations, perte et/ou modification de la configuration des agrégats au niveau du terrain • Trafic difficile sur les routes nationales suisses • Danger pour les personnes • Perte de données
R4	Panne de courant	• Défaillance de la connexion réseau • Panne du réseau électrique	• Perte de la vue d'ensemble centrale • Défaillance de l'alarme EES • Restrictions de circulation sur les Routes nationales • Défaillance de composants EES
R5	Divulgation d'informations (Information Disclosure)	• Des personnes non autorisées ont accès aux données des routes nationales • Perte de données sensibles (p. ex. données du domaine SZP-EES)	• Les données sont publiées • L'OFROU est victime de chantage • Les données sont vendues au plus offrant
R6	Défaillance fonctionnelle	• Défaillance des systèmes centraux, du contrôle-commande, de l'alarme	• Perte de la vue d'ensemble centrale • Défaillance de l'alarme EES

		•	Défaillance des systèmes décentralisés	•	Restrictions de circulation sur les routes nationales suisses • Défaillance de composants EES • Danger pour les personnes
R7	Dysfonctionnement	•	Dysfonctionnement d'origine technique	•	Restrictions de circulation sur les routes nationales suisses • Défaillance de composants EES • Danger pour les personnes
R8	Vandalisme	•	Les composants non protégés de la EES sont manipulés	•	Restrictions de circulation sur les Routes nationales • Défaillance de composants EES • Destruction d'appareils OT
R9	Perte de données	•	Les données relatives à la commande EES sont perdues • Perte de données sensibles • Perte des sauvegardes	•	La perte de données de paramétrage d'une commande d'installation peut, dans certaines circonstances, avoir un impact significatif sur la disponibilité. • Les données historiques ne sont plus disponibles. Les optimisations sont retardées • Perte de documentation
R10	Redémarrage	•	Les systèmes ne peuvent plus être démarrés	•	Défaillance de l'alarme EES • Conduite difficile sur les Routes nationales • Défaillance de composants EES
R11	Absence de personnel	•	Les systèmes ne peuvent plus être servis • Les dysfonctionnements ne peuvent plus être corrigés	•	Les perturbations/alarmes ne sont pas traitées ; Circulation difficile sur les routes nationales • Défaillance des composants de la EES

5 Les règles : Processus, rôles et organisation

5.1 Aperçu

Les rôles et organes suivants concernent la sécurité OT :

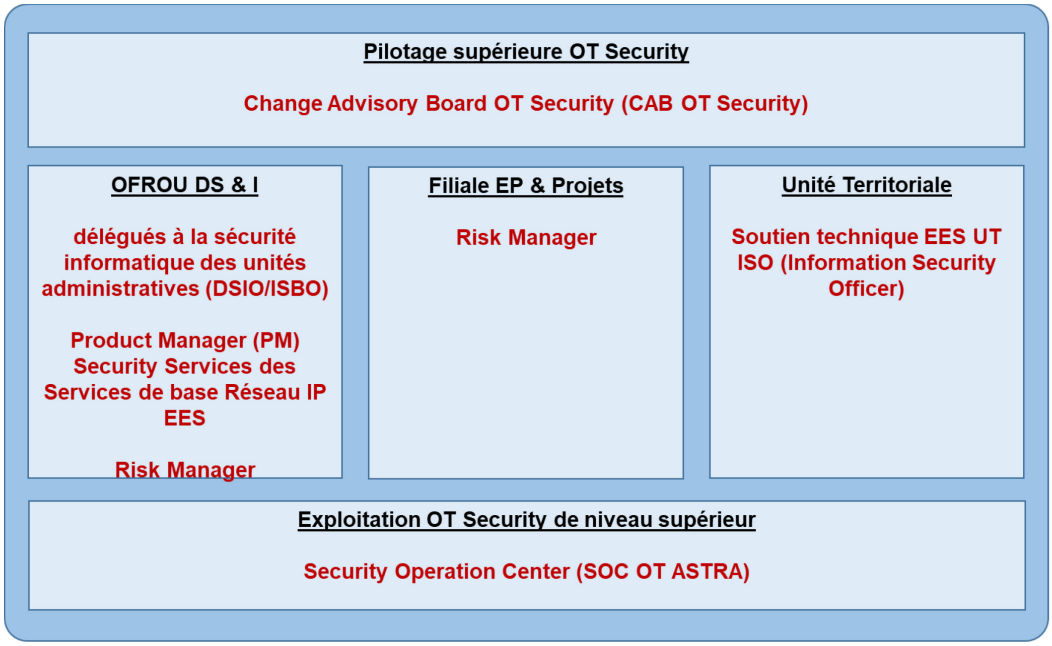

Fig. 5.1 Aperçu des rôles et des organes dans le contexte de la sécurité OT

Les rôles futurs et supplémentaires seront décrits lors de la révision des instructions 73001 et 73002 de l'OFROU.

5.2 Rôles de sécurité

Tab. 5.4 Rôles de sécurité

Rôle	Description	Emploi / Unité organisationnelle
Responsable de la sécurité informatique de l'organisation (ISBO) (selon ISO 27000, il s'agit du responsable de la sécurité de l'information)	L'ISBO coordonne les aspects liés à la sécurité des TIC au sein de l'OFROU ainsi qu'avec les services fédéraux de rang supérieur. Il élabore les bases nécessaires à la mise en œuvre des directives de sécurité TIC au niveau de l'OFROU. L'ISBO organise les analyses des besoins de protection (SCHUBAN) et est le point de contact à l'OFROU pour les problèmes de sécurité généraux.	OFROU DS
Gestionnaire de risques	Le Risk Manager s'occupe de l'analyse, de l'évaluation et de la gestion des risques. Il identifie les points faibles qui pourraient porter préjudice à l'OFROU d'un point de vue financier, opérationnel ou sécuritaire, les prévient et coordonne les propositions de solutions lors de leur mise en œuvre. Il est responsable de l'élaboration de stratégies, de processus et de systèmes de gestion et de surveillance des risques afin de protéger la continuité des activités.	Le rôle du risk manager est assumé de manière centralisée et au niveau des filiales de l'OFROU

