Norme minimale pour la sécurité des technologies de l'information et de la communication (TIC) dans le domaine de l'élimination des déchets

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie,
de la formation et de la recherche DEFR
Office fédéral pour l'approvisionnement économique du pays OFAE

VBSA
ASED
ASIR

Avant-propos

Chères lectrices, chers lecteurs,

En travaillant dans la gestion des déchets, nous évoluons dans un secteur d'importance systémique : une panne de nos installations, à commencer par les usines de valorisation thermique des déchets (UVTD), affecterait sensiblement la société. Les *cyber*attaques constituent le premier facteur de risque. Ces derniers temps, des entreprises, des autorités et des organismes proches de l'État, dont des UVTD, ont été à plusieurs reprises victimes de *cyber*attaques ciblées, exécutées par des professionnels de haut vol. Or ces attaques ne provoquent pas seulement le blocage ou la suppression de données ; elles peuvent aussi entraîner le sabotage, la manipulation ou la destruction d'éléments d'installations physiques comme les postes de pesage ou les turbines. L'objectif des *cyber*criminels est généralement d'extorquer de l'argent.

Une UVTD a de nombreux points sensibles qui peuvent présenter des failles face aux *cyber*attaques, tels le dispositif de pesage, le grappin, le système de commande, les turbines ou encore les capteurs mesurant les émissions, sans compter les accès à distance dont bénéficient les prestataires des différents services de maintenance. Le point le plus délicat reste cependant le facteur humain et le manque de rigueur dans l'utilisation des technologies de l'information et de la communication (TIC). Afin de garantir une protection durable de l'information, la direction de l'entreprise doit s'engager et montrer l'exemple en la matière, et les collaborateurs doivent être impliqués dans la démarche et correctement formés.

Où en sommes-nous aujourd'hui dans notre branche ? La sécurité de l'information est traitée de manière très variable selon les installations. Alors que certaines UVTD y ont dédié un poste ad hoc, d'autres négligent quelque peu la thématique. La présente norme entend professionnaliser et harmoniser la résilience vis-à-vis des attaques informatiques. Il s'agit d'un guide rédigé par des professionnels pour des professionnels, qui cible des mesures de protection concrètes et directement applicables, afin de ne pas finir dans les tiroirs d'un préposé à la sécurité. En mettant en œuvre ce guide, vous vous conformez aux prescriptions formulées par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) dans sa norme minimale pour améliorer la résilience informatique (norme minimale pour les TIC) et apportez une contribution importante à la *cyber*résilience de votre entreprise.

L'Association suisse des exploitants d'installations de traitement des déchets (ASED) soutient les démarches visant à améliorer la sécurité de l'information dans le secteur de la gestion des déchets. Elle recommande à l'ensemble de ses membres de mettre en œuvre cette norme, propose des plateformes dédiées à l'échange d'informations et s'engage en faveur d'une communication transparente des incidents.

En réussissant à nous prémunir contre les *cyber*attaques, nous économiserons de l'argent, ménagerons nos nerfs et garantirons le bon déroulement des processus de valorisation des déchets : nous en sommes redevables aussi bien à la société qu'à l'environnement.

Robin Quartier
Ariane Stäubli
Secrétariat de l'ASED

Sommaire

1 Résumé

La présente norme, qui s'adresse aux entreprises d'importance systémique actives dans l'élimination des déchets, formule des recommandations sur la manière de réduire les *cyber*risques à un niveau acceptable, moyennant des dispositions anticipatives et économiquement pertinentes Une stratégie de sécurité informatique efficace assure la protection des équipements et services qui sont indispensables à l'exécution des processus opérationnels critiques. Outre des mesures techniques, elle englobe les procédures ad hoc, la formation et l'information des collaborateurs ainsi que la gouvernance. Augmenter la résilience informatique apporte par ailleurs des avantages économiques.

La mise en œuvre de la norme minimale revêt une haute importance, et ce pour les raisons principales exposées ci-dessous.

I. Les risques d'attaques tendent à augmenter, parce que la cybercriminalité est une activité très lucrative, et les entreprises industrielles sont elles aussi visées par des activités de sabotage.

II. À mesure que la transition numérique progresse, la nécessité de pouvoir échanger des données au sein de l'entreprise de manière entièrement informatisée se fait de plus en plus sentir, comme dans le cas de la lecture et de l'interprétation des données saisies par les capteurs utilisés dans le processus d'épuration des fumées. Il en va de même pour les échanges de données interentreprises, requis par exemple pour l'exécution de services de maintenance à distance sur certaines parties de l'installation.

III. Plus la dépendance à l'égard des processus TIC augmente, plus la vulnérabilité est grande. Dans les entreprises industrielles comme les UVTD, on fait la distinction entre les systèmes IT (technologies de l'information) et les systèmes OT (technologies opérationnelles). Alors que les systèmes IT recouvrent le traitement électronique des données, notamment dans le cadre des processus administratifs, les systèmes OT englobent l'infrastructure matérielle et logicielle nécessaire à la surveillance et/ou au pilotage directs des installations et processus industriels. Les systèmes OT qui permettent par exemple d'actionner les turbines sont eux aussi exposés au risque d'être manipulés ou mis hors service. Il est donc crucial d'implémenter et d'appliquer dès aujourd'hui des plans durables et résilients pour assurer la sécurité des infrastructures OT.

IV. Les infrastructures critiques (PIC) sont interdépendantes (gestion des déchets hospitaliers, protection de l'environnement, p. ex.).

Il ne faut pas oublier que le renforcement de la sécurité informatique dans le cadre de la mise en œuvre d'une *cyber*stratégie exige non seulement de nouveaux procédures et systèmes de sécurité, mais aussi des ressources en personnels supplémentaires. Même le système de sécurité le plus performant ne sert à rien si personne n'est là pour réagir aux alertes, en déterminer les causes et les traiter.

Dans des installations industrielles critiques pour la sécurité de l'approvisionnement comme les UVTD, il est particulièrement important que les objectifs de protection suivants soient garantis en tout temps :

- la disponibilité, à savoir la fiabilité des services informatiques ;
- la confidentialité, à savoir la protection contre les accès non autorisés ;
- l'intégrité, à savoir la protection contre l'effacement ou la falsification de l'information électronique.

Alors que, s'agissant de l'informatique, la confidentialité, l'intégrité et la disponibilité des informations sont d'importance égale, la disponibilité est l'objectif de protection prioritaire pour la technologie opérationnelle (cf. figure ci-dessous).

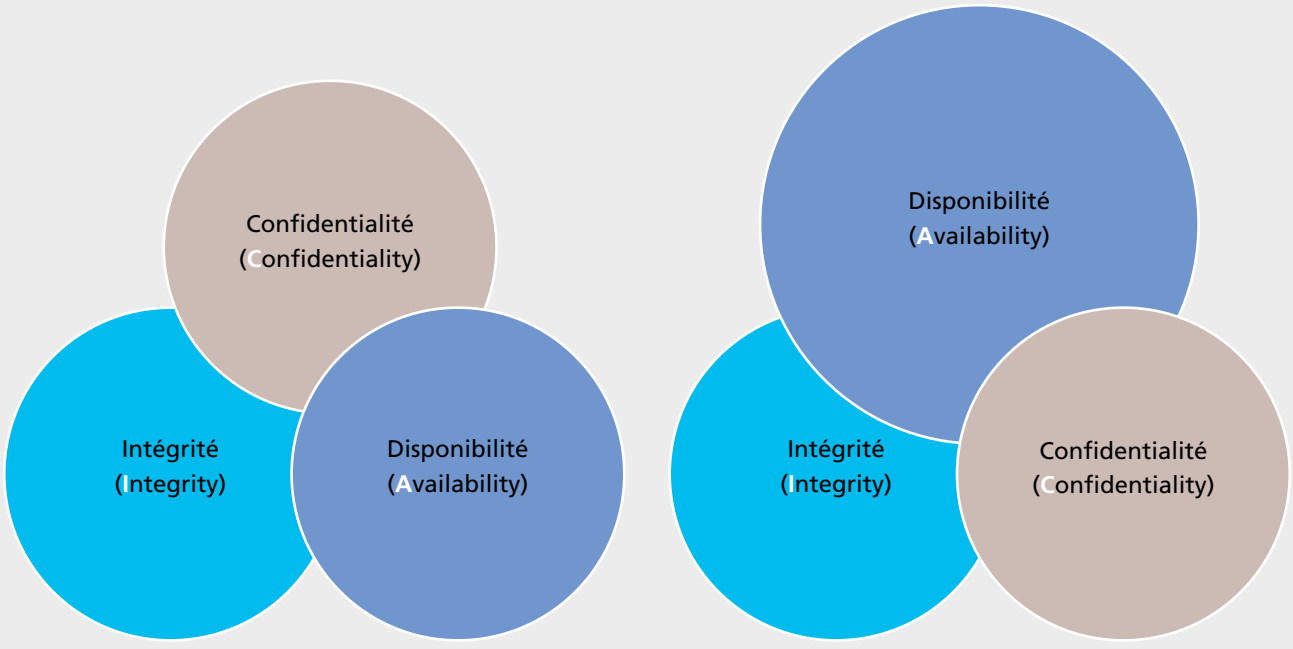
La section suivante illustre l'imbrication toujours plus étroite entre les systèmes IT et les systèmes OT. La convergence entre l'IT et l'OT permet notamment d'assurer un contrôle intégral de l'exploitation indépendamment du lieu et d'analyser facilement des données issues de systèmes complexes. En situation de panne ou d'urgence, les fournisseurs, les cadres et les collaborateurs ont ainsi accès aux données en temps réel de leurs systèmes et installations, ce qui leur permet de trouver plus rapidement de meilleures solutions aux problèmes.

Mettre en œuvre et intégrer une *cyber*stratégie conforme à la norme minimale pour améliorer la résilience informatique apporte les avantages suivants :

- moins de cloisonnement entre les systèmes IT et OT, exploitation des synergies ;
- moins de coûts de développement, d'exploitation et d'assistance et moins de pannes, grâce à la maintenance préventive ;
- plus grand respect des prescriptions légales, l'implémentation d'une *cyber*stratégie permettant d'accroître la transparence et d'améliorer la gestion et le contrôle des systèmes IT et OT ;
- meilleures automatisation et visibilité des OT décentralisées (cf. prestataires), grâce à la possibilité de transmettre et d'analyser les données de maintenance en temps réel ;
- utilisation plus efficiente de l'énergie et des ressources, les systèmes OT pouvant être paramétrés plus précisément en fonction des besoins effectifs (optimisation de l'utilisation des moyens du production grâce à l'analyse des données issues de capteurs, p. ex.) ;
- gestion plus efficace des installations, étant donné que tous les systèmes IT et OT sont répertoriés et gérés selon une méthode commune, permettant d'avoir une vue d'ensemble.

Les UVTD qui s'attacheront à la mise en œuvre systématique de la norme minimale pour améliorer la résilience informatique en exploitant les opportunités qu'elle offre reconnaîtront que la sécurité informatique n'est pas un facteur de coût, mais bien un avantage économique sous l'angle de la sécurité d'approvisionnement de la Suisse.

Objectifs de protection pour l'IT et l'OT



Objectifs de protection pour la sécurité informatique (triade CIA)

Objectifs de protection pour la sécurité de la OT (disponibilité prioritaire)

Figure 1 : Objectifs de protection pour l'IT et l'OT

2 Contexte

En Suisse, 80 à 90 millions de tonnes de déchets sont produites chaque année. Il s'agit en grande partie de matériaux d'excavation et de percement, ainsi que de matériaux de déconstruction. Vu le niveau de vie élevé qui prévaut en Suisse, notre pays figure parmi les plus gros producteurs de déchets urbains à l'échelle mondiale, avec 716 kg par habitant. Le taux de recyclage est d'environ 53 %. Afin de réduire la consommation de ressources primaires de la Suisse, la Confédération souhaite prendre en considération tous les flux de substances et matières le long de la chaîne de valeur, de l'exploitation des matières premières à la gestion des déchets, en passant par la conception des produits.

La loi sur la protection de l'environnement définit les déchets comme « les choses meubles dont le détenteur se défait ou dont l'élimination est commandée par l'intérêt public »[1]. Selon la loi, l'élimination des déchets comprend leur valorisation ou leur stockage définitif ainsi que les étapes préalables que sont la collecte, le transport, le stockage provisoire et le traitement. La notion de traitement désigne toute modification physique, biologique ou chimique des déchets. Par utilisation, on entend toute opération impliquant des substances, des organismes ou des déchets, notamment leur production, leur importation, leur exportation, leur mise dans le commerce, leur emploi, leur entreposage, leur transport et leur élimination.

L'ensemble des activités et tâches en lien avec la prévention, la réduction, la valorisation et le stockage des déchets relèvent de la gestion des déchets : cette dernière peut être confiée à des entités publiques, privées ou mixtes.

La gestion des déchets couvre :

- la planification stratégique de la gestion des déchets à l'échelle locale, régionale, cantonale et nationale ;
- les possibilités de limitation et de prévention des déchets, moyennant par exemple des services de conseil en matière de déchets ;
- le tri et la séparation des déchets mixtes collectés ;
- la valorisation et le recyclage des déchets (compost, combustibles dérivés de déchets, déchets de chantier, matériaux d'excavation, métaux, p. ex.) ;
- la collecte et le transport des déchets (points de collecte, conteneurs, véhicules, unités de transbordement) ;
- le traitement (mécanique, chimique, biologique, thermique) des déchets à des fins de valorisation en aval (recyclage) ou de stockage ;
- le stockage des déchets et des résidus de traitement (recherche de sites, planification, mise en décharge des déchets, lixiviats de décharges, etc.).

Transport des déchets

Le transport des déchets comprend les différentes prestations de collecte auprès des producteurs de déchets et l'acheminement des déchets entre les acteurs impliqués dans la valorisation et le stockage. Il est assuré par les entreprises qui collectent et transportent les déchets, exploitent des centres de transbordement, effectuent des collectes mobiles de déchets spéciaux provenant des ménages pour le compte d'une commune et les remettent directement à une entreprise d'élimination sans stockage intermédiaire, ou encore les entreprises qui exploitent des véhicules sans dispositif d'assainissement des eaux usées (camions hydrocureurs).

Une perturbation à large échelle de la collecte des déchets donnerait lieu, à moyen terme, à un entassement des déchets dans les villes et les communes et, selon toute probabilité, à une multiplication des décharges sauvages. Les déchets entreposés dans les rues entraîneraient de graves problèmes d'hygiène, qui s'accompagneraient de risques sanitaires. Assez vite, les entreprises pâtiraient elles aussi de l'amoncellement de déchets : les clients déserteraient, le manque de capacités de stockage rendrait la production impossible, les conditions d'hygiène ne permettraient pas de travailler normalement, etc. De plus, les déchets spéciaux non traités risqueraient de polluer l'environnement, de favoriser la propagation de maladies, voire de provoquer des épidémies.

