Recommandation de la branche

Sécurité physique pour les sous-stations

Niveaux de réseau 1 et inférieurs (pour les sous-stations utilisées en commun avec le niveau de réseau 1)

SPS – CH 2019

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Téléphone +41 62 825 25 25, Fax +41 62 825 25 26, info@electricite.ch, www.electricite.ch

Impressum et contact

Éditeur
Association des entreprises électriques suisses AES
Hintere Bahnhofstrasse 10
CH-5000 Aarau
Téléphone +41 62 825 25 25
Fax +41 62 825 25 26
info@electricite.ch
www.electricite.ch

Auteurs de la première édition

Christian Brütsch	Repower	
Heinz Götschi	CFF Énergie	Depuis juin 2017
Beat Hanselmann	Services municipaux de la ville de Winterthour	
Robert Hauser	ewz	
Hans-Peter Mölbert	Swissgrid	
Lukas Petrig	Alpiq	
Theodor Pfister	BKW	
Beat Schüpbach	Swissgrid	Responsable du groupe de travail
Olivier Stössel	VSE / AES	Secrétaire de la Commission EAE-TSO
Beat Stucki	CFF Énergie	Jusqu'en juin 2017
Martin Wolf	CKW	
Roland Ziegler	Axpo	

Responsabilité commission
La Commission EAE-TSO de l'AES est désignée responsable de la tenue à jour et de l'actualisation du document.

Chronologie

De juillet 2016 à mars 2018	Élaboration du document
De novembre 2018 à février 2019	Consultation
5. mai 2019	Approbation par le Comité de l'AES

Ce document a été élaboré avec l'implication et le soutien de l'AES et de représentants de la branche.

L'AES a approuvé ce document à la date du 05.05.2019.

Imprimé n° SPS/f, édition 2019

Égalité linguistique des sexes
La forme masculine est utilisée par défaut dans ce document afin d'en faciliter la lecture. Tous les rôles et toutes les désignations de personnes sont néanmoins susceptibles de se rapporter aussi bien à des femmes qu'à des hommes. Nous vous remercions pour votre compréhension.

Table des matières

Liste des figures

Liste des tableaux

Avant-propos

Le présent document est un document de la branche publié par l'AES. Il fait partie d'une large réglementation relative à l'approvisionnement en électricité sur le marché ouvert de l'électricité. Les documents de la branche contiennent des directives et des recommandations reconnues à l'échelle de la branche concernant l'exploitation des marchés de l'électricité et l'organisation du négoce de l'énergie, répondant ainsi à la prescription donnée aux entreprises d'approvisionnement en électricité (EAE) par la Loi sur l'approvisionnement en électricité (LApEl) et par l'Ordonnance sur l'approvisionnement en électricité (OApEl).

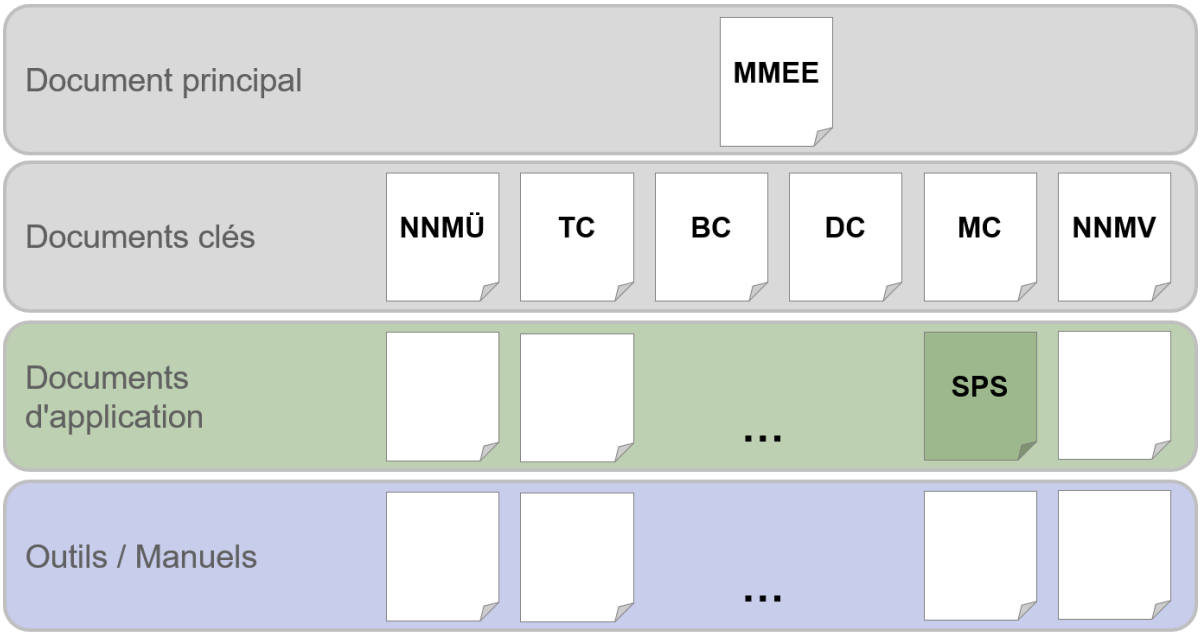
Les documents de la branche sont élaborés par des spécialistes de la branche selon le principe de subsidiarité; ils sont régulièrement mis à jour et complétés. Les dispositions qui ont valeur de directives au sens de l'OApEl sont des normes d'autorégulation.

Les documents sont répartis en quatre catégories hiérarchisées:

- Document principal: Modèle de marché pour l'énergie électrique – Suisse (MMEE–CH)
- Documents clés
- Documents d'application
- Outils / Logiciels

La présente norme de sécurité physique pour les sous-stations constitue un document d'application.

Structure des documents



Résumé

Le présent document, s'appuyant sur le guide PIC de l'Office fédéral de la protection de la population (OFPP), constitue un manuel pour le développement efficace et concret de mesures de sécurité dans les sous-stations des niveaux de réseau 1 et inférieurs (pour les sous-stations utilisées en commun avec le niveau de réseau 1).

Il donne également une vue d'ensemble des normes minimales recommandées dans le domaine de la protection physique de telles sous-stations. Il peut aussi servir de guide pour la protection des sous-stations dépourvues d'installations de niveau de réseau 1. Cela présuppose cependant que les travaux préliminaires nécessaires, tels que la définition de la criticité des installations et l'évaluation des risques, soient également menés à bien.

L'analyse exhaustive des menaces existantes et des dangers significatifs qui en découlent permet d'identifier et d'évaluer les risques concrets encourus (probabilité d'occurrence et ampleur des dommages potentiels). Cette analyse devrait être effectuée pour chaque sous-station ou pour chaque groupe de sous-stations[1] présentant des caractéristiques similaires.

Dans un deuxième temps, les objectifs de protection, qui peuvent varier suivant l'entreprise et l'importance de l'installation, sont définis.

Des mesures appropriées pour la réduction des risques définis sont ensuite élaborées sur cette base.

Il peut s'agir par exemple de solutions techniques liées à la protection du périmètre de la sous-station, parmi lesquelles l'intégration à la protection de base d'un système de fermeture électronique.

Pour ce faire, il convient de prendre en considération la criticité de la sous-station (importance de l'installation pour le réseau entier et pour la sécurité d'approvisionnement) lors de la planification desdites mesures de sécurité.

Les normes formulées dans le présent document tiennent en outre compte des normes régulatoires et légales qui se reflètent dans la définition des mesures de protection dites «de base».

Des mesures complémentaires de protection dite «moyenne» et «haute» peuvent être appliquées pour des sous-stations présentant une criticité plus élevée. Pour ce faire, une comparaison entre les investissements dans des mesures de sécurité et leur impact sur la réduction des risques est utile.

Il est ensuite question de l'importance des mesures opérationnelles (sensibilisation, etc.), en complément des solutions techniques précitées.

Étant entendu que seule la prise en compte de l'ensemble des paramètres de sécurité permet une solution globale efficace et pertinente, la dernière section du document est consacrée à l'interaction entre les mesures de protection physique et celles touchant à la cybersécurité.

[1] Une sous-station peut également être appelée «poste de transformation HT/MT».

Introduction

Les changements ayant eu lieu ces dernières années dans le paysage électrique suisse en lien avec la séparation des activités entre le réseau et la production («unbundling») dans le secteur électrique se répercutent sur le niveau de criticité des différents risques. Le transfert de la totalité des actifs du réseau de transport à la société nationale du réseau a accru le risque d'une défaillance totale, pouvant affecter par exemple le pilotage de la totalité du réseau de transport. Ce risque cumulé de défaillance n'existait auparavant pas sous cette forme.

À cela s'ajoute la forte augmentation de l'utilisation de technologiques numériques survenue ces dernières années, qui s'accompagne elle aussi de nouveaux risques. Ces derniers doivent être identifiés, évalués et traités par les entreprises énergétiques, afin qu'elles puissent remplir leur mandat légal, conformément à la Loi sur l'approvisionnement en électricité, à l'Ordonnance sur l'approvisionnement en électricité ou à la Loi sur l'énergie.

L'Office fédéral pour l'approvisionnement économique du pays (OFAE) a réalisé une analyse des risques et des vulnérabilités du sous-secteur lié à l'approvisionnement électrique. Ses (principales) conclusions sont les suivantes:

- La sécurité d'approvisionnement électrique est, au jour d'aujourd'hui, moins vulnérable aux menaces (liées aux TIC, notamment) touchant la production d'électricité injectée dans les sous-stations que celles touchant à l'exploitation des réseaux de distribution et de transport.
- Le risque induit par des erreurs de manipulation, volontaires ou non, commises par des collaborateurs sur les systèmes critiques est significatif et augmente continuellement du fait du processus de centralisation des centres de conduite.
- La vulnérabilité globale de l'approvisionnement électrique en lien avec les TIC va continuer de croître.

En étroite collaboration avec les exploitants des infrastructures critiques, l'Office fédéral de la protection de la population (OFPP) a rédigé un «guide PIC», qui fournit à ces derniers une marche à suivre pour une protection appropriée de leurs infrastructures critiques.

Pour récapituler, et à l'exception des installations nucléaires, qui sont déjà soumises à des exigences régulatoires considérables de l'Inspection fédérale de la sécurité nucléaire (IFSN), il n'existe à l'heure actuelle que très peu de dispositions (légalement) contraignantes relatives à la sécurité physique des infrastructures électriques critiques.

La nouvelle Loi sur l'approvisionnement du pays, entrée en vigueur le 1er juin 2017, confère à l'Office fédéral pour l'approvisionnement économique du pays (OFAE) la compétence pour la mise en œuvre, à titre subsidiaire, des mesures préventives visant à garantir l'approvisionnement en énergie.

Cette lacune de dispositions en matière de sécurité physique devrait être comblée par la présente norme minimale – qui constitue une mesure préventive au sens de la Loi fédérale sur l'approvisionnement économique du pays – et qui suit les recommandations contenues dans le guide PIC de l'OFPP.

Le présent document a été élaboré dans le cadre d'un groupe de travail de l'AES. Le but de ce groupe a été de créer un document contraignant visant à définir pour la branche électrique suisse une norme minimale concrète basée sur l'évaluation des risques pour les sous-stations de niveaux de réseau 1 et inférieurs utilisées en commun et acceptée par le propriétaire du réseau de transport, ainsi que par les propriétaires de réseaux de distribution ou de centrales concernés.