Tab. 5.4 Rôles de sécurité

Rôle	Description	Emploi / Unité organisationnelle
Agent de sécurité de l'information (ISO)	L'ISO est une personne désignée par la direction de l'UT pour veiller, au nom de la direction, à ce que les exigences de sécurité soient couvertes dans le domaine de l'infrastructure OT (notamment le pare-feu) avec ses commandes industrielles et à ce que l'organisation de la sécurité issue du domaine ISO soit intégrée dans le système de gestion de la sécurité OT (OT-SMS).	Support technique EES Unité territoriale (FaS EES UT)
Chef de produit (PM) Security Services Services de base Réseau IP EES	Le chef de produit Security Services BD IP-Net EES est un rôle qui s'occupe de la mise en place et du développement des services et outils centraux tels que IAM EES, Multifactor Authentication/MFA, Single-Sign-On, Security Dashboard IP-Net EES, en étroite collaboration avec les parties prenantes OFROU, les filiales, les unités territoriales et les fournisseurs.	Chef de produit (PM) Security Services Services de base Réseau IP EES

5.3 Contrôle centrale de la sécurité OT

Le Change Advisory Board (CAB OT Security) coordonne la sécurité OT pour l'exploitation des EES et se charge de la gestion des changements pour les fonctions supérieures. Il prend également des recommandations ou des décisions concernant les tâches UT qui touchent à la sécurité.

Le CAB OT Security est un organe central au niveau de l'OFROU. Au minimum les rôles suivants doivent être représentés au sein du comité :

- Informatique Responsable du contrôle de gestion de l'organisation (ICBO) ;
- Responsable de la sécurité informatique de l'organisation (ISBO) ;
- Représentant I-B ;
- Représentant I-FU / soutien spécialisé EES SA-CH ;
- Direction du programme SA-CHt ;
- Au moins deux représentants de l'UT (ISO UT).

5.4 Centre opérationnel de sécurité OT (SOC OT ASTRA)

Le Security Operation Center OT (SOC OT ASTRA) est le point de contact central pour les questions de sécurité des systèmes OT des EES. Le SOC OT ASTRA utilise des personnes, des processus et des technologies pour surveiller et améliorer en permanence la situation de la EES en matière de sécurité, tout en prévenant, détectant, analysant et réagissant en temps réel aux incidents de cybersécurité.

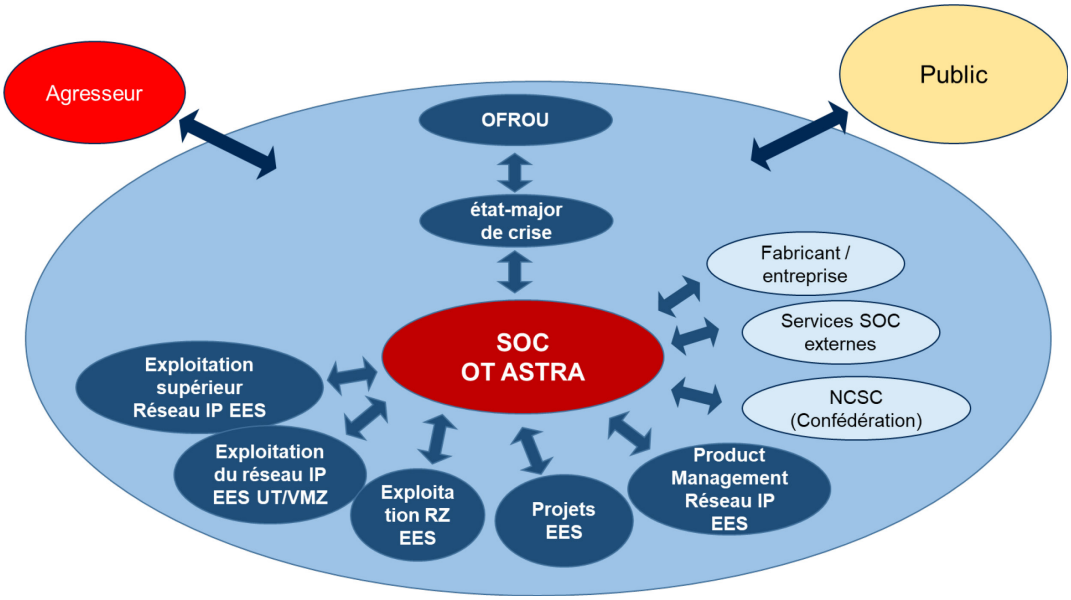

Fig. 5.2 Le SOC OT dans le contexte des parties prenantes

Le SOC OT OFROU disposera d'un personnel spécialisé et sera mis en place au cours des prochaines années.

6 Personnel : qualification, formation et sensibilisation

6.1 Savoir-faire, formation et sensibilisation

Tab. 6.5 Savoir-faire, formation et sensibilisation

ID	Description	
GS-1	Sensibilisation et formation	
	GS-1.1	Tous les utilisateurs de systèmes OT doivent être sensibilisés et formés dans le domaine de la sécurité OT en fonction de leur niveau ou de leur fonction.
	GS-1.2	Ils doivent connaître les directives d'utilisation pertinentes pour les systèmes OT et sont tenus de les respecter.
	GS-1.3	Ils doivent suivre chaque année une formation sur l'utilisation consciente des systèmes OT (formation de sensibilisation).
GS-2	Déclaration obligatoire	
	GS-2.1	Tous les utilisateurs de systèmes OT doivent signaler le plus rapidement possible les événements tels qu'un comportement anormal et suspect du système ou une perte physique au service compétent en la matière.
GS-3	Contrôle de sécurité des personnes (PSP)	
	GS-3.1	Les contrôles de sécurité des personnes ne sont en principe pas nécessaires.
	GS-3.2	Le contrôle de sécurité des personnes ne s'applique qu'aux personnes occupant des fonctions sensibles en matière de sécurité et ayant accès à des informations, du matériel ou des installations classifiés.
GS-4	Rôles de sécurité	
	GS-4.1	Les rôles de sécurité selon chap. 5.2 sont à pourvoir.