[1] *Loi sur la protection de l'environnement (LPE), RS 814.01, art. 7.*

Le schéma suivant montre la structure de la branche de la gestion des déchets et les recoupements avec d'autres sous-secteurs critiques :

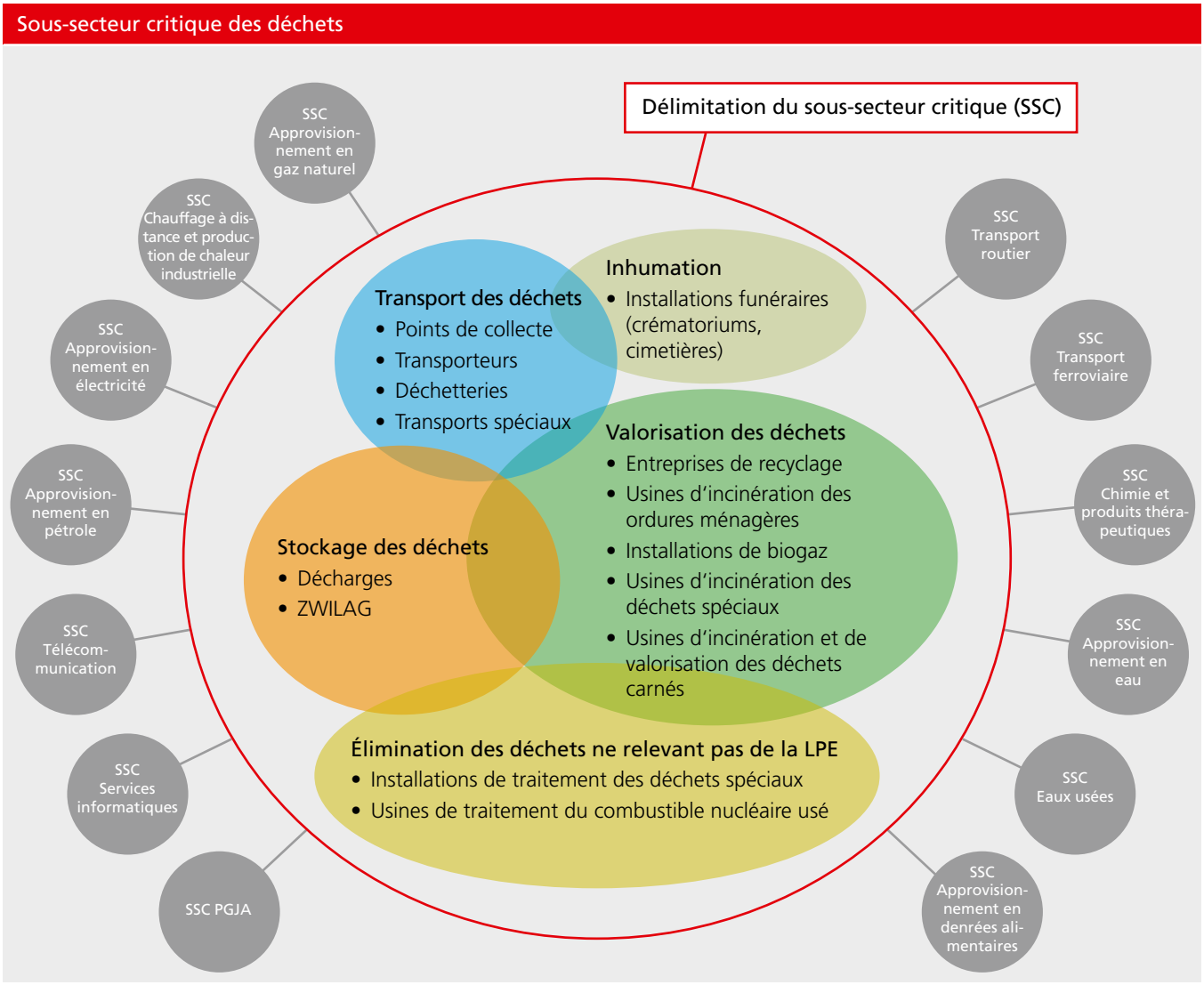


Figure 2 : Sous-secteur critique des déchets

Valorisation des déchets

La gestion des déchets poursuit plusieurs objectifs, dont la récupération des matières premières (dans les limites de ce qui est possible et économiquement raisonnable), la valorisation énergétique des déchets et la limitation des quantités de déchets destinés à une mise en décharge à long terme. Différentes méthodes sont employées pour la valorisation thermique, la valorisation matière ou une combinaison de ces deux procédés.

En 2020, les UVTD ont incinéré plus de 4 millions de tonnes de déchets, exploitant ainsi l'intégralité de leurs capacités. Une panne prolongée d'une installation générerait des tensions notables sur le circuit d'élimination des déchets dans le pays. Les déchets provenant des régions étrangères proches de des frontières sont acceptés, ce qui est judicieux sur le plan écologique car cela évite de longs transports. Par ailleurs, la Suisse exporte plusieurs centaines de milliers de tonnes de déchets qui ne peuvent pas être traités ou valorisés dans le pays (déchets spéciaux, déchets plastiques issus du tri sélectif, p. ex.).

En Suisse, il existe à ce jour 29 UVTD qui incinèrent les déchets non valorisables d'une autre manière, tout en préservant l'environnement. La chaleur dégagée par l'incinération est utilisée à des fins de chauffage et de production d'électricité. Les métaux et autres matières sont séparés des scories et des poussières de filtration restantes, tandis que les résidus sont mis en décharge.

Il existe d'autres installations thermiques que les UVTD, comme les incinérateurs de boues d'épuration ou les centrales thermiques au bois. Aussi différentes soient-elles, ces installations ont pour dénominateur commun l'élimination des substances. Ces déchets, dont certains ont un pouvoir calorifique élevé, peuvent être utilisés comme combustibles de substitution pour la production d'énergie ou pour économiser des ressources primaires.

En ce qui concerne les déchets biogènes, le compostage et la méthanisation présentent de nets avantages écologiques par rapport à l'incinération dans une UVTD, car ils permettent un recyclage de la substance naturelle.

Environ la moitié des déchets urbains sont collectés séparément, puis triés, ce qui les rend en grande partie recyclables. Les principales matières premières réintégrées dans le cycle de production à partir de déchets sont le papier, le verre, les déchets verts, le métal, le bois et les textiles. Une grande partie des déchets de chantiers minéraux, comme le béton, peuvent également être retraités et réutilisés en tant que matériau de construction recyclé.

La communication des autorités sur la gestion des déchets joue un rôle important dans la valorisation des déchets. En l'absence d'une sensibilisation et d'une information régulière, la population se retrouve rapidement moins au fait des gestes corrects à effectuer pour éliminer les déchets dans le respect de l'environnement.

La valorisation des déchets a une importance économique directe considérable du fait de la valeur ajoutée générée par le sous-secteur lui-même ainsi que pour les acheteurs de produits recyclables, de matières premières et des énergies thermique et électrique issues de la valorisation.

Stockage des déchets

Le sous-secteur du stockage des déchets couvre la mise en décharge et le stockage des déchets.

Les déchets qui ne peuvent pas être valorisés doivent être traités de manière à ne pas nuire à l'environnement une fois mis en décharge. Le type de décharge choisi (A, B, C, D, E) pour le stockage définitif d'un déchet est fonction de sa composition et de sa concentration en polluants. Les critères de classification et d'admissibilité applicables à la mise en décharge des déchets à stocker sont définis dans l'ordonnance sur les déchets (OLED).

Les déchets fortement contaminés, comme les cendres volantes ou les résidus issus du traitement de ces cendres par lavage, sont en partie exportés à l'étranger pour être stockés dans une décharge souterraine.

Une large part des déchets peut être valorisée en tant que matière première. Par valorisation des déchets, on entend leur valorisation thermique ou leur valorisation matière. Les méthodes d'élimination usuelles des déchets en Suisse sont décrites ci-après.

2.1 Valorisation matière

Recyclage

Le recyclage désigne la réutilisation immédiate des produits usagés (vêtements de seconde main ou pièces de véhicule encore utilisables, p. ex.), d'une part, et la valorisation matière, d'autre part, soit la récupération de matières premières secondaires à partir de déchets (production de verre à partir de débris, fonte de débris de fer ou fabrication de matériaux de construction recyclés à partir de déchets de chantier, p. ex.). Le décyclage *(downcycling)* désigne la transformation de déchets en matériaux de qualité inférieure à celle des matériaux utilisés à l'origine.

Valorisation des matériaux d'excavation et des déchets de chantier

Les matériaux d'excavation et les déchets de construction issus de la démolition de bâtiments et d'infrastructures représentent, en termes de volume, la plus grande partie des matériaux passant par la filière de la valorisation matière. Ils proviennent aussi bien de la démolition contrôlée de bâtiments ou étages complets que de la construction d'annexes ou de transformations. Contrairement aux anciennes pratiques de démolition incontrôlée à la boule de démolition ou par dynamitage, la démolition de bâtiments prend aujourd'hui souvent la forme d'une déconstruction sélective, avec un tri affiné des fractions de déchets effectué directement sur place.

Compostage et méthanisation

Le compostage et la méthanisation des déchets biogènes ou organiques sont un autre pan important de la valorisation matière. La notion de déchet organique recouvre les déchets d'origine végétale, animale ou microbienne, qui proviennent de l'agriculture, de l'industrie agro-alimentaire ou de la consommation privée.

2.2 Traitements physico-chimiques et biologiques

Les traitements physico-chimiques ou biologiques éliminent les polluants contenus dans les déchets ou permettent un stockage sécurisé. Les procédés de traitement biologique transforment les polluants en produits inoffensifs à l'aide de micro-organismes ou de plantes.

Les traitements physico-chimiques ou biologiques comprennent les principaux procédés ci-dessous :

- Les déchets aqueux sont libérés de leurs polluants par filtration, précipitation ou d'autres techniques comme la décomposition par le biais de micro-organismes, de sorte que l'eau peut ensuite être déversée dans la canalisation d'eaux usées. Selon leur composition, les polluants séparés sont soit incinérés, soit mis en décharge contrôlée.
- Les différents composants des déchets liquides mixtes sont dissociés en vue d'une revalorisation partielle.
- Les déchets à consistance boueuse doivent souvent être déshydratés avant de pouvoir être incinérés ou mis en décharge contrôlée.
- Les déchets solides fortement pollués ne peuvent pas être mis en décharge sans avoir été préalablement traités. La teneur en polluants des matériaux d'excavation peut être réduite grâce au lavage. Les polluants organiques sont détruits à l'aide d'un traitement thermique, ou décomposés en substances inoffensives grâce à l'action de micro-organismes ou de plantes. Les déchets ayant une forte teneur en métaux lourds, tels que les cendres volantes issues des installations d'incinération des déchets, sont soumis à un lavage acide, qui permet d'extraire les métaux lourds contenus dans les cendres.

Décharges

Les résidus issus de l'incinération ou les déchets qui ne se prêtent pas à la valorisation matière ou thermique sont stockés dans des décharges conformes aux dispositions légales. S'ils ne remplissent pas les exigences relatives au stockage, ils doivent être prétraités.

2.3 Valorisation thermique

En Suisse, les déchets sont incinérés pour réduire les quantités mises en décharge ainsi qu'à des fins de stérilisation. L'énergie libérée par l'incinération est ensuite récupérée et réutilisée. Les déchets qui font l'objet d'une valorisation thermique sont les déchets combustibles qui ne peuvent pas être soumis à une valorisation matière. Ils sont incinérés dans des UVTD ou encore dans des cimenteries ou d'autres installations industrielles. Les UVTD suisses utilisent toutes la chaleur de la combustion pour produire de l'électricité ou pour alimenter des réseaux de chauffage urbain et des installations industrielles. Par ailleurs, le traitement des scories permet la récupération de fer, d'aluminium, de cuivre et d'autres métaux.

Dans les cimenteries et les autres installations industrielles, les déchets servent de source d'énergie afin de produire de la chaleur industrielle qui est utilisée pour fabriquer ou transformer des produits (le ciment p. ex.).

L'incinération des déchets dégage des polluants atmosphériques qui sont en grande partie filtrés par un système d'épuration des fumées et de dénitrification à plusieurs niveaux, de sorte que seules de faibles quantités de polluants sont rejetées dans l'environnement.

Le graphique ci-après illustre la structure d'une UVTD. La présente norme traite des aspects liés à l'élimination des déchets. Des normes séparées ont été rédigées pour les domaines du chauffage à distance, de l'approvisionnement en électricité et des eaux usées (bien que la plupart des installations relèvent de l'ensemble de ces sous-secteurs).

Structure d'une usine de valorisation thermique des déchets

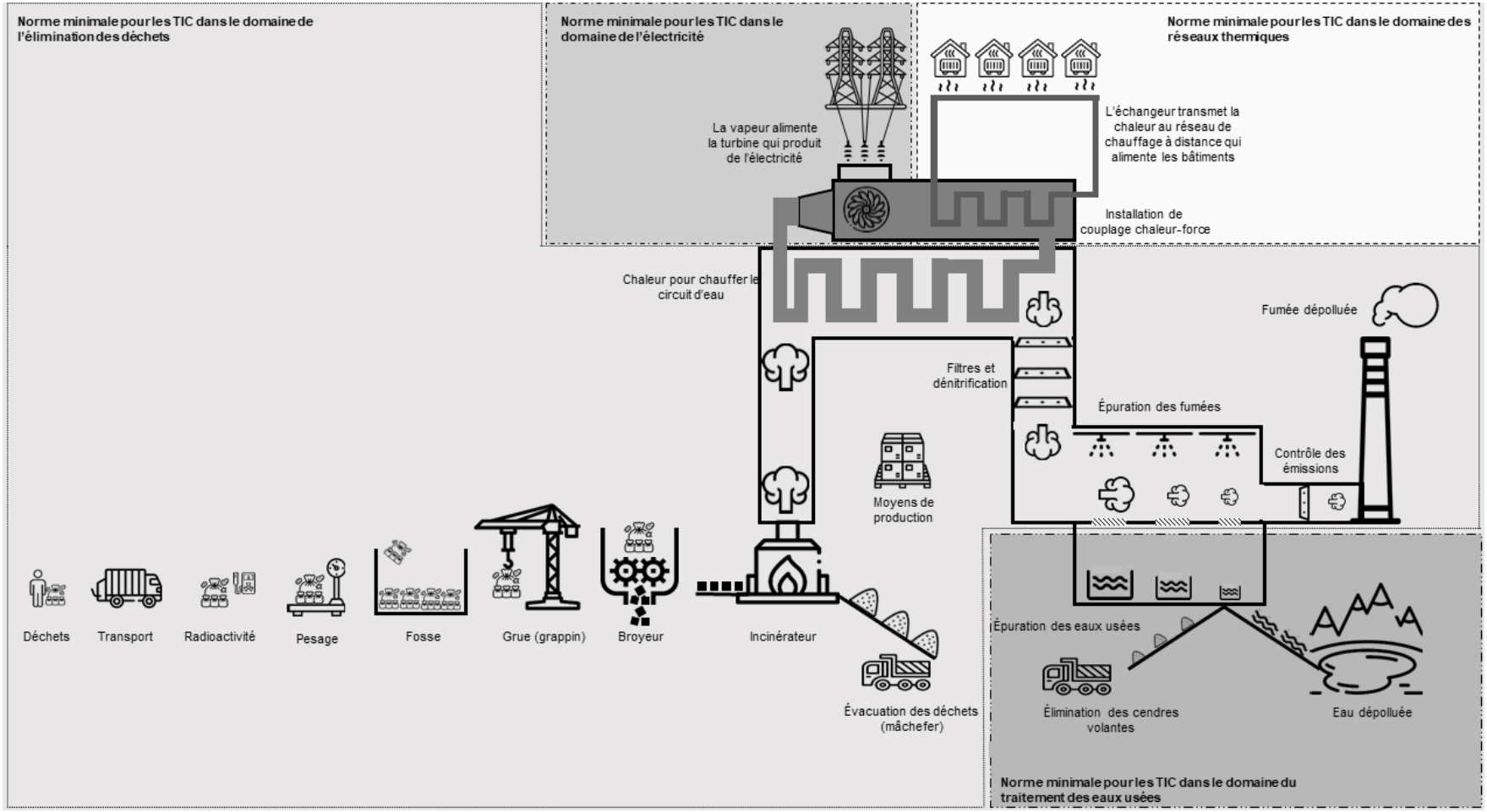


Figure 3 : Structure d'une usine de valorisation thermique des déchets

3 Objectifs de la norme minimale

Le présent document s'adresse aux entreprises actives dans la gestion des déchets. Il formule des recommandations sur la manière de réduire à un niveau acceptable les risques pesant sur la protection de l'information, par l'application d'une approche fondée sur les risques et d'une stratégie de défense en profondeur.