À cette fin, il convient de définir des mesures de protection physique contre les accès non autorisés, les détériorations intentionnelles et la dégradation des systèmes pouvant toucher l'approvisionnement électrique. Les mesures proposées dans ce document concernent les installations du niveau de réseau 1, ainsi que celles de niveaux inférieurs, pour autant que ces dernières ne soient pas structurellement séparées du niveau de réseau 1 ou ne puissent être exploitées indépendamment de celui-ci.

La méthodologie du présent document peut également être utilisée pour les sous-stations des niveaux de réseau inférieurs au niveau de réseau 1.

1. Délimitation

(1) En raison de l'absence quasi totale de principes juridiques relatifs aux mesures de sécurité physique, la présente recommandation de la branche suit une approche fondée sur le risque se rapportant au guide PCI de l'OFPP. Elle vise à traiter les principaux risques en matière de sécurité physique. L'objectif du présent document consiste à mettre à la disposition des responsables de la sécurité au sein des entreprises d'approvisionnement en énergie (EAE) une méthodologie et des instructions pour pouvoir évaluer les risques pesant sur la sécurité de leurs sous-stations, et ce, en tenant compte, notamment, des configurations particulières des interfaces entre réseau de transport et réseau de distribution. Parallèlement, des mesures de sécurité ad hoc, répondant aux risques principaux de façon appropriée, sont élaborées. Afin de faciliter ce processus, le document fournit une vue d'ensemble des possibilités actuelles de mise en œuvre, prenant en compte l'importance des infrastructures à protéger. Ces recommandations permettent de définir des mesures pour une protection physique dite «de base» et de présenter des exemples pour des mesures de protection physique étendue.

(2) Cette approche contribue grandement à l'amélioration de la résilience et, partant, de la sécurité d'approvisionnement.

(3) Les recommandations du présent document sont étroitement liées à la recommandation de la branche AES «Protection de base pour les technologies opérationnelles (OT) des infrastructures critiques d'approvisionnement en électricité». Les deux recommandations de la branche doivent se renforcer mutuellement et se compléter lorsque cela est possible.

(4) Les normes existantes (ISO, NERC et autres) ont été prises en compte pour l'élaboration de cette recommandation de la branche. Certains des concepts ou recommandations y figurant, par exemple la question de la définition d'une partie critique d'installation, ont été repris pour l'élaboration de la présente norme.

1.1 Délimitation du contenu

(1) La sécurité électrique et opérationnelle des moyens d'exploitation du réseau et les questions relatives aux mesures de protection des personnes et de sécurité au travail (visés par les dispositions de l'Ordonnance sur les installations électriques à courant fort, de la SUVA, de la LAA, etc.) ne relèvent pas de la présente recommandation de la branche.

(2) Le document s'applique aux sous-stations de niveaux de réseau 1 et inférieurs (en cas d'utilisation commune des sous-stations avec le niveau de réseau 1). Toutefois, la méthodologie se prête également à des niveaux de réseau inférieurs.

(3) La prise en charge des coûts ne fait pas l'objet du présent document. À ce sujet, il convient de se référer aux bases légales et régulatoires existantes.

(4) Les risques naturels, météorologiques (séismes, inondations, glissements de terrain, etc.) ou liés aux animaux ne sont pas traités dans ce document. Ces sujets sont à traiter lors de la phase d'autorisation de construire, en fonction des particularités locales et suivant les dispositions légales.

1.2 Bases légales existantes et contexte national

1.2.1 Lien avec le contexte national

(1) Le 27 juin 2012, le Conseil fédéral a adopté la stratégie nationale pour la protection des infrastructures critiques (PIC) et a chargé l'Office fédéral de la protection de la population de coordonner sa mise en œuvre. Au total, la stratégie nationale PIC englobe 15 mesures visant l'amélioration de la capacité de résistance (résilience) des infrastructures critiques suisses face aux défaillances et aux perturbations. Parmi les plus importantes de ces mesures figurent notamment la réalisation d'un inventaire des infrastructures critiques et l'élaboration de plans d'intervention, destinés à la protection de la population et à l'armée, qui interviennent en soutien aux exploitations de ces objets critiques en cas de catastrophes ou dans les situations d'urgence. Cette stratégie a été remplacée par la stratégie nationale PIC 2018-2022 sur décision du Conseil fédéral du 8 décembre 2017. Le guide PIC de l'OFPP et la stratégie nationale PIC peuvent être téléchargés sur la page principale de l'OFPP (www.babs.admin.ch).

(2) Le renforcement de la résilience des infrastructures critiques constitue une autre priorité à part entière. À cette fin, le Conseil fédéral a chargé les instances compétentes (autorités compétentes, exploitants des infrastructures critiques, etc.) d'examiner les risques existants et, en cas de besoin, de prendre des mesures de renforcement de la résilience de ces infrastructures critiques. Il s'agit de la mesure M15 de la stratégie nationale PIC. L'OFPP a rédigé un guide décrivant la méthodologie et les éléments à prendre en considération. Ce guide a été élaboré dans le cadre du groupe de travail PIC, au sein duquel étaient représentés les offices fédéraux concernés de tous les départements, ainsi que les cantons. Il a en outre fait l'objet d'une consultation professionnelle auprès des associations, des exploitants et des conférences cantonales. Dans le cadre d'un projet pilote, le guide a été mis en œuvre par le gestionnaire de réseau de transport, Swissgrid. Cette mise en application a été réalisée en collaboration avec les autorités concernées, parmi lesquelles l'OFEN, ElCom et l'OFAE. Le guide PIC s'appuie également sur les travaux de définition et de mise en œuvre des stratégies nationales de protection des infrastructures critiques et de protection de la Suisse contre les cyberrisques.

(3) Le rapport final sur le projet pilote de guide Swissgrid se limite au réseau de transport au titre de l'Ordonnance sur l'approvisionnement en électricité (OApEl). Exemples de risques à l'appui, il aborde les procédures et les normes de sécurité qui en résultent. Ce document a pour objectif d'indiquer aux entreprises des approches de sécurisation adéquates, fondées sur les risques et adaptées à leurs différentes situations.

1.2.2 État des lieux des dispositions légales existantes

(1) Conformément à la Loi sur l'approvisionnement en électricité (LApEl), les exploitants sont tenus de garantir un «réseau sûr, performant et efficace».[2] Ni la LApEl ni l'OApEl ne précisent toutefois le niveau de sécurité à atteindre. En outre, si l'Office fédéral de l'énergie (OFEN) peut, d'après l'OApEl, «fixer des exigences techniques et administratives minimales concernant un réseau sûr, performant et efficace», il n'existe pour l'heure aucune disposition relative à la protection intégrale du réseau.

(2) L'Inspection fédérale des installations à courant fort (ESTI) a quant à elle défini différentes réglementations techniques et opérationnelles. L'Ordonnance sur les installations électriques à courant fort

[2] Art. 8 LApEl

(Ordonnance sur le courant fort 734.2) contient également certains principes relatifs à la sécurité, tels que la définition d'une hauteur de clôture minimale.

1.2.2.1 Bases générales

- Stratégie nationale de protection des infrastructures critiques (PIC), y compris plan de mise en œuvre
- Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), y compris plan de mise en œuvre

1.2.2.2 Bases juridiques spécifiques pertinentes

- Loi fédérale sur l'approvisionnement économique du pays (LAP)
- Loi fédérale sur la protection de la population et sur la protection civile (LPPCi)
- Loi sur l'énergie (LEne)
- Ordonnance sur l'énergie (OEne)
- Loi sur l'approvisionnement en électricité (LApEl)
- Ordonnance sur l'approvisionnement en électricité (OApEl)

1.2.2.3 Travaux préliminaires pertinents des autorités

- **Office fédéral pour l'approvisionnement économique du pays (OFAE)**
  - Analyse des risques TIC dans le secteur électrique (contrôle-commande, transmission des données et communication vocale), Berne, 2011
  - Analyse des risques et des vulnérabilités du sous-secteur lié à l'approvisionnement électrique
- **Département fédéral de la défense, de la protection de la population et des sports (DDPS)**
  - Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)
- **Office fédéral de la protection de la population (OFPP)**
  - Travaux d'inventaire PIC, Berne, 2014
  - Guide PIC, Berne, 2014
  - Rapport sur la gestion des risques «Catastrophes et situations d'urgence en Suisse», Berne, 2013

1.2.2.4 Travaux préliminaires pertinents de la branche / des associations de branche

- **Association des entreprises électriques suisses (AES)**
  - Recommandation de la branche pour le marché suisse de l'électricité «ICT Continuity», Aarau, décembre 2011
- **North American Electric Reliability Corporation (NERC)**
  - NERC CIP – Critical Infrastructure Protection, 2006 ff
- **Bundesamt für Sicherheit in der Informationstechnik (BSI, Allemagne)**
  - IT-Grundschutz-Kataloge, 2016
- **Société nationale du réseau de transport / VSE**
  - Procédure en cas de défaillance de la charge et/ou de la production supérieure à 400 MW, Frick, janvier 2013
  - Accord de branche marché électrique suisse, Transmission Code 2013

2. Méthodologie

2.1 Approche méthodologique

(1) L'approche choisie s'appuie sur les principes définis dans le guide PIC de l'Office fédéral de la protection de la population (OFPP). Ce guide se fonde quant à lui sur les concepts et normes établis en matière de gestion des risques, de la continuité et des crises (p. ex. ISO 31000, ISO 22301, BS 25999, ISO 27001). Le processus d'amélioration continue pour la protection des infrastructures critiques représentée dans le guide a été adaptée au cas des sous-stations.

(2) Un critère d'analyse à considérer (celle de la criticité) a été ajouté.