7 Technologie : Spécifications techniques

7.1 Principes

Pour la sécurité OT, on applique les mêmes principes que pour la construction de l'infrastructure EES. C'est-à-dire que la sécurité est également construite selon le principe de la pelure d'oignon (multicouche), comme toutes les installations EES. L'échange de données ne se fait que via des interfaces/accès définis et les réseaux d'unités territoriales sont fermés sur eux-mêmes.

Si un mécanisme échoue, un autre s'enclenche immédiatement pour déjouer une attaque. Cette approche multicouche avec des redondances ciblées augmente la sécurité d'un système dans son ensemble et cible de nombreux vecteurs d'attaque différents.

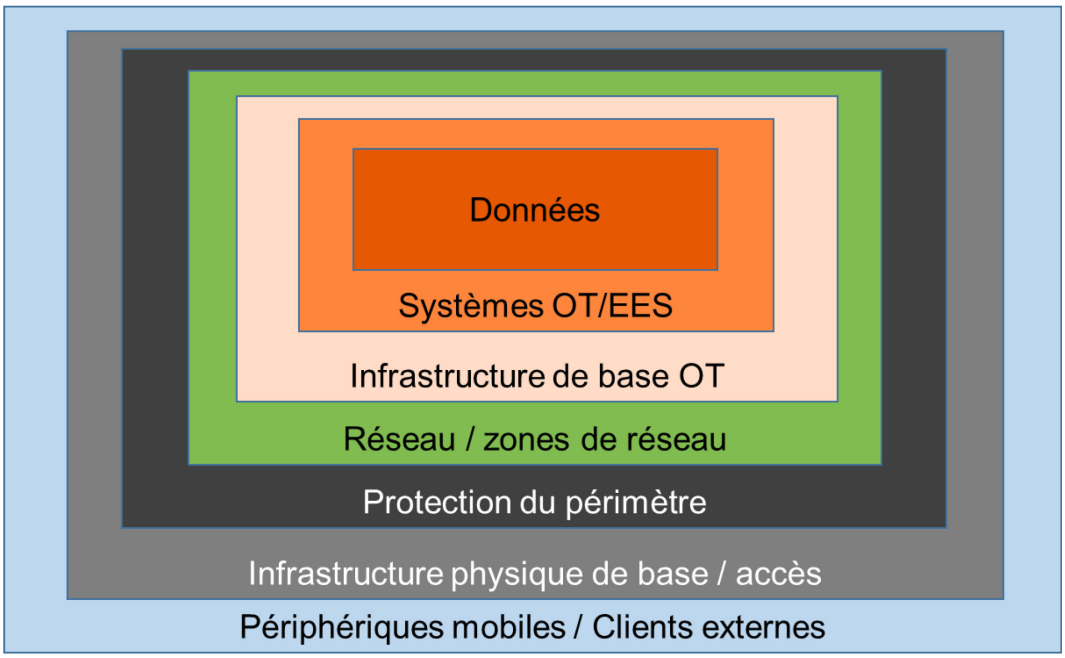

Fig. 7.1 Principe des exigences / mesures de sécurité à plusieurs niveaux – principe « Defense-in-Depth »

En outre, les principes suivants s'appliquent :

État de la technique : toutes les mesures de sécurité utilisées (préventives, détectives et/ou réactives) doivent correspondre à l'état de la technique, idéalement être standardisées et testées dans l'exploitation opérationnelle. Les mesures obsolètes ou pour lesquelles des vulnérabilités ou des points faibles importants sont connus doivent être améliorés ou remplacés en temps utile et indépendamment du cycle de vie. Par état de la technique, on entend le niveau de développement actuel des procédés, des installations et des modes d'exploitation qui a été testé avec succès dans des installations comparables en Suisse et à l'étranger ou qui a été utilisé avec succès lors d'essais et qui peut être transposé à d'autres installations selon les règles de l'art ; et qui est économiquement supportable.

Principe du « moindre privilège » ou du « besoin de savoir » : l'attribution des droits d'accès et des privilèges doit être minimale.

Principe « Security by Design » : lors du développement de composants matériels et logiciels ou de leur utilisation dans des systèmes et applications OT, la sécurité doit être prise en compte dès le départ et maintenue à jour, de manière à ce qu'ils soient aussi exempts que possible de points faibles et de vulnérabilités et que les possibilités d'attaque correspondantes soient réduites.

Principe « Security by Default » : les installations EES doivent être développées, configurées et exploitées de manière à ce que toutes les mesures de sécurité utiles dans un environnement spécifique soient activées par défaut et puissent déployer leurs effets sans que les utilisateurs aient à s'en préoccuper.

Traçabilité, piste d'audit : les systèmes doivent être conçus de manière à ce qu'en cas de dommage, la traçabilité des activités de l'utilisateur et du système puisse être présentée.

7.2 Protection de base

La protection de base définit la sécurité minimale qui doit être atteinte par tous les systèmes impliqués. Lorsqu'il existe des prescriptions de sécurité supplémentaires, celles-ci doivent être respectées. En cas de contradiction entre les dispositions, celles qui entraînent un niveau de sécurité plus élevé prévalent.