En plus d'assurer sa mission première, à savoir éliminer les déchets dans le respect de l'environnement et des prescriptions légales, la valorisation thermique des déchets génère de l'énergie utilisable. En outre, le traitement des scories permet la récupération de métaux. Les résidus contaminés issus de l'incinération, quant à eux, doivent être entreposés dans des décharges. Le traitement et la mise en décharge engendrent des flux de matières supplémentaires, qui, perturbés ou interrompus, sont susceptibles d'entraver considérablement la réalisation de la mission première de la valorisation thermique. On l'aura compris, une UVTD présente de nombreux vecteurs d'attaque insoupçonnés, qu'il convient de ne pas sous-estimer.

Pourquoi protéger l'information ?

- D'une part, les risques tendent à augmenter, parce que la *cyber*criminalité est une activité très lucrative. D'autre part, les entreprises industrielles sont visées par des activités de sabotage.
- La dépendance croissante vis-à-vis des systèmes d'information et de commande accroît les facteurs de vulnérabilité.
- Les infrastructures critiques sont interdépendantes (gestion des déchets hospitaliers, protection de l'environnement, p. ex.).
- Augmenter la résilience de son entreprise en améliorant la sécurité de l'information apporte des avantages économiques.

Afin de préserver la sécurité de l'information, cette norme propose une **approche fondée sur les risques,** qui consiste à évaluer les processus sous l'angle des risques et à quantifier leurs conséquences en termes de criticité (Cf. tableau 3 Processus critiques dans les UVTD).

L'autre méthode utilisée est la stratégie de défense en profondeur.

La stratégie de défense en profondeur est une approche qui s'inspire du principe militaire selon lequel un ennemi aura plus de difficultés à surmonter un système de défense multicouche complexe qu'à franchir une simple barrière. L'objectif de cette stratégie est donc de mettre en place plusieurs mesures de sécurité à différents niveaux de protection afin de confronter l'attaquant au franchissement d'une multitude de barrières de sécurité complexes.

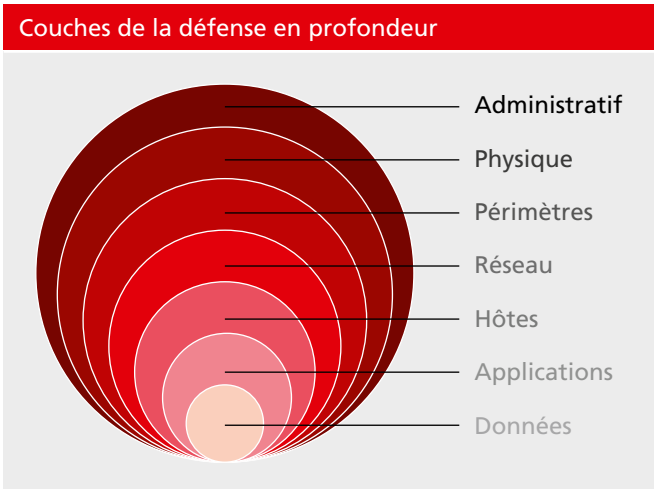


Figure 4 : Couches de la défense en profondeur

4 Processus et activités critiques

Le schéma suivant présente les potentielles cibles d'attaques d'une UVTD :

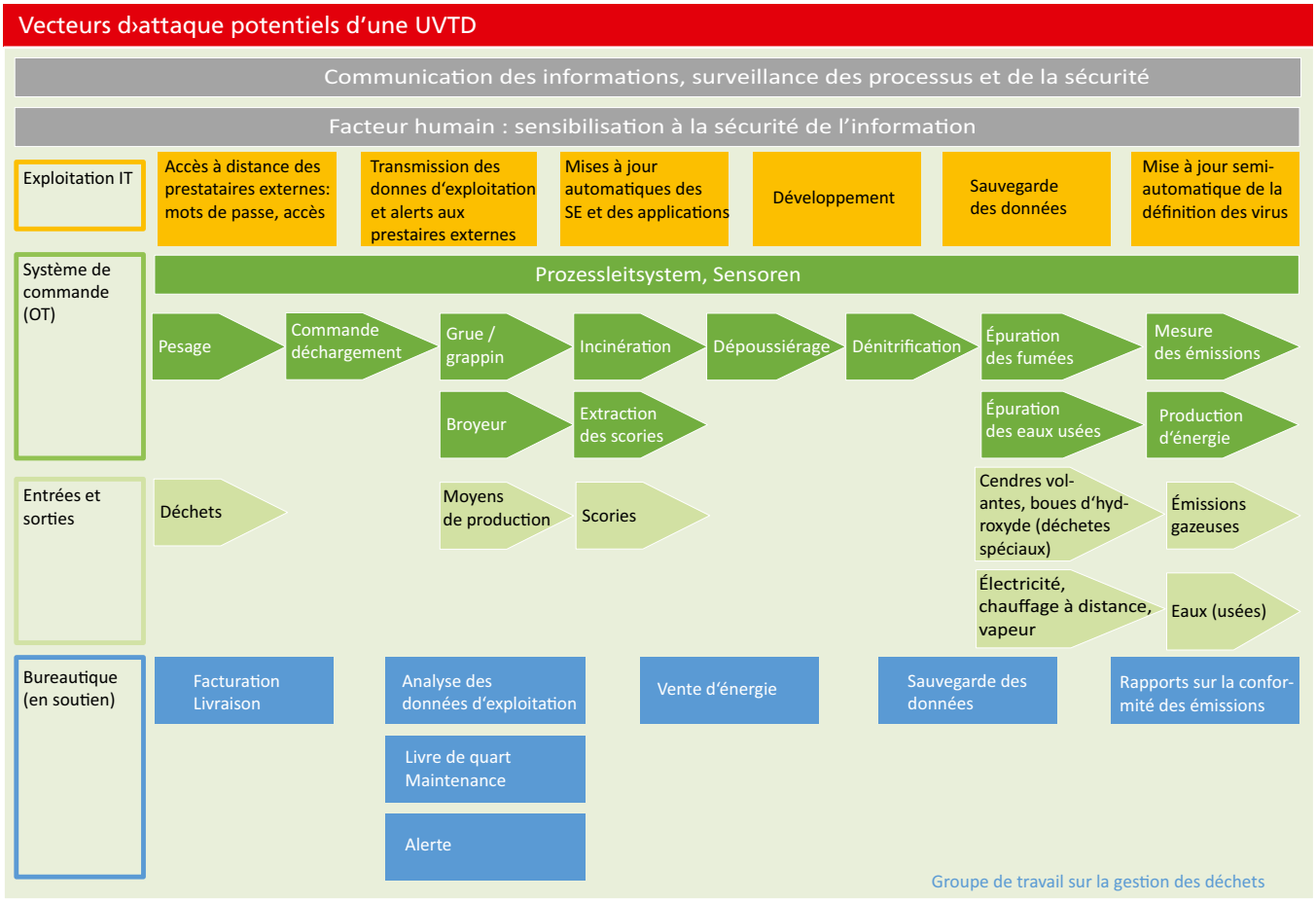


Figure 5 : Vecteurs d'attaque potentiels d'une UVTD

À des fins d'analyse de la vulnérabilité, les différents champs thématiques sont exposés ci-dessous, assortis de diverses solutions possibles.

4.1 Communication

Il est impossible aujourd'hui de se passer de systèmes de communication fiables (voix et données), que ce soit pour assurer le bon déroulement des processus ou pour garantir que toutes les personnes de l'entreprise sont joignables en cas d'urgence.

La communication d'urgence avec les services externes, notamment, ne doit pas être oubliée si l'on souhaite être en mesure de contacter les autorités ou les organisations d'intervention d'urgence en cas de crise. La définition des moyens et canaux de communication devrait se faire en amont, et non au moment où se déclare une crise. Il convient également de définir les applications de messagerie utilisées pour la communication mobile. Il est important d'opter uniquement pour des applications qui transmettent les données de manière sécurisée (grâce au cryptage, p. ex.). S'agissant des applications mobiles, il faut par ailleurs veiller à ce que les données ne soient pas synchronisées involontairement et, partant, transmises à des tiers.

En prévention d'une panne de système, les numéros de téléphone les plus importants et les plans d'urgence devraient être imprimés et consignés dans un classeur consacré aux situations d'urgence.

Moyens de communication internes	Moyens de communication externes
• Téléphonie IP • Radio, radiocommunication à usage professionnel • Téléphones DECT, WiFi, opérateurs de téléphonie sans fil • Système d'alerte ou d'évacuation • Opérateurs d'installations GSM, téléphones GSM (appareils mobiles/téléphones portables)	• Ligne de secours directe qui est reliée au central téléphonique du quartier (Swisscom, p. ex.) et contourne le central interne • Stations radio Polycom/talkie-walkie • Téléphones GSM (portables) • Messagerie sécurisée • Système de messagerie électronique alternatif en cas de panne de la messagerie interne

Tableau 1 : Communication interne et externe

Comme bien souvent dans le domaine technique, il n'existe pas de solution unique pour couvrir tout l'éventail des besoins ; il s'agit de combiner plusieurs solutions pour assurer la disponibilité souhaitée.

Les systèmes GSM (téléphones portables) sont ainsi moins adaptés à la communication dans les sous-sols ou dans des bâtiments blindés comme les constructions métalliques, le signal reçu y étant fortement limité en l'absence d'antennes internes coûteuses. Il en va de même pour la radiocommunication à usage professionnel usuelle dans les bandes de 4 m, 2 m et 70 cm et pour les installations de téléphonie DECT, car ces dernières ont également besoin d'antennes et de stations relais pour fonctionner dans les sous-sols et les locaux à fort blindage électromagnétique.

Il convient, lors de l'utilisation de services de messagerie, de veiller à ce qu'aucune copie de données, en particulier les coordonnées des contacts, ne soit envoyée au prestataire de solutions. De plus, le service devrait proposer un chiffrement de bout en bout des messages vocaux et textuels afin d'assurer la confidentialité des communications.

4.2 Facteur humain : formation et sensibilisation des collaborateurs

Les erreurs commises par les employés sont à l'origine d'une large majorité des *cyber*attaques. D'où la nécessité de cours de formation et de sensibilisation pour pallier les vulnérabilités dues au facteur humain. Une description détaillée à ce sujet figure au chapitre 6.6. Les collaborateurs doivent être sensibilisés aux thèmes suivants :

Possibilité d'attaque	Menace
Spams et courriels d'hameçonnage *(phishing)*	Les courriels malveillants représentent une menace récurrente pour la sécurité de l'information d'une entreprise. On désigne par les termes de spams ou de courriels indésirables les messages non sollicités, généralement importuns et de nature publicitaire, transmis en masse par voie électronique sans le consentement de leur destinataire. Les spams peuvent « inonder » le serveur de messagerie de l'entreprise au point de le ralentir, voire de le paralyser. Les courriels d'hameçonnage, quant à eux, présentent un danger bien plus grand. L'hameçonnage *(ou phishing)* désigne l'envoi de courriels falsifiés destinés à piéger le destinataire par la fraude. Les courriels d'hameçonnage ont souvent pour but de pousser les destinataires à divulguer des informations financières, des données d'accès ou d'autres informations sensibles.
Maliciels *(malware)*	Les logiciels malveillants, ou maliciels sous leur dénomination abrégée, sont des logiciels destinés à endommager les systèmes ou à nuire aux utilisateurs qui se propagent le plus souvent de manière autonome. Le pirate informatique peut par leur biais parvenir à espionner (clavier, disque dur) ou crypter des données et à obtenir des accès d'administrateurs. Les principales formes de maliciels sont les virus, les chevaux de Troie, les logiciels espions et les rançongiciels *(ransomware)*.
Ingénierie sociale	L'ingénierie sociale consiste à manipuler une personne sur le plan psychologique dans le but de gagner sa confiance et, par exemple, de lui soutirer des informations confidentielles ou d'obtenir des données de cartes de crédit ou des mots de passe. L'ingénierie sociale peut se pratiquer par voie physique, par courriel, par téléphone ou via les médias sociaux.

Tableau 2 : Possibilités d'attaque et menaces

Comme déjà mentionné au début de ce chapitre, les vulnérabilités dues au facteur humain constituent les principales portes d'entrée permettant aux *cyber*attaques de toucher leur cible. Il est donc primordial de faire suivre au personnel une formation régulière à raison de 2 à 3 sessions annuelles dans le cadre d'un programme de sensibilisation continu à la sécurité de l'information. Il faut que les collaborateurs aient une perception de la sécurité de l'information qui les conduise à se comporter correctement de manière intuitive, autrement dit qu'ils développent une compétence inconsciente, selon les termes utilisés pour qualifier cette phase de l'apprentissage.

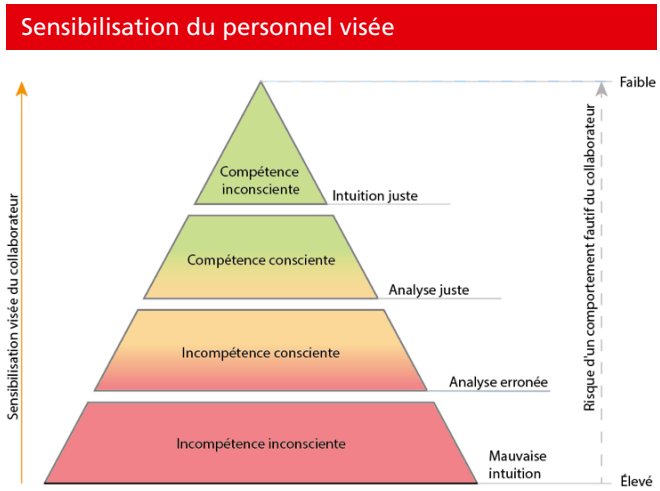


Figure 6 : Sensibilisation du personnel visée

4.3 Système vidéo

Le système vidéo est un des maillons indispensables de la chaîne de sécurité physique, mais il comporte certains risques s'il n'est pas installé par une personne qualifiée et géré selon des règles strictes. La question la plus importante qui se pose est le respect de la loi fédérale sur la protection des données (LPD). À cette fin, il est nécessaire de disposer d'un concept d'exploitation qui spécifie notamment ce qui est enregistré, où et quand, les utilisateurs qui ont accès aux vidéos, la durée de conservation des images et les personnes qui sont habilitées à ordonner leur vérification ainsi que les cas où elles peuvent le faire. En outre, une attention particulière doit être accordée aux modalités de sauvegarde des données, car il faut s'assurer que les images sont effacées après le délai de conservation.