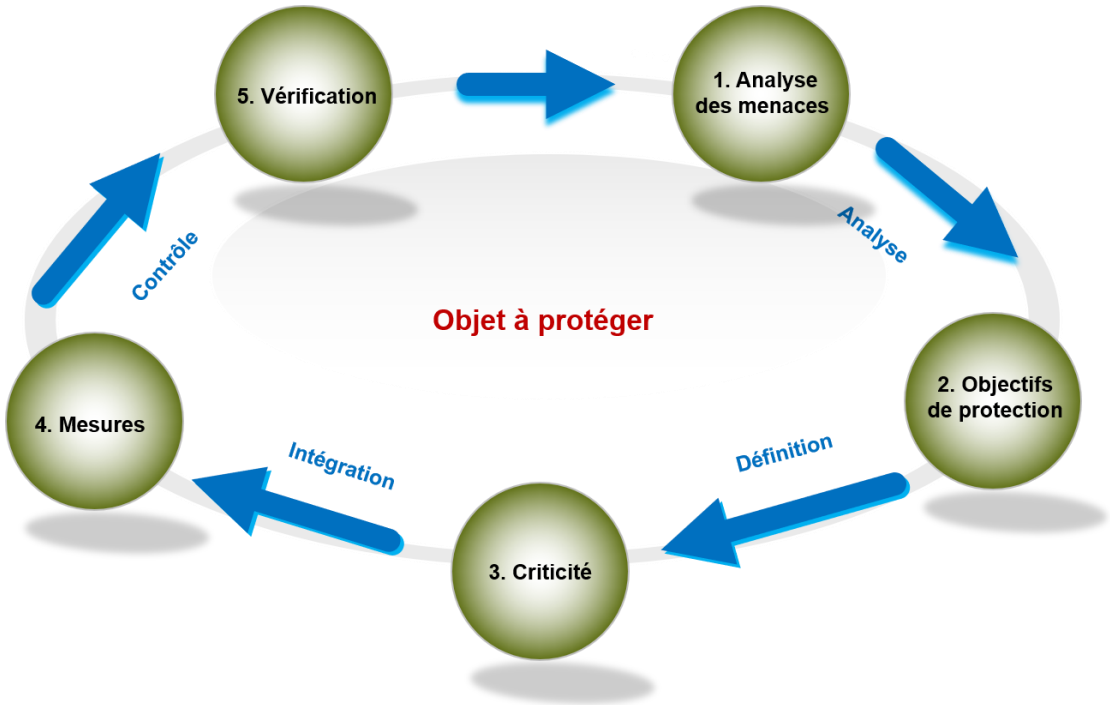


Figure 1 Processus d'amélioration continue

2.2 Étape 1: Analyse de la menace

(1) L'analyse des menaces vise à établir une liste priorisée des fonctionnalités, des processus et des infrastructures critiques, en vue de définir les objectifs de protection. Pour ce faire, il convient d'identifier les processus et les infrastructures critiques d'une sous-station, puis de réaliser une analyse des menaces pouvant les impacter.

(2) Afin de pouvoir identifier les processus et les infrastructures critiques indispensables à la fonctionnalité de la sous-station, il convient de disposer de bonnes connaissances sur la criticité ainsi que la fonctionnalité de ladite sous-station.

(3) Dans un deuxième temps, il s'agit de déterminer les éléments critiques dont le dérangement ou la défaillance sont susceptibles de mener à une perturbation ou, dans le pire des cas, à une mise hors tension complète de la sous-station.

(4) Il convient alors de définir les menaces significatives susceptibles d'entraîner de tels dérangements ou défaillances de ces éléments critiques. Une menace est considérée comme «significative» lorsqu'elle est susceptible de nuire de façon très importante à la fonctionnalité de l'élément critique.

(5) L'étape suivante consiste à définir différents scénarios décrivant le déroulement potentiel des événements pour chaque menace. Chaque menace peut se voir associer plusieurs de ces scénarios (examen de la menace).

(6) Il s'agit ensuite de déterminer et d'évaluer les risques que présente chaque scénario identifié. Une représentation graphique sous la forme d'une matrice des risques contenant la probabilité d'occurrence et l'ampleur des dommages potentiels résultant de l'événement est recommandée (cf. document de l'AES «Protection de base pour les technologies opérationnelles (OT) dans l'approvisionnement en électricité»).

(7) Une quantification des risques (probabilité d'occurrence x ampleur des dommages) permet ensuite d'identifier, d'évaluer et de chiffrer la valeur monétaire des risques relatifs aux menaces concernées (examen des risques).

2.2.1 Examen des menaces

(1) L'absence de prescriptions légales ne permet pas de définir directement une protection de base exhaustive dans le domaine de la sécurité physique, raison pour laquelle le présent document s'appuie globalement sur des approches des bonnes pratiques reconnues.

(2) Afin de mettre en place des mesures de protection appropriées, il est indispensable de se pencher préalablement sur le niveau de la menace.

(3) L'OFPP décrit ainsi, par exemple, comme événement de référence un «attentat conventionnel», par opposition aux attentats de type A, B et C (OFPP, Analyse nationale des dangers – Dossier sur les dangers «Attentat de type conventionnel», 30 juin 2015).

(4) En tant qu'actions délibérées menées contre la sécurité physique, les attentats conventionnels peuvent prendre différentes formes et relever de différentes catégories de menaces.

(5) En partant d'une pyramide des menaces proposée par l'Office fédéral de la sécurité des technologies de l'information (Allemagne), une pyramide similaire a été imaginée pour les menaces physiques (figure 2). Les étages de la pyramide représentent les différentes catégories d'attaquants, classés selon leur niveau de professionnalisme croissant. Au sommet de la pyramide se trouve ainsi l'acte étatique (guerre).

(6) Un risque apparaît pour l'objet à protéger lorsque des menaces identifiées rencontrent un point faible (faille de sécurité), Cette faille peut être comblée par des mesures de protection, ou l'entreprise peut au contraire accepter le risque encouru (propension au risque, cf. 2.2.2.2).

(7) Les menaces émanent de divers acteurs disposant de différents niveaux de connaissances, de formation, de support logistique, de ressources et de motivation.

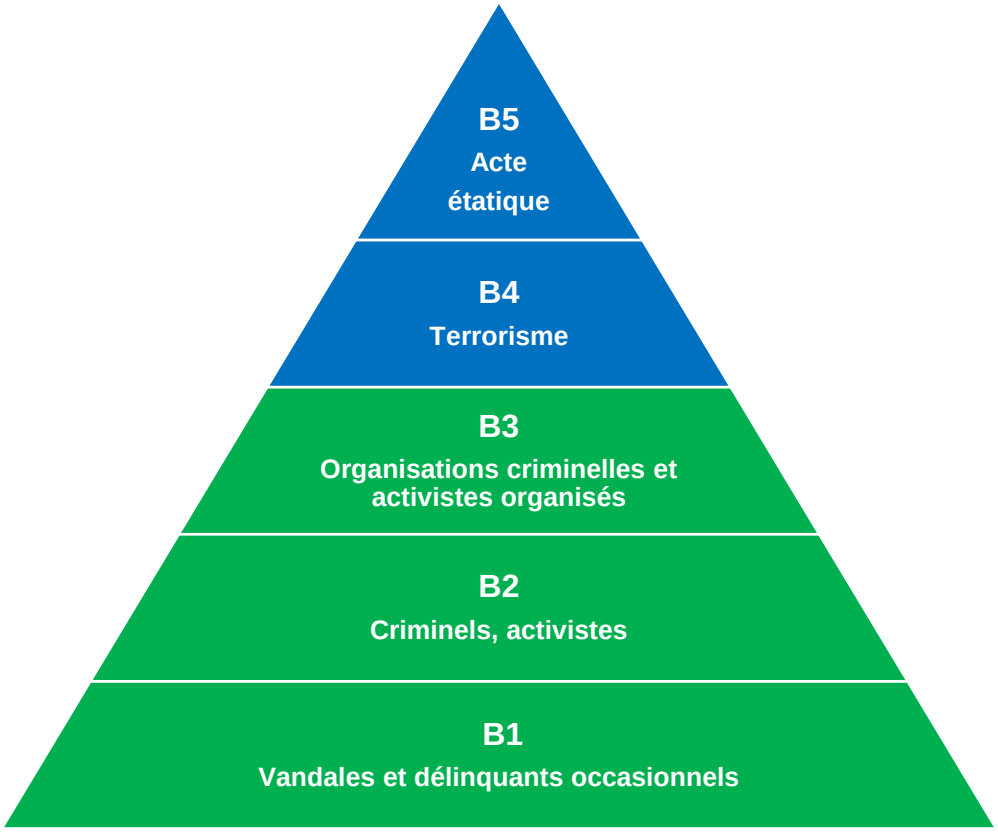


Figure 2 Pyramide des menaces

Niveau de menace		Description	Dommages
B1	Vandales et délinquants occasionnels	Auteurs d'attaques ne possédant pas de connaissances très approfondies. Ils profitent d'une occasion favorable et commettent de petits délits (vandalisme) ou des vols, sans mise en œuvre de techniques sophistiquées ou recours à d'importantes ressources.	Faibles
B2	Criminels, activistes	Personnes cherchant de façon délibérée à exploiter des points faibles pour commettre des délits (vol) ou à mettre leurs connaissances au service d'objectifs politiques ou idéologiques (activisme).	Moyens
B3	Organisations criminelles et activistes organisés	Criminels élaborant des modèles économiques ciblés dans le but de commettre des délits (vol de cuivre) ou de bloquer des installations en recourant à des attaques physiques. Ils sont généralement bien organisés et disposent des ressources nécessaires et de soutien logistique.	Élevés
B4	Terrorisme	Attaques physiques extrêmes perpétrés avec une grande violence dans le but de détruire ou de mettre hors service des infrastructures: enlèvements, attaques d'installations critiques avec des armes à feu.	Très élevés
B5	Acte étatique	Actes de guerre provenant d'États étrangers: tirs de missile et d'artillerie, p. ex.	Très élevés

Tableau 1 Niveaux de menace

(8) Il est impossible pour une entreprise de se prémunir contre tous les acteurs et donc de réduire activement tous les risques. Certains risques résiduels subsistent et doivent être identifiés, acceptés ou redirigés par l'entreprise.

(9) La mise en œuvre des mesures de protection dépend du niveau de la menace. Plus la catégorie est élevée, plus elle nécessite de ressources (financières, savoir-faire) afin de contrer les attaques ou de maîtriser leurs conséquences.

(10) Les menaces de niveau B4 et B5, entrant dans le champ du terrorisme et de l'acte de guerre, ne peuvent pas être gérées par une entreprise seule, mais relèvent des compétences de l'État et ne sauraient être gérées sans son soutien (intervention de l'armée, p. ex.).

(11) Cela signifie que des failles de sécurité subsistent inévitablement, malgré tous les efforts qu'une entreprise peut déployer.

(12) Il est du ressort des responsables de chaque entreprise d'accepter ces failles de sécurité ou de prendre des mesures visant à les combler, quand bien même la compétence et la responsabilité de l'État seraient en jeu.

2.2.2 Examen des risques

(1) En cas d'apparition d'une menace identifiée sans qu'aient été définies des mesures de protection suffisantes, l'objet à protéger encourt un risque.

(2) Comme alternative, il est possible de combler la faille de sécurité (mise en œuvre de mesures de protection) ou d'accepter le risque (résiduel).

(3) Comme mentionné ci-dessus, il est impossible de réduire tous les risques, si bien qu'un risque résiduel persistera toujours. Il est du ressort de l'entreprise concernée de procéder à l'examen de ces risques.

(4) Il convient ainsi de procéder à une analyse des risques, en s'appuyant sur les menaces définies à la section 3.2.2.

(5) À cette fin et pour chaque événement, la probabilité d'occurrence et l'étendue des dommages potentiels sont à évaluer.

(6) L'accent est mis sur l'estimation des dommages pour la population et l'économie suisses qui résulteraient de perturbations dans le réseau de transport, en l'occurrence dans les sous-stations des niveaux de réseau 1 et inférieurs (pour autant qu'elles soient utilisées en commun avec le niveau de réseau 1).

(7) Les risques sont à représenter au moyen d'une matrice de risque. Un exemple est présenté ci-après. Il existe actuellement différentes approches quant aux dimensions de la matrice. Idéalement, cette dernière aura une dimension correspondant aux standards utilisés au sein de chaque entreprise.