Lorsque des écarts justifiés par rapport à la protection de base sont nécessaires, ils doivent être documentés et validés par le CAB OT Security.

7.2.1 Informations (données)

Tab. 7.6 Protection de base Informations (données)

ID	Description	
GS-5	Admissibilité des systèmes OT	
	GS-5.1	Les informations importantes pour l'entreprise ne peuvent être stockées et traitées que sur des systèmes OT dont le propriétaire est soit une unité administrative de l'administration fédérale, soit pour lesquels le respect des exigences techniques de sécurité découlant de cette directive est réglé par contrat (p. ex. dans le cadre d'une solution RZ).
GS-6	Confidentialité et intégrité	
	GS-6.1	Les systèmes OT utilisés doivent être aptes à garantir la protection de la confidentialité et de l'intégrité des informations.
	GS-6.2	L'utilisation de procédés cryptographiques ne doit être prévue que dans les cas où elle est absolument nécessaire en raison du besoin de protection.
	GS-6.3	Lorsque des informations sont cryptées, les clés utilisées à cet effet doivent être gérées de manière à ce qu'une restauration et donc un décryptage des informations soient possibles à tout moment. En règle générale, cela implique une gestion complexe des clés (avec un mécanisme de « key recovery ») ainsi que des tests périodiques de la possibilité de récupérer les informations.
GS-7	Disponibilité, sauvegarde et restauration	
	GS-7.1	La disponibilité des informations importantes pour l'entreprise doit être assurée à tout moment en fonction des besoins de protection.
	GS-7.2	L'exploitant responsable des informations doit disposer d'une stratégie de sauvegarde et la mettre en œuvre. Cette stratégie doit prévoir un principe multigénérationnel et un stockage hors ligne des stocks de données importants, de sorte que les données puissent être récupérées même en cas de logiciels malveillants de chiffrement des données (« ransomware »).
	GS-7.3	La restauration des données (restore) doit être testée au moins une fois par an. En outre, la restauration doit être testée à chaque fois que les systèmes OT subissent des changements fondamentaux.
GS-8	Support de données	
	GS-8.1	Les supports de données sur lesquels sont enregistrées des informations importantes pour l'entreprise doivent être protégés à tout moment en fonction du besoin de protection des informations. Des processus appropriés doivent être définis et mis en œuvre, notamment pour la réparation et l'élimination des supports de données.
	GS-8.2	L'utilisation de supports de données mobiles, tels que les clés USB, etc.

7.2.2 Systèmes OT

Tab. 7.7 Systèmes OT

ID	Description	
GS-9	Configuration et réglage	
	GS-9.1	Avant sa mise en service dans l'environnement de production, un système OT doit être configuré et réglé de manière à être protégé contre tout accès non autorisé, à être durci dans la mesure où cela est techniquement possible et à être exploité dans une configuration minimale nécessaire à l'accomplissement des tâches et non modifiable par l'utilisateur (c'est-à-dire que les interfaces, modules, services et fonctions non utilisés doivent être désactivés), et à ce que les activités et événements importants pour la sécurité soient enregistrés (avec indication de l'heure) et évalués en temps réel.
	GS-9.2	Les configurations et paramètres de sécurité ne peuvent être activés, modifiés, désactivés et désinstallés que par des personnes autorisées.
GS-10	Environnement productif	
	GS-10.1	L'environnement productif du système OT doit être séparé de l'environnement non productif éventuellement présent (par ex. pour le développement et/ou les tests).
GS-11	Maintenance et entretien	
	GS-11.1	Une maintenance et un entretien professionnels doivent être assurés pendant toute la durée de vie d'un système OT et de ses composants (p. ex. bibliothèques de logiciels, pilotes). Cela comprend notamment l'installation de mises à jour et de corrections d'erreurs (patches) régulières et nécessaires pour l'exploitation ou la sécurité. Les contrats de maintenance et d'assistance nécessaires à cet effet doivent être prévus.
	GS-11.2	Le matériel et les logiciels doivent en principe être remplacés avant la fin du support.
GS-12	Protection de l'intégrité et des logiciels malveillants	
	GS-12.1	L'intégrité des composants logiciels utilisés sur le système OT doit être garantie (par ex. à l'aide de signatures numériques). En particulier, chaque système serveur nécessitant une protection accrue doit être soumis régulièrement à un contrôle d'intégrité.
	GS-12.2	Si une perte d'intégrité est constatée, le système OT doit être déconnecté du réseau, sauvegardé et analysé. En cas de compromission confirmée, il convient d'examiner la marche à suivre en fonction du système OT et des logiciels malveillants reçus (redémarrage, remplacement, etc.).
	GS-12.3	Le système OT doit être intégré dans un concept de protection contre les logiciels malveillants, qui règle en particulier la manière de procéder en cas d'attaque par un logiciel malveillant et quels services doivent être informés et comment.
GS-13	GS-13.1	Pour les systèmes OT critiques, des processus d'urgence et des scénarios de redémarrage doivent être préparés en cas de panne ou de panne partielle de ces systèmes. Ces processus d'urgence et scénarios de redémarrage doivent être régulièrement exercés et améliorés, en particulier pour les systèmes OT relevant de la sécurité.
GS-14	GS-14.1	Pour toute modification d'un système OT, un processus de gestion des changements défini doit être respecté. En mode ordinaire, c'est l'unité territoriale qui en est responsable, en mode projet, les modifications se font selon les directives de la filiale. Les systèmes centraux du niveau gestion relèvent de la responsabilité des prestataires de services concernés.