Voici quelques exemples d'utilisation de la vidéosurveillance :

- surveillance des accès à la limite du périmètre (entrées principales et latérales) ;
- surveillance des processus (fosse, système de déchargement, pesage, etc.) ;
- surveillance des locaux sensibles (salles de serveurs) ;
- enregistrement vidéo déclenché automatiquement en cas d'incident, qui permet de filmer en direct l'évènement et de transmettre les images au poste de conduite afin de réduire les risques de panne.

4.4 Exploitation informatique

4.4.1 Télémaintenance par des prestataires externes

Les prestataires de services ne doivent **jamais pouvoir accéder en permanence** aux systèmes à distance, en particulier lorsqu'il s'agit de systèmes nécessaires à l'accomplissement du mandat légal d'élimination des déchets ou d'approvisionnement.

Les accès accordés à des personnes externes doivent respecter les conditions suivantes :

a) Les accès sont verrouillés par des outils réseau lorsqu'ils ne sont pas utilisés.
b) Les accès sont autorisés uniquement à titre provisoire dans le cadre de maintenances planifiées et se font via des connexions sécurisées (VPN, p. ex.).
c) Le nombre d'utilisateurs chez le prestataire est réduit au strict minimum, moyennant une identification nominative et un compte individuel.
d) Les accès à des fins de maintenance sont, idéalement, administrés de manière centralisée par un système de gestion des accès à privilèges (*Privileged Access Management,* PAM), en usant d'une authentification multifacteur (AMF) et de fonctionnalités d'enregistrement ou de journalisation (piste d'audit). La gouvernance en matière d'accès doit être uniforme. Si des exceptions sont nécessaires pour des raisons impérieuses, elles doivent être documentées et surveillées.

Les mots de passe d'accès au système doivent être renouvelés à intervalles réguliers par l'administrateur système, pour garantir que les personnes qui ne sont plus employées par le prestataire ne puisse pas accéder au système.

4.4.2 Données d'exploitation transmises à des prestataires externes

Les données d'exploitation requises par les prestataires et les fournisseurs externes ne comprennent généralement pas de données de processus en ligne. Elles peuvent donc être générées de manière automatique par le système de commande sur un répertoire hors du réseau de processus. Le prestataire peut ainsi obtenir les données dont il a besoin sans avoir accès au système de commande.

La copie directe d'informations pendant une session de télémaintenance devrait être impossible : il est plus judicieux de fournir à l'utilisateur un disque dur externe pour le transfert de données.

Il est fortement recommandé de définir dans les contrats ou dans un accord de niveau de service *(service-level agreement)* conclu avec le fournisseur ou prestataire externe quelles données seront transférées et dans quel but, quel sera le mode de transfert sécurisé utilisé et pendant combien de temps elles seront conservées chez le fournisseur ou prestataire.

4.4.3 Alarmes

On entend par systèmes d'alarme, outre les alarmes d'évacuation, les détecteurs d'incendie, l'appel – manuel ou relevant du flux de travail – des organisations d'intervention d'urgence en cas de dommages corporels et d'avaries graves, ainsi que la mobilisation automatisée de personnel supplémentaire et d'unités de soutien.

4.4.4 Mises à jour des systèmes d'exploitation et des programmes

Les mises à jour entièrement automatisées sur les réseaux OT sont risquées et ne sont donc pas recommandées. Dans les installations industrielles, les mises à jour devraient être validées, autorisées et, idéalement, installées par le fabricant. Ces prestations sont à définir précisément dans un accord de niveau de service, qui fixera également le nombre de cycles de mise à jour planifiés par an, ainsi que le délai jusqu'à la disponibilité de mises à jour de sécurité importantes entre les cycles planifiés.

Lorsque les réseaux OT étaient encore totalement autonomes et déconnectés d'internet, il suffisait de mettre à jour les systèmes une à deux fois par an et de combler les failles de sécurité. Mais avec l'interconnexion et la fusion croissantes de l'IT et de l'OT, les exigences en la matière ne cessent d'augmenter. Les systèmes dont les logiciels ne peuvent pas ou plus être mis à jour régulièrement doivent être complètement isolés ou accessibles uniquement à des conditions très restrictives lorsque l'accès est établi depuis des zones peu fiables.

Le processus de mise à jour des logiciels doit, à l'interne, faire l'objet d'une directive et, à l'externe, être défini dans un accord de niveau de service. Le respect de l'accord de niveau de service, documentation des prestations incluse, devrait être discuté et vérifié au moins une fois par an avec le fournisseur de prestations.

4.4.5 Développement

Le développement et l'adaptation internes de logiciels requièrent presque obligatoirement la mise en place d'un système de test et d'intégration correspondant au système de production. Étant donné que l'exploitation d'un, de deux ou, dans certains cas, de trois infrastructures systèmes est très coûteuse en termes de ressources humaines et financières, l'arbitrage du « *make or buy* » est ici particulièrement important. Autrement dit, il s'agit de comparer les bénéfices ainsi que les coûts et risques engendrés par le développement des logiciels et de l'infrastructure environnante à l'interne avec ceux d'une externalisation complète.

4.4.6 Sauvegardes

Afin de réduire le risque et les conséquences d'une perte de données (suite à des modifications involontaires ou à des défauts matériels, p. ex.), il convient, dans la mesure du possible, de mettre en place des sauvegardes régulières pour tous les systèmes informatiques. La stratégie de sauvegarde devrait prévoir différents emplacements pour la copie des données. Il est recommandé de conserver une copie locale des données sur les systèmes informatiques de manière à garantir un accès rapide, et de la doubler d'une sauvegarde sur un système central. Afin de prévenir le risque d'une attaque par rançongiciel, une copie de sauvegarde supplémentaire devrait être faite sur un système (« Air Gap »), isolé sur les plans physique et logique.

La stratégie de sauvegarde 3-2-1

Les sauvegardes de données dans des systèmes *cloud* à distance devraient être effectuées, à l'aide d'une technologie appropriée, dans les mêmes infrastructures que les systèmes locaux, afin que les données soient accessibles en cas de crise. Si cela n'est pas possible, il convient de prévoir avec le prestataire des procédures de gestion de la continuité d'activité GCA (*Business Continuity Management,* BCM) en ce qui concerne notamment la disponibilité, l'accès, le transport et le transfert des données.

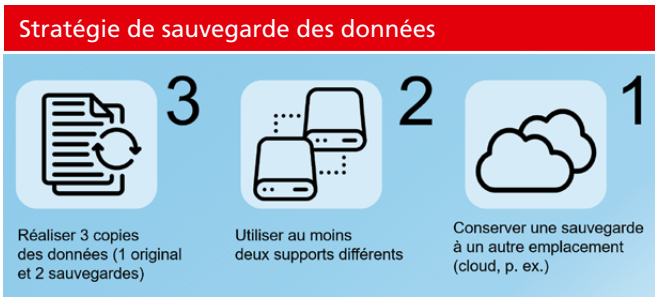


Figure 7 : Stratégie de sauvegarde des données Source : computerweekly.de

La sauvegarde devrait inclure les informations et données suivantes :

- systèmes d'exploitation et micrologiciels *(firmware)* ;
- configurations (routeurs, commutateurs, applications, règles de pare-feu, etc.) ;
- applications ;
- banque de données ;
- données de production ;
- autres données (données de protocole, p. ex.).

4.4.7 Mise à jour des définitions de virus

Une mise à jour automatisée et directe des définitions de logiciels malveillants sans scénarii de test en amont est risquée et n'est pas recommandée dans une infrastructure OT. Un fichier endommagé ou défectueux pourrait affecter un ou plusieurs systèmes, voire provoquer une panne.

Il est par conséquent recommandé de vérifier en détail chaque paquet de mise à jour antivirus avant de l'installer dans un environnement de test. Dans la mesure du possible, l'intégrité du fichier devrait être vérifiée par une somme de contrôle (*hash* MD5). Si l'infrastructure à cet effet manque, on peut opter avantageusement pour une mise à jour séquentielle. Entre les différentes étapes de mise à jour, il convient, pour réduire les risques, de s'assurer que les systèmes déjà actualisés fonctionnent sans erreur et de manière stable. Toutefois, ce déploiement séquentiel ne devrait pas s'étendre sur plusieurs semaines, au risque d'introduire dans le système un logiciel malveillant non détecté.

4.5 Processus OT

4.5.1 Pesage

Le poste de pesage permet de peser tous les véhicules avant et après le déchargement des déchets, des boues d'épuration, des intrants (moyens de production), etc. Les quantités acheminées dans les installations sont ainsi saisies et contrôlées avec exactitude, et les chiffres obtenus sont ensuite utilisés pour la facturation.

Pour le bon fonctionnement des lignes d'incinération, il est indispensable de connaître le plus précisément possible l'intégralité des apports et leur composition, de sorte à pouvoir, d'une part, déterminer la quantité de déchets/boues d'épuration à éliminer ou à mettre en réserve afin d'exploiter les lignes de fours de manière optimale pendant toute la durée de fonctionnement, et, d'autre part, calculer la quantité de intrants (moyens de production) nécessaire à l'exploitation et contrôler le bon déroulement du processus d'incinération.

Le poste de pesage se compose essentiellement d'un système de pesée, d'un affichage, de barrières et/ou de feux de signalisation et d'une interface reliée à un ou plusieurs systèmes externes (exploitation, bureau, facturation) vers lesquels les données sont transmises. On utilise souvent à cette fin un système complet doté d'un automate programmable industriel (API).

Le pesage en tant que tel n'est pas un processus hautement critique et peut être effectué manuellement en cas d'urgence, mais on sous-estime souvent les conséquences qu'une panne de ce dispositif aurait pour l'entreprise.

4.5.2 Système et point de déchargement

Le transport des déchets se fait généralement par camion, par train ou, plus rarement, par bateau. Selon l'installation, les déchets sont soit déversés directement dans la fosse, soit transportés vers la fosse par un système ad hoc, qui peut prendre plusieurs formes. Les déchets peuvent par exemple être déchargés sur une table avant d'être déversés vers la fosse par un dispositif de basculement. L'installation concernée est généralement commandée par un API, qui peut être piloté de manière autonome (par un panneau de commande), via une interface matérielle reliée au système de commande, ou encore par le système de commande principal s'il y est directement intégré. Une UVTD

dispose en général de plusieurs lignes de déchargement. Selon la configuration de l'installation, la commande doit être conçue de manière à ce qu'une panne n'entraîne pas de paralysie totale de l'alimentation du four ou du déchargement des déchets susceptibles de conduire à des problèmes de réapprovisionnement ou à un engorgement au point de déchargement des déchets. Le risque d'une panne totale peut être évité ou réduit grâce à des systèmes de commande indépendants ou redondants.

4.5.3 Grappin (et déchargement)

Le grappin permet de mélanger et d'entasser les déchets dans la fosse avant que ceux-ci ne soient déversés dans la trémie d'alimentation du four. Le grutier le commande généralement depuis la salle de contrôle, d'où est supervisé l'ensemble du processus de combustion.

Le degré d'automatisation des grappins étant déjà très élevé, l'alimentation du four se fait souvent de manière entièrement automatique. Le système de grappin est fréquemment doté d'une interface avec le système de commande, ce qui permet le paramétrage des quantités d'ordures ménagères nécessaires. Les grappins disposent de leur propre système de pesage, qui sert à peser et à consigner systématiquement les quantités requises et les quantités livrées.

Le grappin se commande lui aussi habituellement par l'intermédiaire d'un API, équipé – selon le degré d'automatisation – d'interfaces avec des systèmes externes. En règle générale, le grutier pilote le grappin à l'aide de joysticks, en étant assisté par des systèmes de caméra et/ou un écran. Compte tenu du niveau de disponibilité requis, l'exploitation des grappins est souvent redondante, ce qui signifie qu'un deuxième dispositif est disponible en cas de panne.

4.5.4 Broyeur

Le broyeur est utilisé pour broyer des déchets encombrants, entre autres. Généralement, les matériaux à broyer sont livrés séparément des déchets ménagers.

Selon l'installation, les matériaux à broyer sont soit stockés séparément, soit broyés directement après le déchargement, avant d'être mélangés aux déchets ménagers.

Souvent, les déchets encombrants sont dans un premier temps stockés dans un conteneur séparé ; dans ce cas, c'est à l'arrivée du conteneur que le grutier décide si les déchets doivent être broyés avant d'être mélangés aux autres déchets dans la fosse. Il existe une grande diversité d'applications et de processus, si bien que le risque de panne doit être évalué spécifiquement pour chaque broyeur et chaque installation. S'il n'est plus possible de broyer les déchets encombrants en raison d'une panne du broyeur et qu'il n'y a pas d'autre option pour broyer ou stocker ces déchets séparément, on peut très vite arriver à un goulot d'étranglement. Les propriétés de combustion des déchets, par exemple, peuvent alors changer très rapidement, ce qui complique le réglage du four.

Le broyeur est généralement piloté par un API. Certaines installations sont équipées de plusieurs broyeurs indépendants les uns des autres et alimentés individuellement. On utilise souvent un grappin pour transporter les déchets encombrants dans le broyeur. La commande du broyeur a en règle générale moins d'interfaces avec des systèmes tiers, car c'est habituellement le grutier qui décide quel matériau doit être broyé avant d'être mélangé dans la fosse. Le broyeur est le plus souvent équipé d'un système de détection précoce des incendies, car le procédé du broyage peut produire des étincelles susceptibles d'enflammer les matériaux.

4.5.5 Incinération

L'incinération est le processus central de l'élimination des déchets. En injectant de l'air comme oxydant, on déclenche une réaction d'oxydoréduction qui produit de l'énergie thermique et lumineuse. Un régulateur de combustion permet de paramétrer avec exactitude l'apport de combustible et le système de ventilateurs, y compris, selon les cas, la recirculation des fumées, de manière à assurer la performance thermique requise avec le moins d'excédent d'air possible, conformément aux normes en matière d'émissions. Selon les fours, la défaillance du régulateur de combustion peut provoquer un dommage total à la chaudière. Le dispositif de régulation devrait donc être localisé dans la zone de réseau 1 (cf. ch. 7.1, Zonage du réseau).

4.5.6 Extraction des scories

L'extraction des scories intervient, sur le plan de la matière, directement après l'incinération. Durant ce processus, les cendres et les résidus incombustibles sont refroidis puis stockés temporairement dans des conteneurs à scories, avant d'être transportés dans une décharge. Si le stockage des scories dans un conteneur n'est plus possible, l'incinération doit être stoppée.

4.5.7 Dépoussiérage

Les résidus de cendres produits dans le foyer du four et emportés avec l'air de combustion qui circule dans la chaudière sont connus sous la dénomination de cendres volantes. Ces dernières sont évacuées soit par voie électrostatique, soit par voie mécanique, afin d'assurer la poursuite du fonctionnement des systèmes de traitement des fumées situés en aval (catalyseurs, tours de lavage, p. ex.). L'impossibilité de procéder au dépoussiérage des fumées entraîne généralement un arrêt de l'incinération et donc de l'installation.

4.5.8 Dénitrification

Si la dénitrification intervient après la combustion proprement dite, on parle de traitement secondaire. Les procédés employés visent à réduire en grande partie les oxydes d'azote contenus dans les fumées, ceux-ci étant nocifs pour l'homme et l'environnement. En cas de panne empêchant la dénitrification, l'UVTD peut se voir retirer provisoirement son autorisation d'exploitation.

4.5.9 Épuration des fumées

L'épuration des fumées est en général le dernier processus actif avant le rejet dans l'atmosphère. Il consiste à dépolluer les fumées de sorte à se conformer aux normes environnementales. En cas de défaillance, l'UVTD risque un retrait provisoire de son autorisation d'exploitation.