(8) Exemple d'une matrice de risque possible «Sécurité physique des sous-stations» (niveau de réseau 1 et inférieurs) avec des valeurs fournies à titre informatif uniquement:

Seuil de risque critique menacé: définir des mesures d'atténuation et les mettre en œuvre selon les ressources disponibles

Seuil de risque critique franchi: mesures d'atténuation à mettre en place

Catégorisation qualitative	Fréquence annuelle	Catégorie de fréquence	Catégorie de risque				
Très probable	> 10	5					
Probable	1 – 10	4					
Possible	0,1 – 1	3					
Envisageable	0,01 – 0,1	2					
Improbable	< 0,01	1					

Catégorie d'ampleur des dommages potentiels	A	B	C	D	E
NR1: Préjudices financiers en MCHF	< 0,1	0,1 – 1,0	1 – 10	10 – 100	> 100
NR2-NR3: Préjudices financiers en MCHF	< 0,01	0,01 – 0,1	0,1 – 1,0	1 – 10	> 10
Ampleur des dommages potentiels	négligeable	modérée	substantielle	importante	catastrophique

Tableau 2 Exemple de matrice de risque

(9) Explications générales

La matrice de risque est à compléter de façon indépendante par chaque entreprise, avant d'être consolidée entre les partenaires (en cas d'utilisation commune des sous-stations). Les différents risques, et plus particulièrement l'ampleur des dommages potentiels en résultant, peuvent varier en fonction du niveau de réseau et, par exemple, de la taille de la zone de desserte de l'entreprise. La matrice de risque représentée ci-dessus se réfère au niveau de réseau 1. Il est évidemment possible de rajouter, en sus de l'aspect financier, d'autres axes pour quantifier l'ampleur des dommage potentiels, tels que les dommages corporels, la sécurité d'approvisionnement ou le préjudice à la réputation, et de les intégrer à l'examen des risques. Cette décision est à la discrétion de l'exploitant. Les menaces et leur répartition dans les catégories de risques doivent être régulièrement examinées et faire l'objet d'un accord avec les partenaires (en cas d'utilisation commune des sous-stations).

2.2.2.1 Évaluation et quantification des risques

(1) Le guide PIC de l'OFPP propose de considérer le rapport coût-bénéfices des mesures de protection à mettre en place (coûts marginaux). Il convient ainsi de fixer une valeur monétaire aux risques et de comparer celle-ci avec le coût des mesures à mettre en œuvre. La multiplication de la probabilité d'occurrence (plausibilité) par la valeur monétaire du dommage potentiel permet de calculer la valeur du risque (en CHF / an).

(2) L'art. 15 LApEl prévoit que les dépenses effectuées pour assurer la sécurité du réseau peuvent être comptabilisées comme des coûts de réseau imputables. Le niveau de sécurité attendu pour l'exploitation du réseau n'est cependant pas précisé.

(3) Au cours de cette étape, la question se pose également de déterminer s'il convient de réduire la probabilité d'occurrence d'un risque, l'ampleur des dommages potentiels qu'il génère, ou les deux. Il convient en outre de décider si d'éventuelles exigences externes, ainsi que des obligations régulatoires ou légales doivent entrer en jeu.

2.2.2.2 Gestion des risques

(1) Il s'agit de l'étape préparatoire à la définition ultérieure des mesures de protection à prendre. Elle a pour objectif une représentation exacte de la propension de l'entreprise à prendre des risques.

(2) Il s'agit ici d'appréhender des questions fondamentales, telles que la légalité des mesures possibles et l'importance de l'entreprise en tant qu'infrastructure critique à l'échelle nationale. Il est ainsi tout à fait possible que des mesures ne paraissant pas économiquement justifiables en tant que telles puissent être mises en œuvre si elles répondent à la volonté de protéger des infrastructures critiques.

(3) Plusieurs possibilités peuvent être déployées pour réduire un risque:
- Définition de mesures visant la réduction de la probabilité d'occurrence d'un risque
- Définition de mesures visant la réduction de l'ampleur des dommages potentiels résultant du risque
- Transfert d'un risque (solution d'assurance)

(4) Il est également possible d'accepter le risque (par exemple si une entreprise juge la probabilité d'occurrence d'un risque comme étant minime).

(5) Il se peut ainsi que certains risques soient identifiés, que l'entreprise concernée en prenne note et qu'elle les accepte, ce pour différentes raisons. Les considérations économiques peuvent prévaloir, aussi bien que la question de la responsabilité (pyramide des menaces).

(6) La propension au risque représente l'ampleur des risques que l'entreprise est prête à courir et à accepter sans chercher à les supprimer ou à les réduire.

(7) En sus des objectifs relatifs à la protection, d'autres objectifs (par exemple les objectifs commerciaux) sont pris en compte par l'entreprise pour déterminer sa propension au risque. Il convient cependant de les prendre en compte de façon appropriée.

(8) Le processus global de gestion des risques doit être supervisé continuellement et à intervalles réguliers.

2.3 Étape 2: Définition des objectifs de protection

(1) La définition des objectifs de protection (c'est-à-dire le niveau de protection à atteindre face aux différents scénarios d'attaques et aux groupes d'attaquants) détermine le niveau que doivent atteindre les diverses mesures de protection. Cela permet de distinguer les risques acceptables des risques inacceptables.

(2) La disponibilité des infrastructures critiques représente un indicateur important pour la formulation des objectifs de protection. Le choix des objectifs doit s'orienter vers une durée d'indisponibilité minimale des éléments critiques.

2.4 Étape 3: Criticité des installations

(1) Comme mentionné à l'étape 1, l'importance d'une sous-station ou des parties critiques de ses installations par rapport au système global considéré joue un rôle décisif. À cet égard, une analyse de la criticité (approche globale) doit précéder l'élaboration de mesures locales (approche spécifique).

(2) Dans cette perspective, le concept de criticité se rapporte à l'importance de la sous-station par rapport au réseau dans sa globalité et par rapport à son rôle en lien avec la sécurité d'approvisionnement (cf. section 3.4).

2.5 Étape 4: Mesures: protection de base et protection étendue

(1) Lors de l'élaboration du concept de protection, il convient d'évaluer l'impact de différentes mesures (systèmes électroniques d'accès, renforcement des bâtiments, etc.) pouvant être prises afin de réduire les risques potentiels, et ce dans le but de respecter les objectifs de protection définis. De manière générale, il faut prendre des mesures qui correspondent à l'état actuel de la technique, qui servent à satisfaire aux objectifs de protection et qui soient optimisés économiquement.

(2) Les mesures de protection relatives aux sous-stations peuvent être réparties en fonction de la situation initiale, du type de menace, du risque ou de l'objectif de protection, selon les trois catégories suivantes:

2.5.1 Protection de base

(1) La protection de base résulte des différentes exigences contenues dans les lois, les ordonnances (p. ex. l'Ordonnance sur le courant fort), les normes (contraignantes comme facultatives) et les bonnes pratiques («best practices»). Les mesures constituant la protection de base s'appuient sur ces exigences et découlent de normes établies ou de bonnes pratiques universellement reconnues. Les risques ne sont pas considérés dans la détermination et la définition des mesures faisant partie de la protection de base.

(2) Les bonnes pratiques ont une grande importance: elles reposent sur des procédés éprouvés et montrent comment d'autres sociétés abordent le problème. Les lois contraignantes doivent être systématiquement intégrées aux mesures faisant partie de la protection de base. L'ensemble des recommandations relatives à la protection de base doit en principe être appliqué à toutes les sous-stations.

2.5.2 Protection étendue (moyenne et haute protection)

(1) Parallèlement à la protection de base, qui définit le niveau minimum nécessaire, la propension au risque détermine le niveau de protection considéré comme raisonnable par les responsables des différentes entreprises. Ainsi, l'importance d'une sous-station pour le système dans sa globalité est examinée au moyen d'une analyse de la criticité. Si la sous-station joue un rôle particulier (par exemple en raison de son importance pour l'ensemble du réseau) et doit ainsi être plus particulièrement protégée; il est recommandé de la faire bénéficier d'une protection «moyenne» ou «haute».

(2) Les mesures peuvent en principe être divisées en deux catégories:
- les mesures préventives, destinées à réduire la probabilité d'occurrence d'un risque ou l'ampleur des dommages subis. On y intègre les mesures curatives, telles que les mesures et les processus préparatoires visant à assurer la continuité des opérations.
- les mesures préparatoires, destinées à limiter la durée d'indisponibilité d'une installation critique ou à contribuer à la gestion de l'événement.

(3) Il convient de veiller, dans la mesure du possible, à ne pas négliger les mesures ayant pour but de diminuer l'ampleur des dommages au seul bénéfice des mesures réduisant la probabilité d'occurrence d'un risque. À cette fin, il convient de prendre en compte le fait que la réduction de l'ampleur des dommages ne peut généralement être obtenue que par la suppression ou la réduction du danger potentiel ou par un blindage (passif) et p. ex. un stockage suffisant de matériel de remplacement.

(4) En règle générale, il convient de prendre des mesures qui soient économiquement justifiables, à la pointe de la technique et qui contribuent à la réalisation des objectifs de protection.

(5) Les mesures doivent être intégrées suite à une analyse coûts-bénéfices fondée sur le risque, comparant les investissements qui seraient nécessaires à la mise en œuvre de mesures et les coûts directs et indirects qu'entraînerait une détérioration des infrastructures critiques.

(6) Dans ce contexte se pose également la question du risque résiduel acceptable, qui repose d'une part sur une acceptation consciente et d'autre part sur une mauvaise évaluation ou identification des risques.

(7) Dans le cadre de la protection des infrastructures critiques, une analyse coûts-bénéfices fondée sur le risque doit remplir les critères suivants:
- La mise en œuvre des mesures doit notamment contribuer à la réalisation de l'objectif de protection préalablement défini.
- Les mesures, nouvelles ou résultant d'adaptations, doivent réduire les risques pour l'infrastructure critique ou la durée d'indisponibilité.
- Les coûts des mesures ne doivent pas être excessifs.

(8) Cette analyse coûts-bénéfices garantit que les mesures les plus efficientes (réalisation des objectifs) soient retenues.

2.6 Étape 5: Vérification

(1) Afin de vérifier la qualité de mise en œuvre et l'efficacité des mesures adoptées par rapport à la protection de base et à la propension au risque définir, et afin de pouvoir corriger les écarts constatés, ces mesures font l'objet d'une surveillance constante. Le concept de protection choisi fait lui aussi l'objet d'un contrôle quant à son efficacité et son efficience.

(2) Des vérifications supplémentaires sont nécessaires aux échéances suivantes:
- suite à la mise en œuvre des mesures,
- suite à un événement ayant mené à une crise,
- suite à un agrandissement ou à une transformation de l'infrastructure critique,
- suite à une évolution de la situation en matière de danger.

(3) Ces vérifications doivent être planifiées et les résultats obtenus documentés (voir également section 3.6.