7.2.3 Infrastructure de base OT

Tab. 7.8 Infrastructure de base OT

ID	Description
GS-15	Exploitation
	GS-15.1 Le système OT doit être exploité en respectant les consignes et recommandations de sécurité en vigueur dans le secteur (« meilleures pratiques »).
GS-16	Identités, rôles et autorisations
	GS-16.1 Pour chaque système OT exploité dans le domaine nationalstrassen.admin.ch, il doit exister un concept d'autorisation qui règle l'attribution des autorisations sur la base du principe « Need-to-Know ». Les autorisations doivent être attribuées de manière à ce qu'un utilisateur ne puisse effectuer que les activités prévues.
	GS-16.2 Les identités et les rôles des utilisateurs doivent être gérés par l'IAM EES. En particulier, la nécessité et l'exactitude des identités d'utilisateurs doivent être vérifiées au moins une fois par an et les utilisateurs qui ne sont plus nécessaires doivent être supprimés.
	GS-16.3 Tous les droits d'accès à un système OT doivent être gérés dans le cadre d'un processus défini et documenté et doivent toujours être tenus à jour. En particulier, la nécessité et l'exactitude des droits doivent être vérifiées au moins une fois par an par l'exploitant et les droits qui ne sont plus nécessaires doivent être supprimés.
GS-17	Connexion et authentification des utilisateurs
	GS-17.1 L'accès aux systèmes OT est basé sur des logins personnels.
	GS-17.2 L'authentification d'un utilisateur par rapport à un système OT doit se faire au moyen d'une authentification à 2 facteurs. Si la connexion d'un utilisateur s'effectue à partir d'un poste de commande fixe directement raccordé au réseau OT, à l'intérieur d'un local surveillé de l'UT/OFROU, une authentification au moyen d'un ID utilisateur et d'un mot de passe est suffisante.
	GS-17.3 Les comptes/logins de groupe ne sont en principe pas autorisés.
GS-18	Mots de passe Les exigences suivantes s'appliquent à l'authentification de l'utilisateur par mot de passe.
	GS-18.1 Le mot de passe • doit être personnel ; • ne doit pas être divulgué ; • ne doit pas être noté. Le mot de passe peut toutefois être géré dans un coffre-fort de mots de passe, par exemple ; • doit comporter au moins 12 caractères, provenant d'au moins trois des quatre catégories suivantes : lettres majuscules et minuscules, chiffres et caractères spéciaux ; • peut également commencer par une lettre minuscule, un chiffre ou un caractère spécial ; • peut aussi être une phrase telle que « aujourd'hui à 12 heures, j'ai changé 12$ » ; • n'a pas de durée de validité maximale.
	GS-18.2 Un mot de passe initial défini administrativement doit être modifié lors de sa première utilisation.
	GS-18.3 Si le mot de passe est modifié, il faut s'assurer que le nouveau mot de passe ne correspond à aucun des 10 derniers mots de passe utilisés.
	GS-18.4 Après 5 saisies erronées au maximum, le mot de passe doit être bloqué et ne peut être libéré que dans le cadre d'un processus défini.
	GS-18.5 En cas de suspicion (ou de confirmation) de prise de connaissance par des personnes non autorisées ou d'abus, le mot de passe doit être immédiatement modifié.
	GS-18.6 Côté serveur, il faut s'assurer que le mot de passe ne puisse jamais être lu en clair ou facilement compromis dans le cadre d'une autre attaque.
	GS-18.7 Les mots de passe ne doivent être modifiés qu'en cas de suspicion d'abus.
	GS-18.8 Auto-logout ou écran de verrouillage après une période d'inactivité de xy min (sauf clients spéciaux, par ex. centrale).

GS-19	Accès administratifs et à distance
	GS-19.1 Les accès administratifs aux systèmes OT doivent être effectués de manière documentée et contrôlée. En particulier, ces accès doivent être effectués au moyen de protocoles sécurisés, être enregistrés de manière compréhensible et pouvoir être évalués.
	GS-19.2 L'utilisation des comptes (privilégiés) correspondants doit pouvoir être attribuée à une personne. En outre, les comptes ne doivent disposer que des droits d'accès minimaux nécessaires et si possible de courte durée.
GS-20	Surveillance, journalisation
	GS-20.1 Tous les systèmes OT doivent être activement surveillés (concept de monitoring), dans la mesure où cela est techniquement possible. De même, un logging doit être activé et les logs doivent être analysés systématiquement et en temps réel, afin que les anomalies telles que les tentatives d'attaque, les comportements erronés, les problèmes de matériel, etc. puissent être détectées à temps.
	GS-20.1 Les fichiers journaux ou logs doivent être conservés au moins 12 mois. Il faut s'assurer que les données log restent protégées et ne sont pas manipulées.

7.2.4 Réseau / zones de réseau

Tab. 7.9 Réseau / zones de réseau

ID	Description
GS-21	Réseau fermé (valable par analogie pour les réseaux existants de l'UT)
	GS-21.1 Le réseau IP EES doit être exploité comme un réseau fermé au sens d'un réseau OT. La séparation avec les réseaux Office doit être strictement respectée. Les prescriptions sont définies dans la directive OFROU 13040 Réseau IP EES.
GS-22	Modèle de zone (valable pour les nouveaux réseaux IP EES UT, non applicable aux réseaux existants des UT)
	GS-22.1 Le réseau IP EES met en œuvre un modèle de zone conforme au modèle de zone de la Confédération.
GS-23	NSP réseau IP EES (s'applique aux nouveaux réseaux IP EES UT, non applicable aux réseaux existants des UT)
	GS-23.1 La documentation OFROU 83042 Network Security Policy Réseau IP EES (NSP Réseau IP EES) règle la mise en place et l'exploitation du modèle de zone. Elle fait office de politique pour toutes les zones mises en œuvre dans le périmètre du réseau IP EES. Toute dérogation à cette règle doit être justifiée par les opérateurs concernés et consignée par écrit. Une validation est effectuée par le CAB OT Security.
GS-24	Appartenance à une zone (valable pour les nouveaux réseaux IP EES UT, non applicable aux réseaux existants des UT)
	GS-24.1 Chaque système OT doit appartenir à une zone de réseau et satisfaire aux exigences de politique correspondantes de la Network Security Policy IP-Net EES (NSP IP-Net EES) et être exploité conformément à la NSP IP-Net EES.
	GS-24.2 Les systèmes OT doivent être inventoriés.
GS-25	WLAN (valable par analogie pour les réseaux existants des UT)
	GS-25.1 Le WLAN est en principe autorisé et s'effectue conformément aux directives de la Network Security Policy Réseau IP EES.