4.5.10 Mesure des émissions

Après l'épuration des fumées, c'est-à-dire avant que les fumées ne soient rejetées dans l'atmosphère, il faut mesurer leur teneur en polluants, ce qui permet également de contrôler en dernière instance le bon fonctionnement des processus en amont. Les anomalies constatées ont des répercussions directes sur le paramétrage du régulateur de combustion, qui est alors ajusté soit automatiquement, soit manuellement. Si elle se trouve dans l'incapacité de mesurer ou de paramétrer les valeurs d'émission, l'UVTD peut se voir retirer provisoirement son autorisation d'exploitation.

4.5.11 Épuration des eaux usées

Suivant la configuration globale de l'installation, les processus en amont peuvent générer de grandes quantités d'eaux usées contaminées. Le cas échéant, ces eaux doivent être épurées avant d'être rejetées dans les cours d'eau publics. L'épuration peut être effectuée en interne ou par un prestataire. Une UVTD dans l'impossibilité d'assurer l'épuration des eaux usées risque de se voir retirer provisoirement son autorisation d'exploitation.

4.5.12 Production d'énergie

L'incinération engendre de l'énergie sous formes thermique et lumineuse. La chaleur permet, par des circuits séparés, de produire de la vapeur, de l'électricité et d'alimenter des réseaux de chauffage urbain. Si l'énergie ne peut plus être évacuée, la combustion s'arrête, d'où l'importance d'assurer une évacuation continue.

4.6 Bureautique (partie IT)

La bureautique (IT) et l'OT n'étant pas soumises aux mêmes exigences en termes de protection, elles devraient être strictement séparées via une segmentation du réseau. Les bonnes pratiques en la matière consistent à localiser la bureautique (IT) dans les couches supérieures (niveau 5 ou 6) du modèle de zones de réseau et de la séparer de l'OT par une DMZ (zone démilitarisée). Mieux vaut éviter les accès directs sans rupture protocolaire des zones de bureautique vers les systèmes OT (cf. ch 7.1). De tels accès doivent au moins transiter par un serveur de rebond dans la SCI – DMZ, idéalement en utilisant un système de gestion des accès à privilèges (PAM). Passer par un système de PAM permet, entre autres, de journaliser systématiquement les accès et de gérer de manière sécurisée les informations d'identification hautement privilégiées.

5 Dépendance, criticité et maturité

Le tableau ci-dessous indique le degré de dépendance informatique de chacun des processus critiques précités. Le présent chapitre traite pour l'essentiel de la question suivante : le processus peut-il être réalisé sans recourir aux TIC (dépendance) ? Le degré de dépendance informatique est classé en trois catégories (faible, moyen ou élevé). Il est jugé faible lorsque le processus peut être exécuté, en grande partie, sans recourir aux TIC, moyen lorsque le processus requiert un surplus de ressources (en temps, en personnel, etc.) et, enfin, élevé lorsque le processus ne peut être mené à bien en cas de panne informatique.

Les critères de classification se réfèrent uniquement et au sens strict à la dépendance de chaque processus à l'égard des systèmes IT et OT, et tiennent compte des alternatives existantes.

- Autonome = aucune dépendance vis-à-vis de systèmes IT et OT pilotables.
- Faible = une panne peut être aussi être résolue manuellement sans IT/OT.
- Moyen = une panne a des conséquences directes sur l'exploitation, laquelle est restreinte ; quelques alternatives existent.
- Élevé = une panne rend l'exploitation impossible ; il n'y a aucune alternative.

Cette proposition peut être modulée au cas par cas, en fonction des bilans d'impact sur l'activité (BIA, voir descriptif en annexe au présent document) et des analyses d'interfaces réalisées au sein des entreprises ou organismes. Le degré de maturité ne devrait toutefois pas être inférieur à 2 (exigence minimale relative à la sécurité de l'information, voir figure à la page 20).

Le degré de criticité du sous-processus figurant au tableau 3 permet d'illustrer l'impact en termes d'exécution du « processus clé de l'élimination des déchets (PCE) », indépendamment de la taille de l'installation. Prenons quelques exemples : quand un grappin tombe en panne, il n'est la plupart du temps plus possible d'incinérer des déchets et donc de les éliminer, ce qui entraîne un arrêt total du PCE. Quand l'épuration des fumées tombe en panne, cela a des conséquences désastreuses pour l'environnement. Le PCE s'en trouve perturbé selon l'installation concernée, l'exploitation restant possible moyennant un système de dérivation. Les processus en aval du PCE tels que l'approvisionnement thermique ou électrique de tiers NE SONT PAS pris en considération dans ce tableau, qu'ils relèvent ou non de l'infrastructure critique.

4 = arrêt total du « processus clé de l'élimination des déchets (PCE) »
3 = n'a qu'une légère incidence sur le PCE, forte incidence sur les systèmes périphériques
2 = pas d'incidence directe sur le PCE, possibilité de contourner temporairement le fonctionnement des systèmes périphériques par d'autres moyens
1 = pas d'incidence directe sur le PCE, mais autres conséquences à long terme

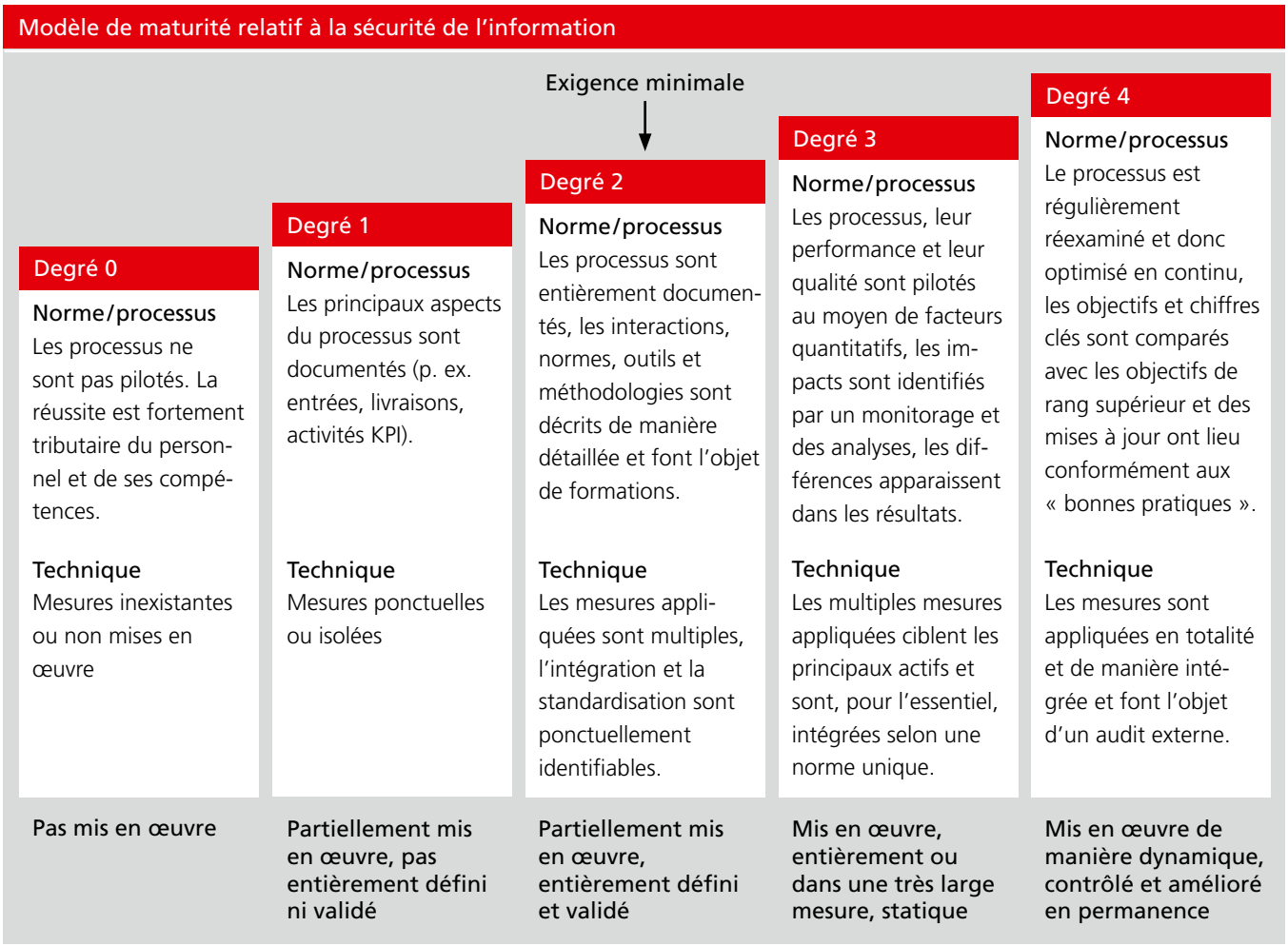


Figure 8 : Maturité en matière de sécurité de l'information

La maturité recommandée pour les UVTD se fonde sur le tableau 3 ci-après :

n/a = processus inexistant
0 = pas mis en œuvre
1 = partiellement mis en œuvre, pas entièrement défini ni validé
2 = partiellement mis en œuvre, entièrement défini et validé
3 = mis en œuvre, entièrement ou très largement mis en œuvre, statique (pas d'amélioration continue du processus)
4 = mis en œuvre dynamiquement, contrôlé et amélioré en continu

Remarque concernant l'indication n/a :
Les évaluations vont en principe de 0 à 4. L'indication n/a ne doit être utilisée que si le processus n'existe pas dans l'entreprise.

5.1 Maturité minimale recommandée

Le tableau suivant indique les maturités minimales recommandées pour chaque processus critique du domaine de l'incinération des déchets.

La recommandation se fonde, d'une part, sur l'évaluation des risques susceptibles d'affecter l'exécution de la mission de base en cas de défaillance du processus et, d'autre part, sur la dépendance du processus à l'égard de l'informatique.

Processus critiques dans les UVTD			
	Degré de dépendance informatique	Risque pour l'exécution du mandat	Maturité recommandée en matière de sécurité de l'information
Communication des informations	Moyen	Moyen	2–3
Facteur humain	Élevé	Élevé	2–3
Accès à distance par des prestataires externes	Élevé	Moyen	4
Évaluation des données d'exploitation	Faible	Faible	2–3
Mises à jour des systèmes d'exploitation et logiciels	Moyen	Faible	2–3
Développement	Élevé	Faible	2–3
Sauvegarde des donnéesOT	Élevé	Faible	3–4
Distribution semi-automatique des définitions de virus	Moyen	Faible	2–3
Pesage	Élevé	Moyen	2–3
Commande de largage	Moyen	Faible	2–3
Grappin	Élevé	Élevé	4
Incinération et chaudière	Élevé	Élevé	4
Dépoussiérage	Autonome	Moyen à élevé	3
Dénitrification	Moyen	Moyen	3
Épuration des fumées	Élevé	Moyen à élevé	4
Mesure des émissions	Élevé	Moyen	3–4
Broyeur	Moyen	Faible	2
Extraction des scories	Élevé	Élevé	3–4
Épuration des eaux usées	Élevé	Moyen	3–4
Moyens de production	Moyen	Moyen à élevé	3
Mesure de la radioactivité	Faible	Faible	2–3
Scories (évacuation)	Faible	Faible	2–3
Turbine	Moyen	Faible	3
Cendres volantes	Moyen	Moyen à élevé	2–3
Chauffage à distance, électricité, vapeur	Élevé	Élevé	3–4
Air comprimé	Faible	Élevé	3–4
Captage d'eau brute	Moyen	Élevé	3–4
Traitement de l'eau	Élevé	Élevé	4
Accès et autorisation	Élevé	Faible	3–4
Surveillance de la sécurité	Faible	Faible	2–3
Composants réseau IT-OT	Faible	Faible	2–3
Facturation, livraison	Élevé	Faible	2–3
Évaluation des données d'exploitation	Élevé	Faible	2–3
Vente d'énergie	Moyen	Faible	2–3
Sauvegarde des données informatiques	Élevé	Élevé	3–4
Conformité et reporting	Élevé	Faible	2–3
Livre de quart	Élevé	Faible	2–3
Alerte (feux bleus, autorités, personnel)	Moyen	Faible	2

Tableau 3 : Processus critiques dans les UVTD

La figure 9 montre la forte dépendance des processus clés (infrastructure, élimination des déchets et conduite de l'entreprise) vis-à-vis des systèmes et des sous-processus jugés critiques. L'idée est de montrer que la défaillance d'un sous-processus n'affecte généralement pas seulement un processus clé, mais plusieurs autres processus.

L'impact des sous-processus sur les processus clés est illustré dans le tableau à la page 23:

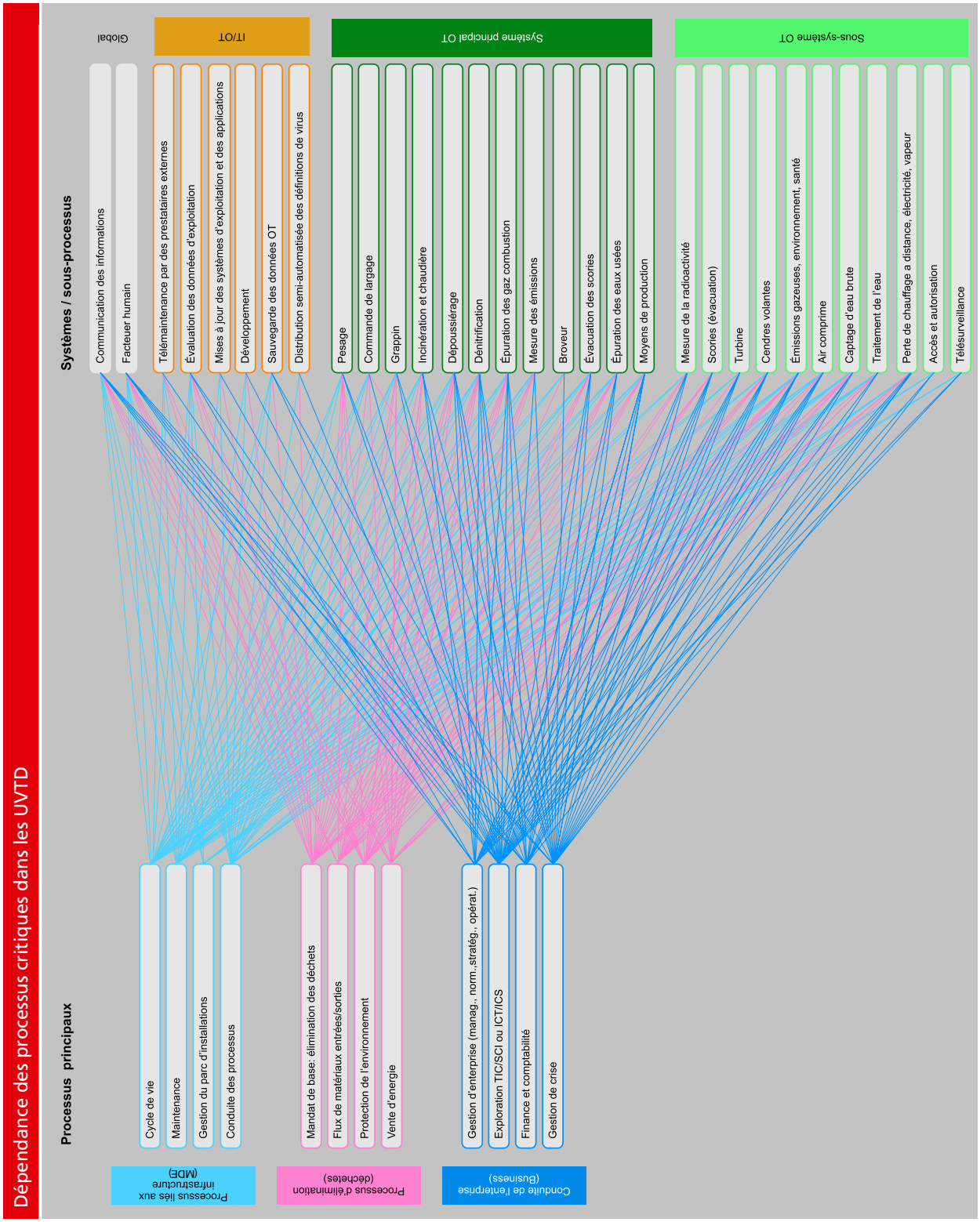


Figure 9 : Dépendance des processus critiques dans les UVTD

Dépendance sur le plan IT/OT des processus critiques dans les UVTD															
Rubrique	Systèmes/sous-processus	Processus clés													
		Infrastructures				Élimination (déchets)				Conduite de l'entreprise (business)					
		Cycle de vie	Maintenance	Gestion du parc d'installations	Conduite des processus (PLS)	Mandat de base : élimination des déchets	Flux de matériaux entrées/sorties	Protection de l'environnement	Fourniture d'énergie	Gestion d'entreprise (management, normative, stratégique, opérationnelle)	Exploitation informatique, SCI	Finances et comptabilité	Gestion de crise
Global	Communication des informations	x	x	x	x	x	x	x	x	x	x	x	x
	Facteur humain	x	x	x	x	x	x	x	x	x	x	x	x
Exploitation IT	Télémaintenance par des prestataires externes	x	x		x	x		x			x		
	Données d'exploitation	x	x	x	x	x	x	x	x	x		x	
	MàJ des systèmes d'exploitation et des applications		x		x	x					x		
	Développement		x		x	x					x		
	Sauvegarde de données TO	x	x		x	x					x		x
	Envoi semi-automatique de définitions de virus				x	x					x		
Système principal OT	Pesage/contrôle à la réception	x	x		x	x	x	x			x	x	
	Commande de largage	x	x		x	x	x		x		x		
	Grappin	x	x		x	x	x		x		x		x
	Incinération, y compris chaudière	x	x		x	x		x	x	x	x		x
	Dépoussiérage	x	x		x	x	x	x	x	x	x	x	x
	Dénitrification	x	x		x	x	x	x	x	x	x	x	x
	Épuration des fumées	x	x		x	x	x	x	x	x	x	x	x
	Mesure des émissions	x	x		x	x	x	x			x		x
	Broyeur	x	x				x						x
	Extraction des scories	x	x		x	x	x	x		x	x	x	x
	Épuration des eaux usées	x	x		x	x	x	x		x	x	x	x
	Moyens de production	x	x		x	x	x	x		x	x	x	x
Sous-système OT	Mesure de la radioactivité	x	x		x		x	x		x	x		x
	Scories (évacuation)					x	x	x		x	x	x	x
	Turbine	x	x		x			x		x	x	x	x
	Cendres volantes	x	x		x	x	x	x		x	x	x	x
	Émissions gazeuses, environnement, santé	x	x	x	x	x	x	x		x	x	x	x
	Perte de chauffage à distance, électricité, vapeur			x	x	x	x		x	x	x	x	x
	Air comprimé	x	x	x	x	x			x		x		x
	Captage d'eau brute	x	x	x	x	x	x	x	x	x	x		x
	Traitement de l'eau	x	x	x	x	x			x		x		x
	Accès et autorisation	x	x							x	x		x
	Vidéosurveillance	x	x							x	x		

Tableau 4 : Dépendance des processus critiques dans les UVTD

Le tableau ci-après décrit les attaques possibles contre les processus et leurs conséquences.

Processus	Attaque possible	Conséquence
Pesage	Blocage	Arrêt de l'exploitation faute de pouvoir réceptionner des déchets. Afin de poursuivre l'exploitation, une saisie manuelle du type de déchets, du client et du poids est-elle possible ?
Commande de largage	Blocage	Arrêt de l'exploitation faute de pouvoir réceptionner des déchets.
Broyeur	Blocage	Baisse de l'efficacité, une partie des déchets (encombrants) ne pouvant plus être valorisée.
Grappin	Blocage ou manipulation	Arrêt de l'exploitation, l'incinérateur ne pouvant plus être alimenté.
Incinération et chaudière	Manipulation du régulateur de combustion (système FLR), alimentation en eau de la chaudière	Arrêt de l'exploitation, l'incinération n'étant plus possible ; mauvaise combustion, donc plus de mise en décharge possible. Risque de dommages irréversibles à la chaudière dus à une surchauffe des murs et des tubulures et à la rouille.
Extraction des scories	Perturbations dans l'épandage et le traitement	Arrêt de l'exploitation lorsqu'il n'est plus possible d'épandre les scories ou d'extraire les matières non brûlées.
Séparation des poussières	Blocage	Émission de poussières ou de cendres volantes entraînant un dysfonctionnement complet du catalyseur en aval.
Dénitrification	Blocage Injection d'ammoniac ou régulation de la température du catalyseur (brûleur/vapeur)	Non-respect de l'ordonnance sur la protection de l'air (OPair), ayant pour conséquence un arrêt de l'installation. Panne totale de l'installation dès lors que la manipulation de processus en amont rend le catalyseur inutilisable. Contournement du catalyseur autorisé uniquement durant une brève période.
Épuration des fumées	Manipulation ou blocage de l'épurateur	Destruction de l'épurateur de fumée par surchauffe entraînant un arrêt de la ligne d'incinération.
Disponibilité des moyens de production (air comprimé, eau de refroidissement, produits chimiques)	Manipulation ou blocage de divers sous-systèmes intervenant dans les processus	Mise en position de sécurité des soupapes de régulation faute d'air comprimé, etc. Arrêt des lignes d'incinération.

Tableau 5 : Processus – Attaques possibles – Conséquences

Le tableau ci-après décrit les attaques possibles contre les produits ou dérivés, et leurs conséquences.

Produits et dérivés	Attaque possible	Conséquence
Cendres, scories, gâteaux de filtration	Perturbation du processus d'élimination	Accumulation de stocks non souhaités sur le site ; les contrats de livraison conclus avec les décharges ne peuvent pas être remplis (p. ex. décharges à ciel ouvert ou souterraines pour cendres volantes).
Eaux usées	Perturbation du processus	Pollution de l'eau, arrêt de tous les processus en amont et, partant, de toute l'installation. Perte de la licence d'exploitation.
Électricité et chaleur	• Manipulation du découplage thermique • Manipulation de la turbine	• Déstabilisation du réseau de chauffage à distance. • Menace sur les infrastructures critiques telles que les hôpitaux ou les bâtiments des administrations publiques. • Destruction mécanique par surrégime, avec pour conséquence une paralysie totale du site.
Émissions gazeuses	Pas de mesure ou mesure erronée	Risque de perte de la licence d'exploitation, dégâts d'image. Responsabilité engagée en cas d'émissions indésirables nocives pour la santé.

Tableau 6 : Produits et dérivés, attaques possibles et conséquences

Le plus grand risque, pour la plupart des processus, est celui d'un blocage ou d'une manipulation. Chaque incident entraîne des pertes d'exploitation et donc des coûts élevés, voire très élevés.

6 Protection de l'information

6.1 Protection de l'information

La protection de l'information vise à sécuriser de manière adéquate les informations et l'infrastructure IT, dans le respect des objectifs définis que sont la confidentialité, l'intégrité et la disponibilité. Il s'agit d'empêcher l'accès non autorisé aux différents systèmes ou la manipulation de données, et de minimiser autant que faire se peut les risques concomitants afin d'éviter les dommages économiques qui pourraient en résulter.

Que les données soient ou non à caractère personnel n'a ici aucune incidence. Les informations peuvent exister sous forme papier ou électronique.

« Protection de l'information », « protection des données » et « sécurité IT » sont des termes souvent pris pour synonymes ou utilisés dans un contexte inapproprié.

Comme le montre le graphique ci-dessous, la protection des données et la sécurité informatique sont des composantes de la protection de l'information, laquelle est elle-même un maillon essentiel de la gestion des risques d'entreprise et de la gestion de la continuité d'activité (*Business Continuity Managements,* BCM).

6.2 Stratégie de protection de l'information

Pour être efficace, une stratégie de protection de l'information doit cibler la protection des équipements et des services indispensables à l'exécution des processus opérationnels (critiques). Il n'existe pas, en ce domaine, de définition formelle des exigences ou des solutions.

Pour parvenir à une identification et une gestion globale des risques pesant sur les systèmes d'information et de communication critiques, il est indispensable de définir une stratégie de protection de l'information multicouche conforme au principe de défense en profondeur[1].

Outre des **mesures techniques,** cette stratégie devrait englober, les **processus** nécessaires, la formation des collaborateurs ainsi que la **gouvernance de la sécurité** requise pour mettre en œuvre la sécurité de l'information de manière durable et efficace.

[1] *Voir chapitre 3 Objectifs de la norme minimale*

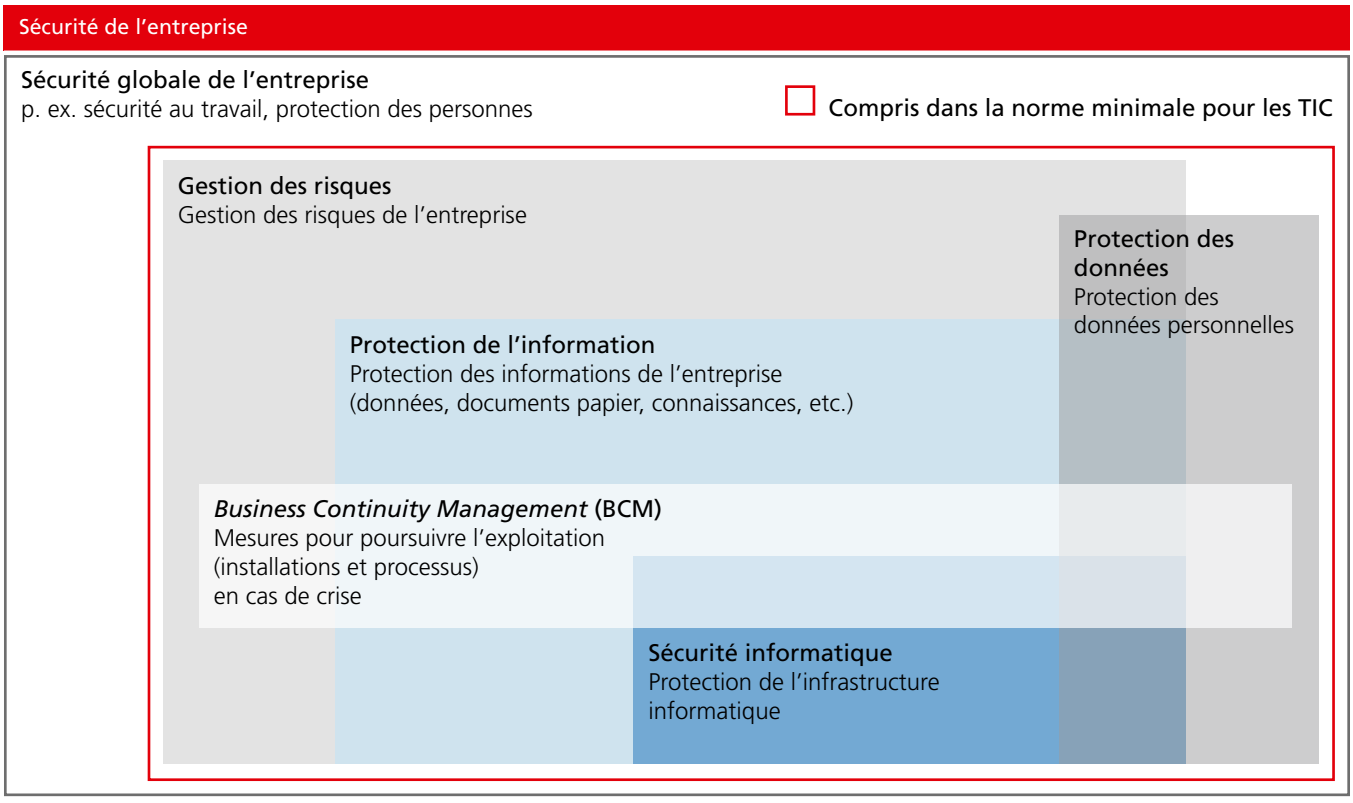


Figure : 10 Sécurité de l'entreprise

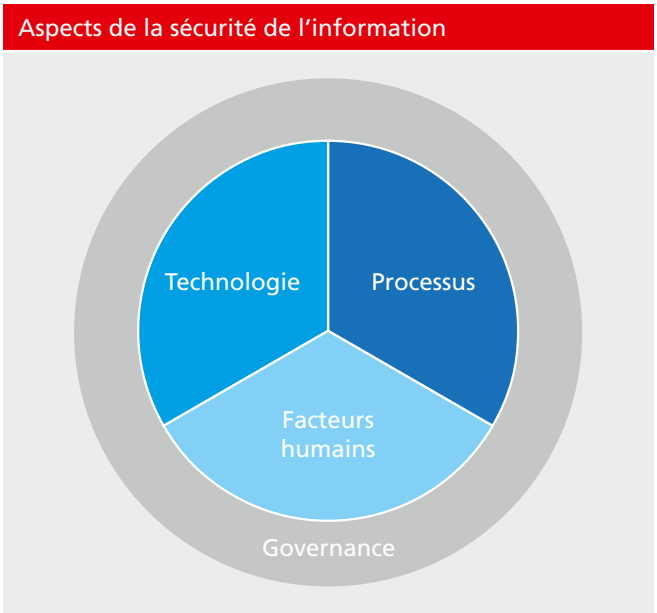


Figure 11 : Aspects de la sécurité de l'information

Chaque stratégie de défense en profondeur est individuelle ; elle doit refléter les besoins, les opportunités et les risques liés à l'organisation. L'approche basée sur les risques tient ici compte non seulement des dépendances internes, mais aussi des dépendances vis-à-vis des processus ou des ressources externes.

La stratégie de défense en profondeur part du principe qu'il ne peut y avoir de protection totale contre toutes les formes de *cyber*menace. Il importe donc d'être conscient de ses points faibles et d'élaborer des stratégies et des mesures visant à identifier l'exposition aux risques liés à la protection de l'information (*IDENTIFY*), à se protéger au mieux (*PROTECT*), à détecter les brèches en matière de *cyber*sécurité (*DETECT*) et à réagir (*RESPOND*) pour revenir au plus vite à une situation normale (*RECOVER*).

IMPORTANT : La sécurité de l'information ne se conçoit pas comme un projet ponctuel, mais constitue un processus d'assurance qualité continu fonctionnant selon le cycle PDCA (*Plan-Do-Check-Act* ou méthode de gestion de la qualité).