3. Application: élaboration de mesures pour la protection des sous-stations

3.1 Application de la démarche pour une sous-station

(1) La démarche proposée repose sur la méthodologie présentée à la section 1, qui repose elle-même sur la procédure décrite dans le guide PIC. Elle peut être représentées, pour les sous-stations, par le schéma ci-dessous:

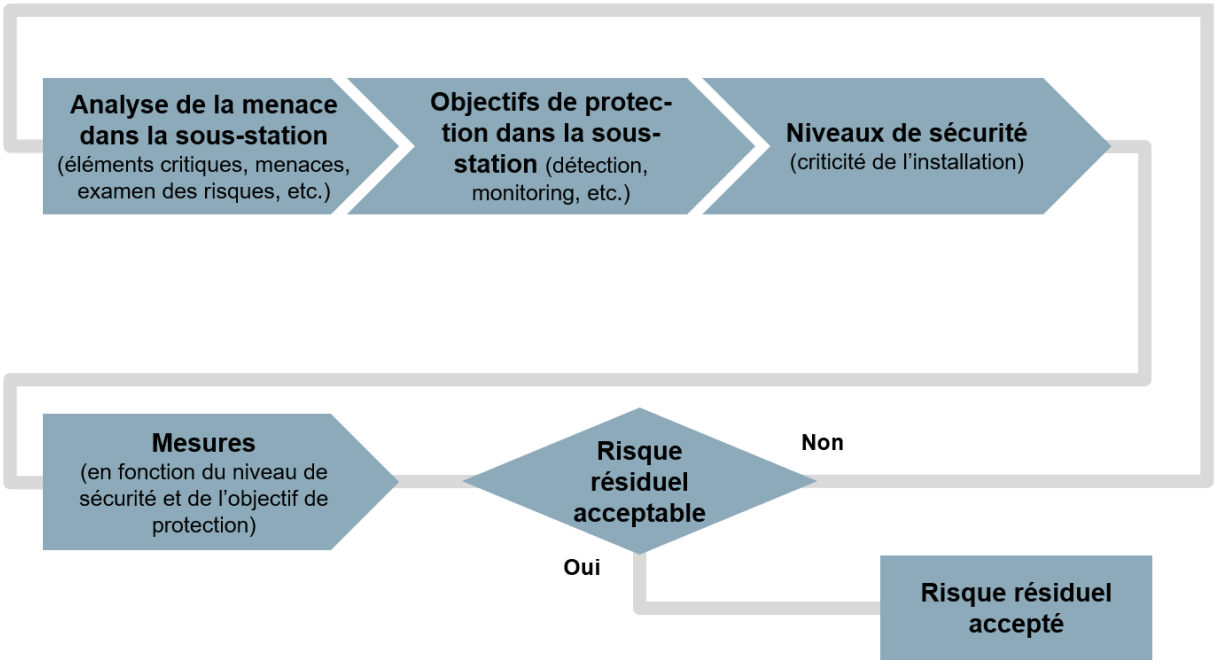


Figure 3 Processus pour la définition des mesures de protection appropriées

3.2 Étape 1: Analyse de la menace

3.2.1 Identification des éléments critiques d'une sous-station

(1) Afin de déterminer les dangers significatifs, il convient de définir préalablement les éléments critiques de la sous-station.

(2) Dans ce contexte, les éléments critiques se définissent comme suit:
- Éléments d'installation pouvant, en cas de défaillance, entraîner une perturbation significative de la sécurité d'approvisionnement conduisant à des préjudices notables pour la population ou l'économie.
- Éléments d'installation dont le remplacement est complexe ou très long à exécuter et qui présentent donc un risque pour la sécurité d'approvisionnement.

Liste des éléments critiques d'une sous-station

Éléments de haute criticité	Éléments de criticité moyenne	Éléments non critiques
Transformateurs très haute tension*	Jeux de barres	Bâtiments de bureaux et de service
Armoires de commande des disjoncteurs	Isolateurs	Routes et voies d'accès
SCADA local (SCADA poste)	Disjoncteurs	Stocks de matériel commun
Dispositifs de mesure, armoires de couplage	Introductions des câbles	Parkings
Dispositifs de protection	Parafoudres	Stocks de matériel de valeur
Armoires du réseau de communication (WAN)	Transformateurs de mesure	Zones d'atelier
Introductions des câbles du réseau de communication (WAN)	Sectionneurs	
Services internes		

Tableau 3 Liste des éléments critiques d'une sous-station

* y compris certains transformateurs spécifiques d'autres niveaux de réseau

(3) La criticité des éléments doit être examinée dans le cadre de l'élaboration du catalogue de mesures de protection. La plus grande attention est donnée à la protection des éléments de haute criticité.

3.2.2 Dangers et risques significatifs

(1) Il convient ensuite de procéder à la définition des dangers significatifs et des menaces y relatives, en s'appuyant sur la pyramide des menaces représentée à la section 2.2.1.

(2) Les dangers considérés comme significatifs sont ceux résultant des scénarios pouvant conduire à une perturbation ou à une défaillance des éléments critiques d'une sous-station.

(3) Il convient d'examiner les menaces physiques potentielles suivantes:

(4) Menaces contre les infrastructures:
- Intrusion, accès non autorisé
- Attaques physiques destructrices par des individus ou des groupes
- Perturbation des systèmes de communication et de l'infrastructure de communication
- Attaque par véhicule ou impact accidentel
- Vol d'informations confidentielles, de biens appartenant à l'entreprise et de ressources matérielles (p. ex. éléments d'installation, métaux, équipement)
- Techniques électroniques de perturbation ou d'écoute criminelles
- Vandalisme
- Attaques de drones sur les infrastructures critiques
- Incendie volontaire d'une infrastructure critique (p. ex. transformateur)

(5) Menaces contre les personnes:
- Ingénierie sociale criminelle
- Embauche de personnel sans contrôle de sécurité préalable
- Attaque physique ou psychologique contre le personnel
- Enlèvement

(6) Les dangers potentiels sont ensuite regroupés par thématiques et des scénarios spécifiques décrivant le déroulement possible des événements sont définis.

(7) Six scénarios principaux (cf. tableaux ci-après) sont ainsi élaborés. Lors de la définition et de la description des scénarios, l'accent est mis sur les événements susceptibles de conduire à une sévère détérioration de la qualité de l'approvisionnement en électricité. Les événements n'entraînant pas de telles conséquences ne sont pas considérés.

(8) Les différents risques identifiés et leurs conséquences potentielles sont à considérer conjointement pour chaque scénario:

1. Attaque physique visant l'affaiblissement et la destruction de l'infrastructure			
Menace	**Niveau de menace**	**Description**	**Risque**
Attaque physique non préparée	B1	Attaque non planifiée ou non professionnelle contre une sous-station ou l'une de ses parties, caractérisée par un faible niveau de criminalité. Les auteurs peuvent recourir à des outils couramment utilisés dans le cadre de cambriolages.	Détériorations modérées d'éléments de l'installation, portes enfoncées et fenêtres brisées, clôtures découpées. Aucune perturbation du réseau à escompter.
Attaque physique préparée	B2	Attaque organisée et planifiée contre une sous-station ou l'une de ses parties, caractérisée par un niveau de criminalité moyen ou élevé. Les auteurs ont recours à des outils, des procédures et des connaissances de spécialistes.	Détériorations ciblées d'éléments de haute criticité, ayant pour conséquence une détérioration très probable de la sécurité d'approvisionnement.
Accident ou attaque avec véhicule	B1, B2	Détérioration de biens par un accident de la route ou par une attaque organisée et planifiée. Les auteurs peuvent utiliser des voitures ou des poids-lourds.	Dommages de nature accidentelle, qui peuvent cependant avoir d'importantes conséquences. Risque d'écoulement de carburant et donc d'incendie et de dégâts environnementaux. Détérioration de la sécurité d'approvisionnement en cas de défaillance de parties critiques d'installation.
Accident ou attaque avec des armes à feu	B2, B3, B4, B5	Détérioration de biens ou de personnes par un accident, par une attaque non-organisée ou par une attaque organisée et planifiée, à l'aide d'armes.	Il faut s'attendre à une dégradation ciblée, due à des tirs, de parties d'installation potentiellement hautement critiques. L'utilisation d'armes de type fusil d'assaut et de catégories supérieures entraîne des dommages considérables. Danger élevé de défaillance de parties d'installations ou de la sous-station.
Attaque par impulsion électromagnétique	B4, B5	Détérioration de biens par l'utilisation de générateurs d'impulsion électromagnétique.	Une attaque ciblée effectuée à l'aide de générateurs d'impulsion électromagnétique endommage le système électronique de la sous-station, ce qui entraîne la défaillance de la technique secondaire et de l'infrastructure de communication. La conduite de la sous-station est rendue difficile. Risque élevé d'arrêt de l'exploitation.
Attaque avec drone	B2, B3, B4, B5	Exploration ou endommagement de biens par l'utilisation de drones ou d'autres engins volants.	Dans des cas extrêmes, l'utilisation d'un drone (largage d'explosifs) peut entraîner des dégâts considérables pour les parties critiques d'installation, qui peuvent conduire à une défaillance de la sous-station.

2. Vol de biens ou d'informations importants pour le fonctionnement de la sous-station			
Menace	**Niveau de menace**	**Description**	**Risque**
Vol d'informations importantes pour le fonctionnement	B1 à B5	Vol d'informations importantes pour le fonctionnement de la sous-station, sous forme physique ou numérique	Le transfert non consenti ou criminel d'informations peut permettre à d'éventuels assaillants de déceler des failles de sécurité générales ou de prendre connaissance de l'architecture de sécurité existante, information susceptible de permettre une attaque ciblée et efficace. Risque accru pour la sécurité d'approvisionnement.
Vol de biens matériels non importants pour le fonctionnement	B1, B2	Vol de biens matériels: mobilier, outils, matériel de bureau, pièces de rechange non stratégiques, matériaux de rénovation, etc.	Préjudice porté à l'entreprise via des pertes de biens. En règle générale, pas d'effet sur la sécurité d'approvisionnement.
Menace	**Niveau de menace**	**Description**	**Risque**
Vol de biens matériels importants pour le fonctionnement	B1, B2, B3	Vol de biens matériels: outils spécialisés, moyens d'exploitation d'installations en service, pièces de rechange stratégiques, éléments de mise à terre, etc.	Cet événement peut impacter l'exploitation des installations et aller jusqu'à la défaillance partielle de la sous-station.

3. Accès non autorisé			
Menace	**Niveau de menace**	**Description**	**Risque**
Accès non autorisé par effraction	B1 à B5	Un individu ou un groupe accède à la sous-station par des moyens tels que la coupure ou l'escalade des clôtures ou le bris de portes et fenêtres.	Détériorations modérées de parties d'installation, portes enfoncées et fenêtres brisées, clôtures découpées. Pas de perturbation du réseau à escompter. Risque de dommages corporels en raison de l'accès inapproprié à l'enceinte.
Accès non autorisé par infiltration	B1, B2	Un individu ou un groupe accède à la sous-station en se joignant à un groupe («back tailing») ou par d'autres procédés d'infiltration.	Détériorations modérées de parties d'installations dans le pire des cas. Pas de perturbation du réseau à escompter. Risque de dommages corporels en raison de l'accès inapproprié à l'enceinte.
Accès non autorisé via manipulation	B2, B3	Un individu ou un groupe accèdent à la sous-station via le vol de clefs ou la manipulation du système d'accès.	Détériorations modérées de parties d'installations dans le pire des cas. Pas de perturbation du réseau à escompter. Risque de dommages corporels en raison de l'accès inapproprié à l'enceinte.