7.2.5 Protection du périmètre

Tab. 7.10 Protection du périmètre

Protection du périmètre	
ID	**Description**
GS-26	Accès à distance
GS-26.1	L'accès à distance (Remote Access) s'effectue de manière centralisée via les deux points d'accès dans les services de base Réseau IP EES BD A/B conformément aux directives de la NSP Réseau IP EES.
GS-26.2	L'accès à distance s'effectue toujours au moyen d'une authentification à deux facteurs.
GS-26.3	Durant la phase de migration du réseau IP EES, les accès à distance peuvent encore être effectués via les accès externes locaux dans les réseaux des unités territoriales. En principe, les directives de la NSP Réseau IP EES doivent également être suivies.
GS-26.4	En principe, les accès à distance (remote access) ne doivent être ouverts que pour une durée limitée et doivent être surveillés. Il faut s'assurer qu'un utilisateur doit se reconnecter après 24h maximum.
GS-26.5	Pendant un accès à distance, les utilisateurs doivent fermer leur session lorsqu'ils quittent leur poste de travail.
GS-26.6	Les jumphosts doivent être utilisés pour les accès à distance afin d'accéder aux systèmes OT. Des outils administratifs pour la maintenance, le diagnostic et la configuration doivent être installés sur ces Jumphosts.
GS-26.7	Les accès à distance et les transferts de données doivent être activés séparément. Les données ne peuvent être transférées qu'avec l'accord de l'exploitant.
GS-27	Internet
GS-27.1	Les accès directs d'Internet aux systèmes OT du réseau IP EES ne sont pas autorisés. De même, les accès directs à Internet depuis les systèmes OT du réseau IP EES ne sont pas autorisés.
GS-27.2	Les connexions Internet doivent être limitées au minimum et se faire via l'infrastructure DMZ des services de base, conformément aux directives de la NSP Réseau IP EES.

7.2.6 Infrastructure physique / accès

Tab. 7.11 Infrastructure physique / accès

ID	**Description**
GS-28	Principe
GS-28.1	L'accès physique aux systèmes EES est réservé aux personnes autorisées.
GS-29	Locaux verrouillables
GS-29.1	Les systèmes OT doivent être placés dans des locaux ou des conteneurs pouvant être fermés à clé. Les capteurs ou actionneurs installés obligatoirement de manière ouverte doivent être surveillés par le système de commande correspondant afin d'éviter tout accès non autorisé et toute manipulation.
GS-29.2	Les postes de travail des opérateurs, les systèmes de serveurs et de stockage doivent être exploités dans des locaux protégés et verrouillables.
GS-30	Normes définies
GS-30.1	Les locaux techniques et les centrales de tunnel doivent être construits et exploités conformément aux normes définies par l'OFROU.
GS-31	Accès aux locaux techniques
GS-31.1	L'accès aux locaux techniques dans les centres d'entretien, les bases, les centrales, etc. ou l'accès aux cabines, aux boîtes de commande, etc. avec des systèmes OT doit être limité et clairement réglementé.
GS-31.2	Les accès aux locaux techniques contenant des systèmes de serveurs doivent être traçables (logging),
GS-31.3	Des concepts de fermeture et d'accès doivent être disponibles. Le cas échéant, surveillance vidéo si seul l'accès physique par clé est possible.

7.2.7 Appareils mobiles et appareils tiers

Tab. 7.12 Périphériques mobiles / clients externes

ID	Description
GS-32	Clients externes
	GS-32.1 Les clients externes (appareils non exploités par l'OT) ne reçoivent pas d'accès direct au réseau IP EES et sont toujours considérés comme des appareils tiers (s'applique également aux appareils des fournisseurs de systèmes). L'accès se fait par le biais de la protection du périmètre.
	GS-32.2 Un accès direct aux systèmes OT, par exemple pour des mises en service ou des urgences, par un appareil tiers n'est autorisé que si l'exploitant l'autorise explicitement.
GS-33	Appareils mobiles
	GS-33.1 Les appareils mobiles ne reçoivent pas d'accès direct au réseau IP EES et sont toujours considérés comme des appareils tiers (s'applique également aux appareils des fournisseurs de systèmes et aux appareils de la propre entreprise). L'accès se fait toujours via la protection du périmètre.