6.3 Mesures destinées à renforcer la protection de l'information

Données	Mesure
Courriel	Ne pas envoyer d'informations classifiées ni de mots de passe par courriel.
Classification des données	Classification correcte des données.
Droits d'accès aux données	Gestion correcte des autorisations.
Emplacement de sauvegarde des données	Sauvegarde des données classifiées uniquement sur des supports sécurisés.
Échange de données avec les fournisseurs	Plateforme d'échange sécurisée, ne partager que les données pertinentes.
Copie de secours	Contrôle régulier des données sauvegardées, supports de données délocalisés ou hors ligne.
Données dans le *cloud*	Assurer la disponibilité hors ligne des données importantes au cas où la connexion avec le *cloud* ne serait pas possible.
Procédures d'urgence	Devraient être disponibles sous forme papier.
Données dans les médias sociaux	Ne publier que le strict nécessaire pour éviter qu'on puisse remonter à la source.
Mots de passe	Miser sur la complexité, cf. politique en matière de mots de passe. La meilleure pratique est l'authentification multifacteur (AMF). Cf. Centre national pour la *cyber*sécurité (NCSC) : Protéger vos comptes (admin.ch)

Tableau 7 : Mesures de mise en œuvre de la sécurité de l'information (non exhaustives)

6.4 Protection des données

La protection des données englobe la protection des données personnelles[2], notamment des données sensibles[3], et la protection du droit à l'autodétermination de chaque individu quant aux informations le concernant. Elle prévoit des mesures organisationnelles et techniques contre le traitement et l'utilisation abusifs de données à caractère personnel.

En Suisse, la protection des données est régie par la loi fédérale sur la protection des données (LPD) et l'ordonnance relative à la loi fédérale sur la protection des données (OLPD). Toutefois, dès lors que l'on traite des données de ressortissants de l'espace européen (clients, collaborateurs), il se peut que les prescriptions du Règlement général sur la protection des données (RGPD) de l'UE doivent également être prises en considération dans notre pays.

Si la protection des données occupe une place toujours plus importante depuis l'avènement de la numérisation, c'est parce les tâches relatives à la conservation, au traitement, à la saisie, à la transmission et à l'analyse des données ne cessent d'être optimisées et simplifiées. Les innovations numériques telles que l'internet, la messagerie électronique, la téléphonie mobile, la vidéosurveillance ou les moyens de paiement électronique élargissent constamment et considérablement les possibilités de collecte de données personnelles.

Les principes suivants régissent notamment l'enregistrement et le traitement de données personnelles :

- Tout traitement de données personnelles doit être licite et
- effectué conformément aux principes de la bonne foi et de la proportionnalité.

Les données personnelles ne doivent être traitées que dans le but indiqué lors de leur collecte, prévu par une loi ou ressortant des circonstances.

6.5 Sécurité IT

En tant que sous-domaine de la protection de l'information, la sécurité IT s'attache à protéger les informations enregistrées sous forme électronique (données), à assurer leur traitement ainsi qu'à réaliser les objectifs de confidentialité, d'intégrité et de disponibilité. Elle veille également au fonctionnement sans heurt et sans interruption ainsi qu'à la fiabilité des systèmes TIC.

Il importe également de prendre en considération les systèmes qui ne sont pas toujours directement assimilés aux systèmes TIC, tels que les installations téléphoniques, les systèmes de commande (SCI) ou les objets connectés.

Lorsque l'on utilise des systèmes *cloud*, le champ d'action de la sécurité IT traditionnelle s'étend au-delà du périmètre de l'entreprise (*cyber*espace).

La propension des fournisseurs à collecter et à évaluer des données s'est fortement accrue, leur but étant, d'une part, d'améliorer leurs produits et, d'autre part, de connaître et de suivre l'utilisation qui en est faite. La communication de telles données requiert au préalable un examen minutieux, une clarification précise et un règlement par contrat. Il convient également de convenir des connexions sécurisées utilisées et de la périodicité de transmission des données aux fournisseurs (en temps réel, chaque jour, chaque semaine, etc.).

[2] Définition selon l'art. 3, al. a, LPD
[3] Définition selon l'art. 3, al. c, LPD

6.6 Prise de conscience des collaborateurs (*awareness*)

L'expérience des dernières années a montré que la technologie en matière de sécurité ne permet pas, à elle seule, de lutter efficacement contre les attaques de plus en plus sophistiquées et les menaces croissantes issues du *cyber*espace.

C'est pourquoi il s'agirait de soumettre régulièrement l'ensemble des collaborateurs à une formation sur la sécurité de l'information et de renforcer ainsi leur perception de la sécurité.

En dispensant aux collaborateurs une formation qui tienne compte de leurs niveaux de compétence respectifs, on réduit considérablement le risque de comportements fautifs involontaires.

Les objectifs de la formation sont multiples :

- Inciter les collaborateurs à faire preuve de vigilance en matière de sécurité.
- Enseigner comment gérer les risques et les incidents.
- Promouvoir et renforcer la reconnaissance de la sécurité de l'information en tant que thématique.
- Donner les moyens aux collaborateurs de comprendre et de soutenir activement les mesures touchant à la sécurité.

Le but d'un programme de sensibilisation est de conférer aux collaborateurs une compétence inconsciente en matière de sécurité de l'information. L'idée est de les amener à adopter spontanément le bon comportement face à des situations délicates, sans qu'ils aient à se demander si la démarche est ou non la bonne. Pour cela, il est crucial de mettre en place, de manière continue, un programme de sensibilisation.

6.7 Gouvernance

La gouvernance désigne l'ensemble des principes et des règles permettant aux cadres supérieurs de piloter et de surveiller les structures et les comportements.

La gouvernance est cruciale pour une mise en œuvre efficace et durable de la stratégie de sécurité de l'information. C'est elle qui crée les conditions nécessaires à l'identification, à l'évaluation et au traitement des menaces pesant sur la sécurité de l'information dans l'entreprise. La gouvernance incarne une « métastructure » visant à soutenir cette dernière dans la réalisation de ses objectifs en matière de sécurité de l'information, aux plans stratégique, fonctionnel et opérationnel. La sécurité de l'information et sa mise en œuvre requièrent une définition préalable des principes informatiques par l'entreprise, laquelle doit notamment se poser les questions suivantes :

- Quelle action entreprendre ?
- Comment la mener à bien ?
- Qui en assume la responsabilité ?
- Comment l'action est-elle évaluée ?

Les principes de la sécurité informatique définissent les règles, les processus, les métriques logicielles et les structures organisationnelles nécessaires à une planification et un contrôle efficaces.

7 Thèmes clés

7.1 Zonage du réseau

7.1.1 Séparation physique

Séparer physiquement les segments de réseau est la méthode la plus fiable pour contrôler et délimiter le trafic entre plusieurs réseaux. Elle implique l'utilisation de nombreux dispositifs tels que des commutateurs, des routeurs et des passerelles de sécurité, et s'avère par conséquent très coûteuse. Il est donc recommandé d'opérer une séparation physique des segments de réseau aux points les plus sensibles du réseau principalement. Il peut s'agir :

- des connexions entre différents emplacements géographiques
- des connexions entre les zones sensibles du réseau, comme le système de commande et la bureautique d'un même emplacement géographique
- des périmètres, à savoir les passerelles entre le réseau de l'entreprise et les réseaux externes (internet, p. ex.)

7.1.2 Réseau local virtuel (*Virtual Local Area Network,* VLAN)

Si, à l'issue d'une évaluation des risques, la séparation physique des segments de réseau n'apparaît pas strictement nécessaire, on peut opérer une segmentation logique par VLAN. Il en résulte un risque résiduel plus élevé qu'en cas de séparation physique ; ce risque peut être dû à des erreurs de configuration ou des scénarios d'attaque tel que le saut de VLAN (*VLAN-hopping*) et doit alors être pris en compte.

7.2 Segmentation du réseau selon le modèle « Purdue »[4]

Le modèle de référence Purdue a été développé aux États-Unis au début des années 1990 par Theodore J. Williams de l'Université de Purdue, dans l'Indiana. Conçu à l'origine pour les réseaux non industriels, il a ensuite été adapté aux réseaux automatisés.

Le modèle de référence Purdue subdivise un réseau industriel, de manière abstraite, en différentes strates. Il peut ainsi servir de point de départ pour des mesures élaborées selon le principe de la défense en profondeur.

Le principe de subdivision d'un réseau de ce type en zones et conduits se retrouve dans le modèle de référence Purdue, sachant qu'il faut distinguer ici entre zone et niveau. Un niveau désigne la classification hiérarchique sur l'ensemble du réseau de l'entreprise, tandis qu'une zone caractérise la segmentation spécifique en fonction des exigences de sécurité. Une zone peut parfois couvrir plusieurs niveaux.

7.2.1 Segmentation horizontale du réseau

Ce modèle protège les processus d'automatisation critiques et sensibles contre les accès non autorisés depuis des segments de réseau non fiables. Le modèle de zones prévoit sept zones qui assument des fonctions déterminées et qui hébergent des systèmes subdivisés selon leurs besoins de protection. Les terminaux critiques sont ainsi rangés exclusivement dans les zones 1 et 2, et séparés des autres zones par des passerelles de sécurité adéquates.

7.2.2 Segmentation verticale du réseau

Le zonage vertical consiste à segmenter le réseau par sites géographiques ou par systèmes. Il est ainsi possible d'exploiter, sur un même niveau de réseau horizontal, plusieurs sites géographiques qui présentent des besoins de protection différents. Les canaux de communication et les interfaces nécessaires sont réalisés via les passerelles de sécurité mises à disposition. La communication interzone passe par des canaux de communication sécurisés, clairement définis et documentés.

En cas d'incident de sécurité, les dommages peuvent être circonscrits à la zone considérée et aux systèmes qui s'y trouvent. Les systèmes sont classés selon des critères prédéfinis, attribués à des zones horizontales et regroupés au sein de celles-ci.

Les critères de regroupement peuvent être la criticité, les risques, les technologies, les domaines de responsabilité organisationnels et les éléments physiques.

[4] *Source : www.sichere-industrie.de (en allemand uniquement), description des zones et du modèle.*

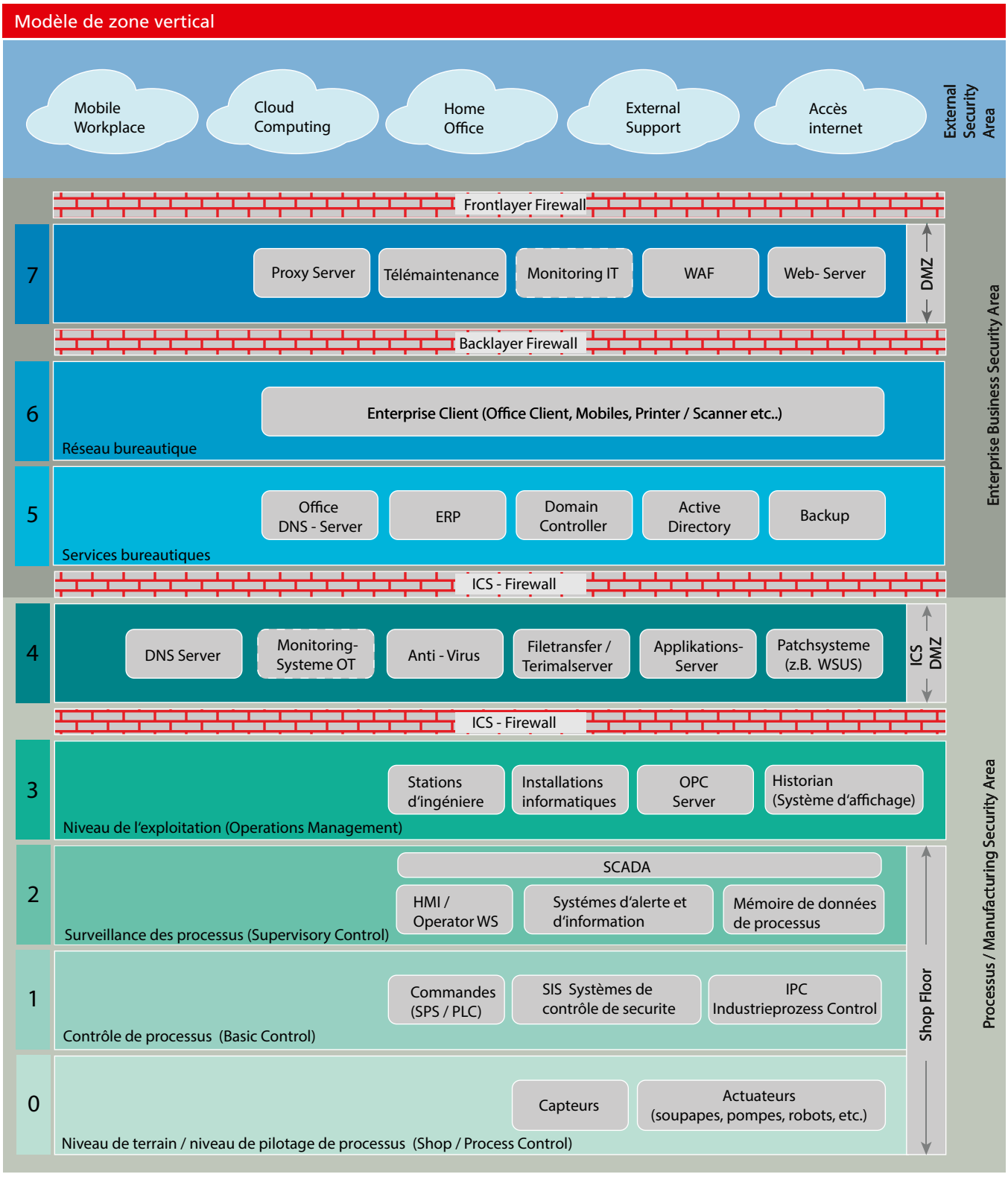


Figure 12 : Modèle de zone vertical

Modèle de zone horizontal

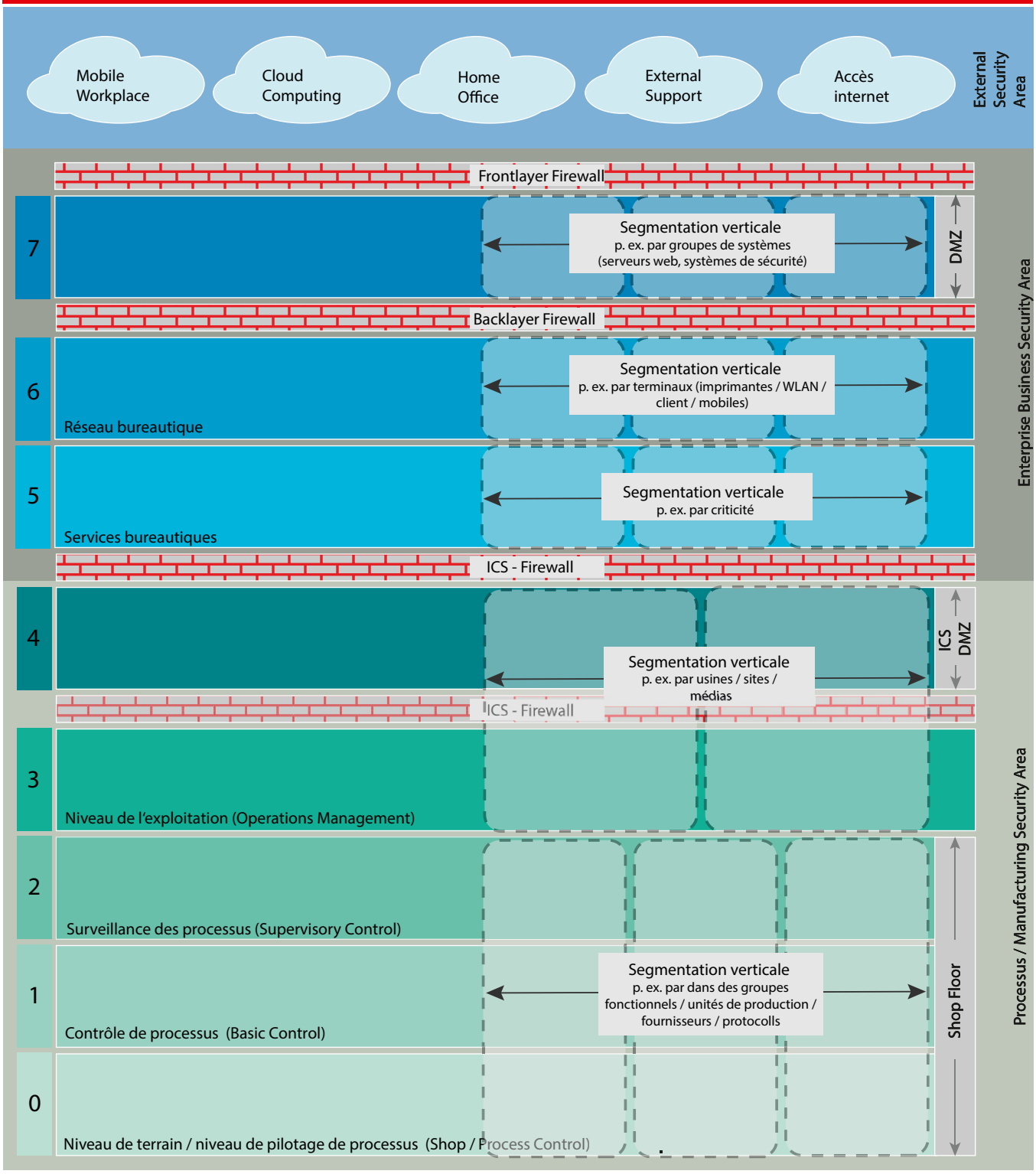


Figure 13 : Modèle de zone horizontal

Niveau de terrain/niveau de pilotage de processus (niveau 0)

C'est dans la couche la plus basse que se déploient, à proprement parler, les processus physiques de l'entreprise. Les ordres des systèmes de niveau 1 sont ici mis en œuvre en temps réel. Ce niveau est également appelé niveau des dispositifs *(device)* ou niveau de terrain.