4. Attaques venant de l'interne			
Menace	**Niveau de menace**	**Description**	**Risque**
Action planifiée de l'interne	B2, B3, B4	Un attaquant interne (personnel interne ou externe) recourt à un savoir-faire suffisant pour mener des attaques et des manipulations.	Dans le pire des cas, dégâts ciblés et mise hors service de parties critiques d'installations, ce qui peut entraîner une défaillance générale du système. Risque élevé pour la sécurité des installations.
Réactions émotionnelles négatives	B2	Un individu ou un groupe exerce une activité criminelle suite à une réaction émotionnelle.	Dans le pire des cas, blessure de personnes et/ou dégâts ciblés et mise hors service de parties critiques d'installations, ce qui peut entraîner une défaillance générale du système. Risque élevé pour la sécurité des personnes et des installations.

5. Menace physique et psychologique contre les personnes			
Menace	**Niveau de menace**	**Description**	**Risque**
Ingénierie sociale	B3, B4	Via p. ex. la collecte ou la recherche d'informations dans un but criminel sur les fonctions critiques et hautement critiques ou sur les applications et éléments d'installation critiques.	La collecte d'informations illégale et non consentie ainsi que leur transfert peuvent permettre de déceler des failles de sécurité ou de prendre connaissance de l'architecture de sécurité existante, informations susceptibles d'ouvrir la voie à une attaque ciblée et efficace. Risque accru pour la sécurité d'approvisionnement.
Attaque contre les personnes	B3, B4	Un individu ou un groupe menace de façon ciblée des personnes, en allant jusqu'à l'attaque physique ou psychologique, dans le but d'obtenir des informations ou un accès.	Dans le pire des cas, menace et blessure de personnes, suivies de dégâts ciblés et de mise hors service de parties critiques d'installations, ce qui peut entraîner une défaillance générale du système. Risque élevé pour la sécurité des personnes et des installations.
Enlèvement	B3, B4, B5	Un individu ou un groupe enlève des personnes pour les pousser à livrer des informations ou à commettre des actions ayant des effets négatifs sur la sécurité d'approvisionnement.	Dans le pire des cas, menace et blessure de personnes, suivies de dégâts ciblés et de mise hors service de parties critiques d'installations, ce qui peut entraîner une défaillance générale du système. Risque élevé pour la sécurité des personnes et des installations.

6. Vandalisme			
Menace	**Niveau de menace**	**Description**	**Risque**
Vandalisme dans et autour de la sous-station	B1, B2	Préjudice financier via dégradation et/ou détérioration de biens par des graffitis ou des dégâts physiques légers.	Implique généralement l'accès non autorisé au site, susceptible d'entraîner le risque de dommages corporels (actions inappropriées). Le vandalisme n'entraîne normalement pas de risque pour la sécurité d'approvisionnement.

3.3 Étape 2: Objectifs de protection

(1) Les objectifs de protection définissent l'étendue et, en partie, le niveau de protection à atteindre, en fonction de l'entreprise. Cette définition détermine également, dans une certaine mesure, la maturité d'une entreprise dans sa gestion des risques en lien avec les menaces physiques envers les installations critiques.

(2) Les trois principaux objectifs de protection pour la protection d'une sous-station sont présentés ci-après.

3.3.1 Objectif de protection 1: Connaître, nommer et surveiller les domaines critiques

(1) L'objectif est de connaître et de dénommer les éléments et domaines présentant une criticité pour le système dans son ensemble. Les différents événements doivent être évalués en fonction de leur criticité (fonctionnement du système général). Il s'agit à la fois de protéger ces éléments/domaines par des mesures appropriées et de les surveiller afin que les attaques, les intrusions, les activités suspectes et les ingérences puissent être détectées.

3.3.2 Objectif de protection 2: Protection et dissuasion/ralentissement des agresseurs

(1) L'objectif est de se protéger des attaques ou de les prévenir le plus en amont possible. La dissuasion des agresseurs potentiels constitue un autre aspect important, pouvant être réalisée via la visibilité des mesures prises (caméras de surveillance) et/ou par l'installation de panneaux de signalisation et d'avertissement.

(2) Les mesures de sécurité doivent ralentir suffisamment les actions des agresseurs pour qu'ils puissent être arrêtés par des forces d'intervention avant de s'introduire sur le site et d'avoir le temps de provoquer des dégâts importants, ou encore pour qu'une alarme sonore perturbe les agresseurs et les fasse fuir.

(3) Cet objectif de protection couvre également la résilience du fonctionnement/de la sous-station.

3.3.3 Objectif de protection 3:Détection et traçabilité des accès

(1) L'objectif est de détecter et de pouvoir tracer chaque accès à l'infrastructure critique (en l'occurrence, la sous-station et les autres parties critiques d'installation). Il faut également être en mesure de juger si un accès est autorisé ou non. La traçabilité des entrées doit faire l'objet d'un programme d'audit.

(2) En outre, les accès non autorisés doivent être transmis à une instance centralisée, via un système de sécurité approprié, afin de pouvoir prendre les mesures qui s'imposent au cas par cas.

(3) Parallèlement à ces objectifs de sécurité à proprement parler, trois autres objectifs opérationnels internes à l'entreprise sont à considérer:

3.3.3.1 Dispositions relatives aux situations exceptionnelles (chantiers, maintenance, etc.)

(1) En cas de situation exceptionnelle dans la sous-station ou dans la partie d'installation concernée, il est nécessaire de s'assurer que les adaptations nécessaires du système de sécurité soient planifiées, exécutées et que le personnel concerné soit formé. Ces adaptations ne doivent en aucun cas entraver la détection et la traçabilité des accès.

3.3.3.2 Processus de sécurité connus, testés et enseignés

(1) La mise en place et l'entretien d'un système de sécurité global sont des éléments clés. Il convient de le faire connaître au personnel concerné et de former ce dernier à toutes les procédures nécessaires. Il importe de veiller à ce que l'organisation de sécurité procède à cette formation conformément aux besoins et aux dispositions légales et remette les différents documents requis. Le fonctionnement et l'adéquation du système général de sécurité doivent faire l'objet d'une vérification dans le cadre d'une approche standardisée de type «Plan – Do – Check – Act».

(2) Les éventuelles modifications pour des situations et des menaces spécifiques doivent être effectuées, documentées et enseignées de façon appropriée.

(3) Étant entendu que le facteur humain joue un rôle capital, il convient de procéder régulièrement à des formations de sensibilisation sur le concept de sécurité existant. Il doit ainsi être donné priorité à l'instauration d'une culture de la sécurité. Dans le cadre d'un processus d'amélioration continu, il importe d'auditer régulièrement ces formations et leur succès. Les résultats d'audit doivent être consignés et constituent, avec les autres informations disponibles, la base pour les étapes ultérieures d'analyse.

3.3.3.3 Enregistrement des incidents et élaboration de mesures ad hoc

(1) L'enregistrement des incidents et les mesures en résultant doivent être intégrés au système de sécurité global. Une telle base de données (p. ex. une liste des événements et des mesures prises) constitue un prérequis à un examen continu de la situation, et s'intègre à une analyse permanente de la menace. Il convient de s'assurer que chaque indicent soit enregistré et analysé conformément aux critères définis au préalable. Les mesures en découlant doivent être mises en œuvre selon leur degré d'urgence (processus de gestion des risques).

(2) Les objectifs de protection doivent tenir compte de la situation de risque et de la criticité des installations à protéger. Tout comme les mesures, les objectifs de protection doivent faire l'objet d'une vérification et d'une actualisation régulières.

(3) La capacité de réaction de l'entreprise à la suite d'une alarme doit elle aussi être régulièrement contrôlée.

(4) Les objectifs de protection doivent également servir, dans une deuxième phase, à évaluer la contribution des mesures à la réalisation desdits objectifs.

3.4 Étape 3: Criticité des installations et niveaux de sécurité

(1) Il est logique qu'un concept de sécurité destiné aux installations et aux éléments critiques tienne également compte de la criticité des installations et parties d'installations à protéger par rapport à leur importance pour le système dans sa globalité.

(2) La même perspective vaut pour l'ensemble des sous-stations et d'installations de couplage à protéger.

(3) Au vu de la différence d'impact sur la sécurité d'approvisionnement et des stratégies internes aux différentes entreprises énergétiques, toutes les sous-stations ne présentent pas la même criticité en matière de mesures de protection physique. En d'autres termes, la prise en compte des effets sur le réseau des différentes sous-stations laisse apparaître différents besoins et niveaux de protection. Ainsi, la défaillance d'une sous-station à la criticité haute pourra menacer la stabilité de l'ensemble du réseau, tandis que la défaillance d'une sous-station non critique ne menacera pas la sécurité d'approvisionnement (globale).

(4) Les critères possibles pour une évaluation de la criticité sont énumérés ci-dessous:
- Importance de la sous-station pour la société nationale du réseau (nombre de niveaux de tension, nombre de lignes nationales et internationales, nombre de transformateurs et leur puissance, nombre de consommateurs, etc.)
- Importance de la sous-station pour le réseau de distribution (nombre de transformateurs concernant le réseau de distribution et leur puissance, nombre de consommateurs, etc.)
- Perspective d'une centrale électrique (nombre de générateurs, puissance, nombre de pompes, importance en termes d'aptitude au démarrage autonome, etc.)

(5) Le renforcement des mesures de sécurité pour les sous-stations des niveaux de réseau 1 et inférieurs (pour les sous-stations utilisées en commun avec le niveau de réseau 1) doit dépendre de leur importance (criticité). On distingue ainsi trois niveaux de sécurisation (protections haute, moyenne et normale). Les mesures de renforcement s'appuient sur la catégorisation des agresseurs tirée des scénarios de menace et sur les menaces et les risques qui en découlent (voir section «dangers significatifs»).

3.4.1 Niveau de sécurité «protection normale» (protection de base)

(1) La protection de base représente le cas de base pour toutes les sous-stations de niveaux 1 et inférieurs (pour les sous-stations utilisées en communs avec le niveau de réseau 1).

(2) Les effets d'une défaillance d'une sous-station comprise dans cette catégorie sur la disponibilité globale du réseau sont faibles. La sous-station ne doit donc être protégée que contre l'intrusion d'attaquants peu motivés, comme des vandales ou des voleurs occasionnels.

(3) Limitations: l'enceinte ne bénéficie pas dans son intégralité d'une surveillance électronique.

3.4.2 Niveau de sécurité «protection moyenne»

(1) Les effets d'une défaillance d'une sous-station comprise dans cette catégorie sur la disponibilité globale du réseau sont modérés. La sous-station doit donc être protégée contre l'intrusion d'attaquants à la motivation moyenne à haute, comme des cambrioleurs organisés (vol de cuivre, etc.).

(2) Mesures: le niveau de sécurisation dit «moyen» doit comprendre la surveillance de l'ensemble de l'enceinte et permettre l'observation de l'ensemble de la sous-station.

3.4.3 Niveau de sécurité «protection haute»

(1) Les effets d'une défaillance d'une sous-station comprise dans cette catégorie sur la disponibilité globale du réseau sont sévères à catastrophiques. La sous-station doit donc être protégée contre l'intrusion d'attaquants à la motivation haute à très haute, comme des criminels organisés ou des activistes.