Glossaire

Terme/abréviation	Begriff/Abkürzung	Définition
AKS-CH	AKS-CH	structure et désignation des équipements d'exploitation et de sécurité
anneau de raccordement	Erschliessungsring	structure de réseau supérieure qui relie tous les segments IP d'une UT. Mise en œuvre technologique par le MPLS ou le SR (Segment Routing).
architecture du système	Systemarchitektur	modèle d'un système qui décrit la relation et les propriétés des différents éléments et de leurs fonctions.
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 (services de base)	BD (Basisdienste)	services de base pour le réseau (outil IPAM, DNS, sources d'horloge/temps, …) pour l'ensemble du réseau IP EES
BGP	BGP (iBGP/eBGP)	protocole de routage IP offrant de multiples fonctions pour l'échange d'informations topologiques complexes. Dans ce contexte, iBGP est utilisé comme protocole interne au réseau et eBGP à la transition externe vers les réseaux tiers (de l'anglais : Border Gateway Protocol).
CAB	CAB	Change Advisory Board
client/hôte serveur	Client/Host Server	termes génériques TIC, sans signification particulière pour les EES, utilisation dans le contexte des protocoles standardisés.
Concept SIPD	ISDS-Konzept	le concept de sûreté de l'information et de protection des données est la base de la définition des mesures de sûreté de l'information et de protection des données. Il indique quels sont les risques résiduels liés à l'exploitation du système informatique et à l'organisation. Il décrit le concept d'urgence.
Commande d'installation	AS	abréviation de l'allemand « Anlagesteuerung »
commutateur	Switch	signifie toujours les éléments réseau L2 du niveau d'accès, autrement mentionné explicitement
DAB	DAB	radiodiffusion numérique (de l'anglais « *Digital Audio Broadcoasting* »)
DDI	DDI	DNS, DHCP and IP Address Management
DHCP	DHCP	protocole de communication dans la technique informatique, permettant à un serveur d'attribuer une configuration réseau à des clients et défini dans la norme RFC 2131 et s'est vu attribuer les ports UDP 67 et 68 par l'IANA (« *Internet Assigned Numbers Authority* ») (de l'anglais « *Dynamic Host Configuration Protocol* »).
DMZ	DMZ	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 (zone démilitarisée).
DNS	DNS	le « système de noms de domaine » (de l'anglais « *Domain Name System* ») est l'un des services les plus importants pour 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.
domaine	Domäne	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 ;

Terme/abréviation	Begriff/Abkürzung	Définition
		- domaine métier : regroupement de différents services métier ; - domaine de processus : regroupement de différents processus.
EES	BSA	équipements d'exploitation et de sécurité
élément réseau	Netzwerkelement	limité à l'équipement actif de communication (routeur ou commutateur)
équipement	Ausrüstung/Gerät	toute sorte d'équipement actif dans un contexte large des EES (même sans connexion au réseau IP EES)
équipement réseau	Netzwerkausrüstung	équipement actif et composant passifs dans un contexte large de réseau (inclus les firewalls, systèmes de gestion, sources d'horloge).
équipement terminal	Endgerät	toute sorte d'équipement connecté à un Userport du réseau IP EES
ERPS	ERPS	Ethernet Ring Protection Switching, ou ERPS, est un protocole standard selon ITU-T G.8032 sur la couche 2 pour garantir des temps de commutation de redondance déterministes inférieurs à 50 ms dans des structures en anneau complexes.
F/filiale	F/Filiale	filiale (cinq structures régionales de l'OFROU
firewall/pare-feu	Firewall	un pare-feu est un système de sécurité qui protège un réseau informatique ou un équipement individuel contre les accès indésirables au réseau
GUI	GUI	Interface utilisateur graphique (de l'anglais « *Graphical User Interface* »
IAM BSA	IAM BSA	Identity Management System BSA
IEC/CEI	IEC	l'organisation internationale de normalisation chargée des domaines de l'électricité, de l'électronique. Pour des beaucoup d'applications industrielles elle intègre la technologie réseau dans ses normes.
IEEE	IEEE	l'Institute of Electrical and Electronics Engineers est une association professionnelle qui crée entre autres activités des standards pour la technologie, le hardware et le software. En particulier dans le domaine de la technologie Ethernet l'IEEE est l'organisation déterminante.
IETF	IETF	l'Internet Engineering Task Force (IETF) élabore et promeut des standards Internet, en particulier les standards qui composent la suite de protocoles Internet. De facto l'IETF est l'organisation de la standardisation de toute la technologie IP.
IP	IP	Internet Protokoll
IPAM	IPAM	IP Address Management
ISO	ISO	Information Security Officer
ITU-T/UIT-T	ITU-T	l'Union internationale des télécommunications ou UIT (en anglais : International Telecommunication Union ou ITU) est l'agence des Nations unies pour le développement spécialisé dans les technologies de l'information et de la communication. Le secteur ITU-T crée des normes pour la télécommunication.
LDP	LDP	un protocole pour gérer et distribuer sur l'ensemble d'un réseau MPLS les chemins logiques (en anglais : label switched paths). De l'anglais Label Distribution Protocol.
LS	LS	commande locale (abréviation de l'allemand « *Lokalsteuerung* »)
monitoring	Monitoring	surveillance et visualisation des fonctions techniques des installations et des systèmes
NAC	NAC	Network Access Control (contrôle de l'accès au réseau)
NCSC	NCSC	Centre national pour la cybersécurité

Terme/abréviation	Begriff/Abkürzung	Définition
niveau d'accès	Access-Bereich	structure L2, mettant à disposition les interfaces d'accès (Userport) aux équipements terminaux.
niveau gestion	Leitebene	voir niveau processus
niveau gestion	Betriebsleitebene	ce niveau propose la surveillance et l'utilisation de toutes les installations au moyen de serveur de gestion de l'exploitation, d'une part par la police en ce qui concerne les événements et les aspects particuliers de l'exploitation, d'autre part par le service d'entretien en ce qui concerne la disponibilité fonctionnelle des installations. Les ordinateurs de gestion d'exploitation sont reliés aux AR par un réseau de communication. Autre désignation : niveau de contrôle supérieur
niveau management (ou ME)	Management-Ebene (oder ME)	niveau gestion central supérieur
niveau processus	Prozessleitebene	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 (réflexes du tunnel) ont lieu à l'intérieur d'une section au moyen d'un AR
NMS	NMS	Network Management System
NNI (anneau de raccordement)	NNI (Erschliessungsring)	La network-to-network interface (NNI) est l'interface entre deux éléments réseau dans l'anneau de raccordement. Contrairement aux Userports les NNI n'acceptent ni des commutateurs du niveau d'accès ni des équipements terminaux.
(partie d')installation	(Teil-)Anlage	limité au sens strict des définitions de l'AKS
QoS	QoS	La « qualité de service » (de l'anglais « *Quality of Service* ») décrit la qualité d'un service de communication du point de vue de l'utilisateur, à savoir à quel point la qualité du service correspond aux exigences de ce dernier.
région EES	BSA-Region	Anlagenspezifisch definierte Region, in der es eine regional übergeordnete Steuerung gibt
réseau IP EES	IP-Netz BSA	le réseau national pour les EES comprenant les éléments (réseaux partiels) suivants :
UT	GE	- 11 réseaux IP EES UT ;
UT section	GE Abschnitt	- la dorsale nationale (réseau IP EES Backbone) ;
BD	BD	- le réseau de la VMZ-CH ;
VMZ	VMZ	- l'interconnexion aux RZ BSA (centre de calculs EES) ;
Backbone	Backbone	- les services de base (BD) sur deux sites.
RFC	RFC	Les requests for comments (RFC), littéralement « demande de commentaires », sont une série numérotée de documents officiels décrivant les aspects et spécifications techniques d'Internet, ou de différents matériels informatiques. Peu de RFC sont des standards qui représentent un consensus de l'industrie, mais tous les documents publiés par l'IETF sont des RFC.
routeur	Router	signifie toujours les routeurs (IP/MPLS ou SegementRouting) des anneaux de raccordement, autrement (p.e. routeur Spoke-Site) mentionné explicitement
routeur	Router	les routeurs (ou routeurs de réseau) sont des éléments réseau qui peuvent transmettre des paquets IP entre plusieurs réseaux informatiques p.e. les segments du réseau IP EES).
RSVP	RSVP	plus précisément RSVP-TE (en anglais : Resource Reservation Protocol - Traffic Engineering) sert à l'établissement des chemins (en anglais : path) pour la technologie MPLS qui est à la base du Réseau IP EES.
rVDE	rVDE	Regionale Verkehrsdatenerfassung
rVL	rVL	Gestion régionale du trafic (abréviation de « regionale Verkehrslenkung »)

Terme/abréviation	Begriff/Abkürzung	Définition
RZ(-EES)	RZ(-BSA)	centre de calcul EES (de l'allemand: Rechenzentrum BSA)
SAP	SAP	dans le réseau IP EES, les « points d'accès au service » (de l'anglais « Service Access Point ») sont en général des ports physiques d'un commutateur ou d'un routeur
section	Abschnitt	la section logique, pas le tronçon physique
section EES	BSA-Abschnitt	section de route nationale géré par un serveur de gestion de section
section (IP)	(IP) Abschnitt	la section logique du réseau, pas le tronçon physique.
segment (de réseau)	(Netzwerk-)Segment	segments selon ASTRA 83040 par (partie d')installation, usuellement réalisés par des VLAN
Segment Routing/SR	Segment Routing/SR	SR est un successeur possible de MPLS qui permet la transmission de paquets le long d'un chemin préalablement établi pour former des réseaux virtuels L2 et L3
Serveur de gestion section	AR	Serveur de gestion section (abréviation de l'allemand « Abschnittsrechner »)
service	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.
SPB	SPB	le Shorted Path Bridging, ou SPB, est un protocole standard selon IEEE 802.1aq sur la couche 2 pour garantir des temps de commutation de redondance déterministes dans n'importe quelle topologie et pour utiliser les ressources de manière optimale.
système de commande/gestion	Leittechnik	Funktionen und Komponenten, die der Überwachung und Leitung von Anlagen dienen.
système de gestion	Leitsystem	sert aux opérateurs pour la surveillance et la commande des installations.
système SCADA	SCADA-System	système informatique interconnecté (système de gestion) affecté à la surveillance, à la commande et à l'optimisation d'installations industrielles (de l'anglais « *Supervisory Control and Data Acquisition* »)
UeLS	UeLS	Übergeordnetes Leitsystem
ULA	ULA	Adresse locale unique (de l'anglais « *Unique Local Address* »)
UNI (anneau de raccordement)	UNI (Erschliessungsring)	les User-Netzwerk-Interfaces (UNI) sont les interfaces des éléments de réseau dans l'anneau de raccordement avec les commutateurs du niveau d'accès.
uplink (niveau accès)	Uplink (Access-Layer)	L'interface Ethernet du niveau d'accès (Uplink du commutateur) pour la connexion à l'UNI du routeur dans l'anneau de raccordement.
userport (niveau accès)	Userport (Access-Layer)	l'interface Ethernet physique au niveau d'accès pour connecter les équipements terminaux au réseau IP EES.
UT	GE	unité territoriale (11 structures supracantonales, exploitant leur réseau IP EES UT).
VM-CH	VM-CH	Gestion du trafic en Suisse (abréviation de l'allemand « *Verkehrsmanagement Schweiz* »)
VMZ(-CH)	VMZ(-CH)	Centrale suisse de gestion du trafic (abréviation de l'allemand « *Verkehrsmanagementzentrale Schweiz* »)
WDM	WDM	utilisation multiple (multiplex) d'une FO par plusieurs longueurs d'ondes optiques (engl. Wavelength Division Multiplex)
zone (de réseau)	(Netzwerk-)Zone	selon la NSP de la Confédération Si003 (séparées par la PEZ).

Bibliographie

Instructions et directives de l'OFROU

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

[2] Office fédéral des routes OFROU, « **Architecture des systèmes de gestion et de commande des équipements d'exploitation et de sécurité** », *directive OFROU 13031*, www.astra.admin.ch.

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

Liste des modifications

Édition	Version	Date	Modifications
2024	2.00	11.01.2024	Version révisée.
2016	1.21	15.12.2018	Publication de la version française. Modifications formelles.
2016	1.20	11.12.2017	Adaptations consécutives à l'introduction du réseau IP EES (Rili 13040).
2016	1.10	01.03.2016	Entrée en vigueur de l'édition 2016.