(2) Mesures: en complément des mesures du niveau de sécurité de protection dit «moyen», la surveillance des espaces intérieurs sensibles et une double détection dans les zones extérieures sensibles sont assurés. Les espaces intérieurs sont répartis en différentes zones de sécurité. Les voies d'accès peuvent être surveillées.

(3) D'une manière générale, les installations doivent être conçues dans le but de présenter la plus grande résilience possible contre toute forme de menace. Il convient également de veiller à utiliser de façon appropriée certaines mesures opérationnelles, comme la réaction rapide suite à des alarmes.

3.5 Étape 4: Mesures

3.5.1 Zones de protection

(1) Les mesures de protection représentées ci-après s'appuient sur les principes énoncés à la section 3.4, relatifs à la criticité des sous-stations et des parties d'installation critiques.

(2) Différentes zones de protection sont à différencier au sein d'une sous-station. En prenant en considération les éventuelles mesures de protection, l'analyse des menaces potentielles et le déroulement théorique d'une attaque physique (venant de l'extérieur ou de l'intérieur), les zones de protection suivantes peuvent être logiquement distinguées:

- Périmètre
- Site
- Bâtiments
- Pièce avec éléments
- Transformateur

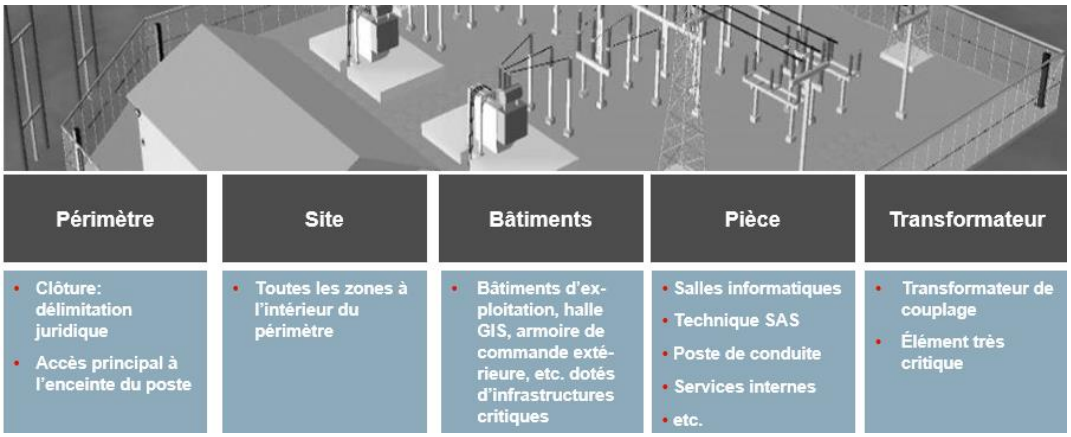


Figure 4 Schéma définissant les différentes zones de protection d'une sous-station

3.5.2 Mesures de protection par zone de protection

(1) Les différentes mesures de protection, déterminées par la criticité de l'installation, sont présentées suivant la zone et l'élément/la mesure de protection correspondant.

3.5.2.1 Clôture

(1) La clôture constitue la délimitation juridique du site et représente dans le même temps une protection physique contre les intrus et contre les dangers dans les installations. La construction d'une clôture permet également la démarcation vis-à-vis de tiers («safety»), cf. les dispositions légales existantes par l'Inspection fédérale des installations à courant fort (ESTI).

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Construction d'une clôture conformément à l'Ordonnance sur le courant fort (définition de la hauteur et du maillage)	2
Protection moyenne	La clôture définie légalement est complétée par une protection contre les tentatives d'escalade, qui peut être sécurisée par un fil de sécurité (fil de fer barbelé ou fil de fer NATO).	2
Protection haute	Les mesures de protection étendue décrites ci-dessus sont complétées par une protection sous-terraine empêchant les intrus de s'introduire dans l'enceinte en creusant sous la clôture. Des mesures supplémentaires peuvent encore renforcer la clôture (p. ex. le recours à des éléments de clôture renforcés, etc.).	2

Tableau 4 Mesure de protection: clôture

Exemples de mise en œuvre:

Clôture avec protection contre l'escalade

Clôture avec protection sous-terraine

Figure 5 Exemples de clôtures

3.5.2.2 Protection anti-collision

(1) Les parties d'installation et éléments critiques – transformateurs, alimentation, etc. – sont protégés contre les dégâts mécaniques. Afin de réduire l'énergie cinétique, des barrages et des rétrécissements peuvent être mis en place à des emplacements stratégiques. Ceux-ci peuvent se trouver en dehors du périmètre (de l'enceinte) et, ainsi, concerner des voies d'accès et des voies parallèles à la sous-station.

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Aucune mesure	
Protection moyenne	Examiner s'il faut prendre des mesures «douces» (glissières de sécurité, piquets, etc.)	2
Protection haute	Examiner s'il faut prendre des mesures «dures» (éléments en béton, bornes, etc.)	2

Tableau 5 Mesures de protection: protection anti-collision

Exemple de mise en œuvre:

Figure 6 Exemple d'éléments de protection en béton

3.5.2.3 Détection au niveau de la clôture

(1) Le périmètre extérieur (en règle générale, la clôture) est surveillé au moyen de mesures de détection appropriées. La mesure a pour objectif de détecter au plus tôt les intrusions et les attaques éventuelles. Le système de détection (clôture intelligente, caméra intelligente) perçoit les tentatives d'escalade, de découpe de la clôture ou d'intrusion sur le site par d'autres moyens. En règle générale, cette mesure doit être couplée à un centre de surveillance en aval capable de réagir en cas d'incident.

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Aucune mesure	
Protection moyenne	Détection de périmètre: surveillance intelligente de la clôture ou du mur au moyen de capteurs ou d'un système de caméras	1, 2, 3
Protection haute	En complément de la détection de périmètre, qui, selon sa conception, peut ne détecter que la survenance d'un incident, recours à des systèmes d'image permettant d'identifier visuellement la raison du déclenchement de l'alarme et, en cas de besoin, de suivre les possibles intrus sur l'image	1, 2, 3

Tableau 6 Mesures de protection: détection au niveau de la clôture

Exemples de mise en œuvre:

Analyse vidéo de la clôture

Système de détection sur la clôture

Figure 7 Exemples de systèmes de détection intelligents au niveau de la clôture

3.5.2.4 Accès principal au site

(1) Une attention particulière est à accorder à l'accès principal au site, afin de le protéger contre les accès non autorisés. L'accès principal peut être celui d'un bâtiment et ne doit pas nécessairement faire partie du périmètre de la sous-station (clôture). Une sécurisation spécifique de l'accès principal devrait permettre dans le même temps de réduire le nombre de points d'accès au site. Dans l'idéal, il ne subsiste ainsi qu'un seul point d'accès au terrain, sécurisé et supervisé. L'accès au site joue un rôle déterminant dans l'architecture de sécurité globale. La traçabilité des entrées dans la sous-station est impérative.

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Le recours à un système électronique de fermeture permet de verrouiller les accès et de les surveiller.	1, 2, 3
Protection moyenne	L'utilisation d'un système électronique centralisé de fermeture modifiable à distance rend également possible l'accès, ce qui permet d'empêcher ou d'autoriser à distance les accès. Cela nécessite toutefois l'existence d'un poste administratif central, à même de gérer et de contrôler les droits. Cette approche a par ailleurs une influence positive sur la sécurité des personnes.	1, 2, 3
Protection haute	Le système électronique centralisé de fermeture modifiable à distance est complété par des caméras surveillant l'accès principal.	1, 2, 3

Tableau 7 Mesures de protection pour l'accès principal au site

Exemples de mise en œuvre:

Figure 8 Exemples de systèmes d'accès

3.5.2.5 Surveillance du site

(1) Grâce aux mesures de surveillance du site, les accès non autorisés font l'objet d'une surveillance technique et d'un suivi, ce qui offre également une protection supplémentaire en matière de sécurité au travail. En outre, des systèmes d'éclairage sont utilisés pour améliorer la visibilité.

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Aucune mesure de surveillance du site	
Protection moyenne	Installation d'éclairages supplémentaires à des emplacements stratégiques et vidéosurveillance des secteurs critiques du site uniquement	1, 2, 3
Protection haute	La protection étendue est complétée par une vidéosurveillance systématique du site. Les systèmes d'éclairage s'allument de manière aléatoire.	1, 2, 3

Tableau 8 Mesures de protection: surveillance du site

Exemples de mise en œuvre:

Figure 9 Exemples de caméras de surveillance

3.5.2.6 Enveloppe du bâtiment

(1) L'enveloppe du bâtiment est renforcée à un niveau défini au moyen de matériaux appropriés, entravant ainsi les tentatives d'intrusion par l'enveloppe du bâtiment. Le niveau de renforcement est fonction de l'importance de la sous-station pour le réseau dans sa globalité et de la situation topographique de celle-ci. Les accès au bâtiment ne sont pas pris en compte dans ces considérations.

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Aucune mesure	
Protection moyenne	Renforcement de l'enveloppe du bâtiment conformément aux normes actuelles (classes de résistance) en fonction de la criticité de la sous-station.	2
Protection haute	La sécurité du bâtiment est complétée par l'ajout d'un système de surveillance antieffraction.	1, 2, 3

Tableau 9 Mesures de protection pour l'enveloppe du bâtiment

Exemples de mise en œuvre:

Barreaux

Système d'alarme antieffraction

Détecteur d'effraction

Figure 10 Exemples de mesures de renforcement du bâtiment

3.5.2.7 Accès au bâtiment

(1) Outre l'enveloppe, les accès au bâtiment sont également sécurisés. Ces mesures de protection visent essentiellement l'accès principal du bâtiment. Idéalement, le nombre d'accès au bâtiment doit être limité au minimum nécessaire à l'activité. Il est à relever que les fenêtres font partie de l'enveloppe du bâtiment. Les mesures concernant les fenêtres sont relativement faciles à réaliser (barreaux, alarme contact, etc.). Si le bâtiment n'est pas entouré d'une clôture et qu'il est accessible directement depuis l'extérieur du périmètre du site, les règles relatives aux accès au site s'appliquent.

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Fermeture mécanique	2
Protection moyenne	Système de fermeture électronique, accès traçables et pouvant être bloqués	1, 2, 3
Protection haute	Système de fermeture électronique centralisé modifiable à distance avec vidéosurveillance	1, 2, 3

Tableau 10 Mesures de protection des accès au bâtiment

(2) Se référer à la section «Accès principal au site» pour des exemples.

3.5.2.8 Surveillance des salles

(1) La surveillance des salles alerte un poste central en cas d'accès non autorisé. L'alerte est alors transmise aux personnes concernées pour traitement, conformément au processus d'alarme en vigueur. L'accès à des personnes autorisées peut être permis par un code, par des clefs ou par une demande au poste central. Les salles hébergeant des installations critiques sont, dans l'idéal, équipées de caméras (traçabilité de l'alarme).

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Aucune mesure	
Protection moyenne	Système d'alarme antieffraction (surveillance des accès et des pièces au moyen de capteurs, p. ex.)	1, 2, 3
Protection haute	Vidéosurveillance	1, 2, 3

Tableau 11 Mesures de protection: surveillance des salles

(2) Se référer aux figures 9 et 10 pour des exemples de systèmes de vidéosurveillance et d'alarme antieffraction.

3.5.2.9 Accès aux salles

(1) Protection de tous les accès à une salle. La protection concerne l'accès principal et, lorsque cela est possible, les autres portes desservant la pièce. Il convient de définir de préférence un accès principal et protégé, les autres accès étant verrouillés.

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Aucune mesure	
Protection moyenne	Fermeture mécanique	2
Protection haute	Système de fermeture électronique, accès traçables et pouvant être bloqués	1, 2, 3

Tableau 12 Mesures de protection pour les accès aux salles

Exemples de mise en œuvre:

Figure 11 Exemples de système de fermeture des salles

3.5.2.10 Élément

(1) Protection d'un rack ou d'une armoire contenant des éléments critiques. En plus des mesures de protection techniques recommandées, il est préconisé d'opter pour une construction massive pour le rack/l'armoire (revêtement en acier massif, pas de vissage visible, etc.).

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Aucune mesure	
Protection moyenne	Système d'alarme antieffraction (surveillance des entrées au moyen de capteurs, p. ex.)	1, 2, 3
Protection haute	Surveillance supplémentaire par caméra	1, 2, 3

Tableau 13 Mesures de protection d'un élément

(2) Se référer aux figures 9 et 10 pour des exemples de systèmes de vidéosurveillance et d'alarme antieffraction.

3.5.2.11 Accès à un élément

(1) L'accès à un élément critique dépend du système de fermeture du rack ou de l'armoire contenant ce dernier. Un élément dont l'accès n'est pas autorisé doit être équipé d'une fermeture adaptée.

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Aucune mesure	
Protection moyenne	Fermeture mécanique	2
Protection haute	Système de fermeture électronique, accès traçables et pouvant être bloqués	1, 2, 3

Tableau 14 Mesures de protection pour l'accès à un élément

(2) Exemples de systèmes de fermeture: mécaniques et mécatroniques, système de fermeture en ligne (figure 11).

3.5.2.12 Protection des transformateurs

(1) Les transformateurs font partie des éléments les plus critiques d'une sous-station. La protection balistique (objets à haute énergie cinétique) représente un défi majeur. En fonction des exigences opérationnelles, les transformateurs peuvent bénéficier d'une protection balistique. Une telle protection est toutefois très coûteuse et il convient de l'examiner au cas par cas dans le cadre de la définition des objectifs de protection.

(2) Dans le cas où une entreprise prend la décision de protéger ses transformateurs contre les effets cinétiques, elle pourrait mettre en œuvre ces mesures selon les catégories suivantes.

Catégorie de protection	Description de la mesure de protection	Objectifs de protection
Protection normale	Aucune mesure	
Protection moyenne	Installation de cloisons autour du transformateur (béton, pierre ou acier)	1, 2
Protection haute	Installation de cloisons, y compris fermeture du «toit»	1, 2

Tableau 15 Mesures de protection des transformateurs

(3) Exemples: gabions, éléments en béton ou variante à treillis/maillage.

3.5.3 Notes explicatives sur les mesures de protection

(1) Si, en raison de son emplacement ou de sa construction (p. ex. poste de couplage souterrain isolé au gaz), une sous-station ne dispose pas d'une clôture, les mesures de la catégorie «Accès principal au site» sont à appliquer à la catégorie «accès au bâtiment».

(2) Selon la typologie et la construction de la sous-station, une combinaison de différentes mesures peut également être mise en place.

3.6 Étape 5: Vérification (cycle d'actualisation et audit)

(1) Une fois planifiées, élaborées et mises en œuvre, les mesures de protection font partie de l'activité normale de la sous-station. Les conditions-cadres (p. ex. l'importance de la sous-station pour la stabilité du réseau dans sa globalité), ainsi que la situation des menaces, p. ex. dans le secteur européen de l'énergie, étant susceptibles d'évoluer, il apparaît nécessaire de procéder à une vérification régulière des mesures adoptées.

(2) Une vérification régulière de la conception globale d'une sous-station en tenant compte des mesures de sécurité technique mises en place (cf. section 3.5.2) est pertinente. Les cycles de vérification s'appuient sur les durées de «demi-vies» des mesures techniques de protection prises.

(3) Il convient également de procéder à une vérification en cas de rénovation ou de remplacement de la sous-station.

3.7 Investissements

(1) Une analyse coûts-bénéfices peut être réalisée pour chacune des mesures de protection ou des combinaisons de mesures potentielles.

(2) Cependant, l'effet d'atténuation des différentes mesures étant insuffisant en cas d'application dans une seule et unique sous-station, on renoncera probablement à y recourir dans ce cas de figure.

3.8 Sensibilisation et mesures opérationnelles

(1) Les solutions techniques ne suffisent pas à elles seules à atteindre les objectifs de sécurité visés. Elles doivent être complétées par des mesures opérationnelles et organisationnelles claires et contraignantes.

3.8.1 Sensibilisation des collaborateurs

(1) Les collaborateurs, les sous-traitants et les exploitants des sous-stations doivent être formés aux risques de sécurité. Outre les mesures de sécurité techniques, il convient d'aborder les principes opérationnels, telles que le sujet de la sécurité dans une sous-station. Des règles de sécurité propres à l'entreprise doivent être définies à cette fin. Une attention particulière sera prêtée à la sensibilisation aux cyberattaques et aux mesures de sécurité physique.

(2) Des formations et des évaluations des connaissances et de la sensibilité ayant trait à la sécurité doivent avoir lieu à intervalles réguliers.

(3) Le développement de la sensibilité des collaborateurs est au cœur de toutes ces mesures, dans le but d'élaborer et d'ancrer une véritable culture de la sécurité.

3.8.2 Définition et suivi des autorisations d'accès

(1) De la même façon qu'on attribue des droits d'administrateurs dans le domaine de la cybersécurité, il convient de réguler l'accès aux parties critiques d'installation et d'attribuer les autorisations y relatives. Ces autorisations peuvent être conditionnées à différents éléments, par exemple:

- Être au bénéfice de compétences suffisantes
- Vérifier l'absence de risques, p. ex. par des contrôles de sécurité relatifs aux personnes

(2) Le contrôle de la sécurité relatif aux personnes joue un rôle particulièrement important dans les installations critiques des niveaux de réseau 1 et 3. La Confédération tient elle aussi compte de cet élément: l'adoption de la Stratégie énergétique 2050 fournit le cadre juridique nécessaire pour que les agences fédérales puissent exiger un tel suivi.

3.8.3 Visites sur site

(1) L'état d'implémentation des mesures est contrôlé lors de visites sur site, au moyen de check-lists. Il en va de même pour le respect des procédures de sécurité.

(2) Ces contrôles constituent l'essentiel du processus d'amélioration continue.

3.8.4 Réaction aux incidents touchant à la sécurité

(1) Des mesures de protection appropriées ne permettent pas d'écarter totalement les attaques et les incidents touchant à la sécurité. Il importe donc d'élaborer et de tester des plans d'urgence en cas d'attaque réussie ou d'autres incidents touchant à la sécurité. Selon le niveau de criticité de la sous-station, ces plans n'ont ni la même étendue ni la même portée.

(2) Les mesures suivantes en font partie:
- Définition de plans d'urgence et de plans de remise en exploitation (base de connaissances, «lessons learned» et lignes de communication) par le biais d'une procédure standardisée. Ces plans sont connus et répétés. Ils sont disponibles sur site et dans un lieu indiqué.
- Un test des plans d'urgence et de remise en exploitation a lieu une fois par an. Il peut s'agir de véritables tests ou d'une simple revue des plans et des principes existants.

3.9 Mesures de protection physique relatives à la cybersécurité

(1) Les mesures de protection physique ne visent pas seulement à protéger les composants primaires d'une sous-station mais contribuent également à la protection des cybercomposants critiques.

(2) Seule une approche intégrale de la sécurité permet de planifier et de mettre en œuvre des concepts de protection efficaces et efficients.

(3) Dans les sous-stations, la protection des composants TIC par des mesures physiques joue un rôle particulièrement important (voir le document AES «Protection de base pour les technologies opérationnelles OT dans les sous-stations»). Elle a notamment pour effet de:
- bloquer l'accès physique à des lieux critiques pour la sécurité à des personnes non autorisées;
- empêcher toute modification, manipulation, vol ou autre soustraction ou destruction physique des systèmes, des infrastructures, des interfaces de communication, du personnel ou des sites physiques existants;
- éviter l'observation non autorisée d'informations sensibles via l'observation visuelle, la prise de notes, les photographies ou tout autre moyen;
- empêcher la mise en place non autorisée de nouveaux systèmes, d'infrastructures, d'interfaces de communication ou d'autres matériels;
- exclure toute introduction illicite d'appareils développés intentionnellement dans le but de réaliser des manipulations matérielles, des écoutes ou d'autres activités nuisibles par le biais de dispositifs de stockage USB, de points d'accès sans fil, du Bluetooth ou d'autres technologies mobiles.

(4) La sécurité physique du centre de conduite ou de la salle de contrôle réduit l'impact de nombreuses menaces. Les centres de conduite et les salles de contrôle possèdent habituellement des environnements informatiques spécifiques permettant l'accès continu et en permanence au contrôle-commande des installations; la rapidité de réaction et la surveillance en continu des installations jouent ici un rôle de premier plan. Ces environnements contiennent souvent les serveurs eux-mêmes ainsi que d'autres nœuds informatiques et systèmes de contrôle-commande critiques. L'accès à de telles parties critiques d'installations doit être régi par des mesures physiques appropriées permettant un monitoring et une identification sans équivoque. Dans de nombreux cas, il est nécessaire de prévoir un centre de conduite de secours situé dans un autre site afin de pouvoir garantir le contrôle des installations dans le cas où le centre de conduite principal deviendrait inutilisable.

(5) Afin de pouvoir prendre les mesures de protection appropriées des systèmes informatiques critiques, il importe de mener une analyse préalable des composants informatiques critiques et des scénarios de menace possibles (Document AES «Protection de base pour les technologies opérationnelles (OT) dans les sous-stations»). Les connaissances résultant d'une telle analyse sont nécessaires pour la mise en place d'une protection efficace.

(6) Lors de l'élaboration et de la mise en œuvre de mesures de protection physique, il convient de garder à l'esprit que les systèmes de sécurité informatiques (caméras IP, p. ex.) représentent des cibles supplémentaires, qui doivent être couvertes par des mesures de cyberprotection appropriées.

(7) Le document AES «Protection de base pour les technologies opérationnelles (OT) dans l'approvisionnement en électricité» contient les informations nécessaires sur cette thématique.

4. Abréviations

ElCom	Commission fédérale de l'électricité
ICT (anglais)	Technologies de l'information et de la communication (TIC)
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFEN	Office fédéral de l'énergie
OFPP	Office fédéral de la protection de la population
PIC	Protection des infrastructures critiques
SCADA	Système de contrôle et d'acquisition de données (Supervisory Control and Data Acquisition)
TIC (français)	Technologies de l'information et de la communication (ICT)