Les systèmes concernés sont typiquement des moteurs, des soupapes, des pompes et des commandes à distance d'entrée/sortie (*Remote* I/O)

Contrôle de processus (niveau 1)

Ce niveau comprend les systèmes qui ont une incidence directe sur l'exécution et le pilotage des processus physiques. Parmi les tâches qui leur incombent, citons la surveillance des capteurs et le maintien du bon fonctionnement des installations. Ces systèmes travaillent en temps réel. Un dérangement à ce niveau impacte directement les processus automatisés.

Sont typiquement concernés : API / PLC, SCADA, DCS (systèmes numériques de contrôle-commande), RTU (unités de terminal à distance)

Surveillance de processus (niveau 2)

Les systèmes du niveau 2 concernent la surveillance et le pilotage des processus spécifiques. Le traitement des données n'intervient pas encore en temps réel ; un dérangement des systèmes résidents n'a pas d'impact direct sur la disponibilité de la solution d'automatisation.

Les systèmes concernés sont typiquement les interfaces homme-machine (IHM), les systèmes d'alerte et de notification et les mémoires de données de processus

Niveau de l'exploitation (niveau 3)

Figurent au niveau 3 les systèmes qui servent principalement à l'exploitation. Cette couche concerne, d'une part, la mise à disposition des systèmes, services et applications nécessaires au réseau industriel, et, d'autre part, la planification des différentes étapes d'automatisation.

Les systèmes concernés sont typiquement les services et protocoles informatiques (DNS, DHCP, *Active Directory,* etc.), les stations d'ingénierie et les logiciels de pilotage de la production

SCI DMZ (niveau 4)

La DMZ ou zone démilitarisée est un sous-réseau dans lequel on trouve des connexions provenant idéalement de segments qui requièrent un besoin de protection accru. Typiquement, une DMZ est placée entre le réseau bureautique et l'internet, emplacement où l'on trouve par exemple des systèmes comme les serveurs web, qui doivent être accessibles depuis l'internet. Dans le contexte qui nous intéresse, la zone démilitarisée est exploitée entre la zone bureautique et la zone d'installation, pour y placer, par exemple, des ressources partagées.

Les systèmes concernés sont typiquement des antivirus, des dispositifs de télémaintenance, des serveurs d'échange de fichiers et des systèmes de déploiement des mises à jour et correctifs informatiques

Services bureautiques / réseau bureautique (niveaux 5 et 6)

Il s'agit ici de systèmes destinés à soutenir l'activité de l'entreprise, dont ceux utilisés par les services de comptabilité, de distribution et de gestion du personnel. L'interface avec le réseau d'installations se situe entre le niveau 4 et le niveau 3. Du point de vue du réseau d'installations, le réseau de l'entreprise est jugé très peu sûr.

Il s'agit typiquement des systèmes ERP, de l'accès à internet, des accès de télémaintenance et des terminaux de travail.

DMZ (niveau 7)

Cette couche de réseau est une sorte de « zone tampon » assurant l'intégration entre le réseau IT de l'entreprise et l'internet ou d'autres réseaux externes.

Trafic de données entre les zones

En principe, toutes les zones sont isolées les unes des autres et aucune communication interzone n'est possible. Toutefois, lorsqu'une communication doit avoir lieu, la source, la destination et le port IP doivent être définis, documentés et ouverts via une passerelle de sécurité. Ces exceptions doivent être réévaluées périodiquement.

Réseaux sans fil

Les réseaux sans fil permettent d'accéder facilement, sans câble, au réseau des entreprises. C'est pourquoi il convient d'accorder une attention particulière à la protection des réseaux sans fil.

En outre, de nombreux systèmes proposent d'établir des connexions par bluetooth, infrarouge ou *Near Field Connection* (NFC). Ces connexions sont généralement mal protégées et peuvent être utilisées comme vecteurs d'attaque.

Il est donc recommandé d'abandonner totalement ces modes de connexion. Des mesures de protection spéciales doivent être déployées concernant les systèmes pour lesquels le *bluetooth*, l'infrarouge ou le NFC ne peuvent pas être désactivés.

Exemple de mesure :

Selon l'emplacement de l'émetteur, le *bluetooth* peut rayonner au-delà de l'enveloppe du bâtiment et donc être capté dans un périmètre allant jusqu'à 100 m dans l'espace public. Des mesures constructives appropriées peuvent empêcher cela. Le *bluetooth* émet sur la bande de 2,4 GHz, et donc avec une longueur d'ondes d'environ 12 cm. Une grille métallique mise à la terre avec un maillage inférieur à 12 cm entre l'émetteur et l'enveloppe du bâtiment empêche efficacement le rayonnement vers l'extérieur.

7.2.3 Téléphones mobiles/tablettes[5]

Aujourd'hui, les smartphones et les tablettes sont de plus en plus utilisés dans l'environnement professionnel, au point de devenir le principal outil de travail de bon nombre de collaborateurs. Actuellement, un nombre considérable d'appareils fonctionnent avec des systèmes d'exploitation différents. Modernes et simples d'utilisation, les smartphones et les tablettes sous iOS ou Android sont plutôt destinés au grand public, moins à un usage professionnel qui nécessite un niveau de protection élevé.

Ils se différencient donc fondamentalement d'autres concepts de terminaux mobiles dédiés spécifiquement au monde de l'entreprise. Les appareils tournant sous iOS ou Android sont toutefois de plus en plus utilisés pour le travail, au point de supplanter des solutions établies telles que les ordinateurs portables.

La manière dont il convient d'utiliser et d'administrer les terminaux mobiles doit être évaluée en fonction du besoin de protection. Si celui-ci est faible à normal, l'utilisation des programmes natifs suffit. Pour un besoin de protection accru voire élevé, il s'agit d'utiliser une solution MDM *(Mobile Device Management),* associée éventuellement à un programme d'inscription des appareils (*Device Enrollment Program,* DEP). Lorsque le besoin de protection est élevé, il est recommandé d'utilisé un conteneur sécurisé, seul moyen d'éviter au maximum l'interaction entre une utilisation professionnelle et une utilisation privée du terminal mobile, et de stocker de manière sécurisée les données de l'entreprise.

Avant d'intégrer des terminaux mobiles dans une structure d'entreprise, il est recommandé de définir des règles d'intégration claires. Ces directives de sécurité fixent entre autres les conditions générales régissant le choix des appareils, la sélection des données pouvant être traitées sur les appareils, les restrictions imposées aux utilisateurs et le bridage des possibilités offertes par les appareils (sur les plans matériel et logiciel).

Un risque résiduel demeure, même en optant pour des paramètres sécurisés sur les terminaux mobiles, mesure qui a pourtant pour effet de restreindre grandement la liberté d'action des utilisateurs et les possibilités offertes par les applications. Ce risque tient essentiellement au fait que les appareils sont utilisés en dehors d'un environnement sécurisé, souvent dans une situation où l'on n'utiliserait pas un ordinateur portable. La perte potentielle d'appareils (et donc des données qu'ils contiennent) est un danger qui ne peut jamais être totalement écarté. On ne peut qu'espérer, en l'espèce, que les mécanismes mis en place pour protéger les données seront encore efficaces et que les mesures prises a posteriori (effacement à distance p. ex.) fonctionneront.

La présence de risques résiduels difficiles à appréhender ne peut être écartée, même en cas de recours à un container sécurisé. Citons par exemple l'utilisation non autorisée du microphone de l'appareil à des fins d'écoute clandestine.

De plus amples informations sur les mesures de protection des appareils mobiles figurent dans le document « *Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit* » du *Bundesamt für Sicherheit in der Informationstechnik* BSI (en allemand uniquement).

7.3 Services en *cloud*

Le terme de *cloud* est la forme abrégée *cloud computing.* Un *cloud* est constitué de plusieurs serveurs distants, auxquels il est possible d'accéder en tout temps, depuis n'importe quel endroit, via une connexion internet sécurisée et protégée.

Cloud privé

Lorsqu'une entreprise utilise ses propres serveurs pour le *cloud* computing, on parle alors de *cloud* privé. Les utilisateurs accèdent de facto aux serveurs de l'entreprise. Les données et les services qui y sont stockés ne sont pas disponibles pour le grand public. Ainsi, les données critiques sur le plan de la sécurité restent dans l'entreprise. Toutefois, l'utilisation d'un *cloud* privé est synonyme de fortes sollicitations pour l'administration de systèmes et s'avère chronophage et coûteuse.

Cloud public

Un *cloud* public propose ses services à plusieurs utilisateurs en même temps via l'internet (infrastructure partagée). La surveillance, la maintenance et l'adaptation continue du système aux besoins des utilisateurs sont assurées par le fournisseur. L'entreprise n'a donc pas à supporter les coûts de création, de maintenance et de mise à jour continue d'une architecture serveur interne.

[5] Source : Publication de l'Office fédéral allemand de la sécurité des technologies de l'information (BSI) relative à la cybersécurité | iOS, en allemand uniquement (https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_074.pdf ?_blob=publicationFile&v=1)

Cloud hybride

La combinaison des deux solutions (*cloud* privé et *cloud* public) est appelée *cloud* hybride. Les données sensibles sont stockées dans l'entreprise, tandis que d'autres données de travail sont accessibles, sous forme sécurisée, via une infrastructure partagée.

Exemples d'application des services en *cloud* :

- évaluation des données d'exploitation (processus OT)
- applications de communication et de *workflow*
- protection des points d'accès
- passerelle et service de messagerie
- systèmes téléphoniques
- bureautique
- systèmes d'alerte (SMS, courriel, *workflow*)

Modèles de service en *cloud*

Les modèles de service disponibles en *cloud* sont les suivants :
- IaaS (*Infrastructure as a Service*)
- PaaS (*Platform as a Service*)
- SaaS (*Software as a Service*)
- DaaS (*Desktop as a Service*).

Architecture de sécurité du *cloud*

Chaque modèle de service *cloud* possède sa propre architecture de sécurité, gérée par le fournisseur de services *cloud* et par le client. Les architectures de sécurité pour les services *cloud* diffèrent selon que le *cloud* proposé est public, privé ou hybride.

Selon la criticité des informations traitées, une application *cloud* (*cloud* privé) doit aussi être rangée dans la catégorie de protection correspondante et protégée par des mesures appropriées.

Responsabilités en matière de sécurité *cloud*

Ces responsabilités sont fonction du modèle de service et de déploiement. En principe, la sécurité *cloud* donne toutefois lieu à un partage de responsabilité jusqu'à un certain point.

Dans le cadre d'une solution IaaS de services *cloud* de type « public », par exemple, le fournisseur gère les interfaces réseau physiques, les hyperviseurs et le stockage des données, tandis que le client se charge des systèmes d'exploitation, des applications et des données correspondantes.

Dans cette architecture, le fournisseur de services *cloud* surveille la sécurité « externe » du *cloud*, c'est-à-dire le matériel et les logiciels essentiels, par exemple les bases de données et la capacité de traitement d'un centre de calcul, tandis que le client se concentre sur la sécurité « interne », à savoir comment les demandes d'accès sont accordées ou refusées, comment les pare-feu de l'entreprise sont configurés et comment d'autres activités sont gérées lors de l'utilisation d'un service *cloud*.

Un fournisseur de services qui déploie des modèles PaaS, SaaS et DaaS dans le cadre d'un *cloud* public assume davantage de responsabilités en matière de sécurité que dans le cadre du modèle IaaS. Un client qui opte pour le modèle SaaS est notamment déchargé de la gestion des serveurs, des bases de données et des mécanismes de sécurité sous-jacents (cryptage de bout en bout p. ex.). Cet arrangement ne signifie toutefois pas que les SaaS sont sans risque, car le client doit soumettre le fournisseur de services *cloud* à un examen minutieux et s'assurer que l'accès aux applications est suffisamment sécurisé.

Les *clouds* privés et les *clouds* hybrides qu'une organisation utilise pour gérer des ressources réservées à un usage exclusif, exigent généralement davantage de responsabilités de la part du client en ce qui concerne le stockage sécurisé des données. La gestion des données dans des *clouds* privés ou hybrides présente certains avantages, car ces données sont moins dépendantes d'une infrastructure partagée que les données situées dans un *cloud* public. La charge directe en matière de sécurité qu'elle représente pour le client peut toutefois être plus importante.

Accord de niveau de service

Un accord de niveau de service (SLA) pour le *cloud computing* est un accord conclu entre un fournisseur de *services cloud* et un client dans le but d'assurer le maintien d'un niveau minimum de service. Il garantit un certain degré de fiabilité, de disponibilité et de réactivité des systèmes et des applications, fixe les responsabilités en cas d'interruption de service et décrit les sanctions prévues en cas de non-respect du niveau de service.

Le rôle d'un SLA est en fin de compte le même que celui d'un contrat : un document régissant les relations client-fournisseur. Ces règles convenues constituent le socle de la collaboration.

Le niveau de service défini dans le SLA doit être spécifique et mesurable, afin de permettre une analyse comparative et, si l'accord le prévoit, d'appliquer des primes ou des pénalités appropriées.

8 Conclusion

La sécurité de l'information n'est pas une fin en soi. Les mesures de protection contre les *cyber*attaques visent toutes la sécurité de l'exploitation et la fiabilité du système dans son ensemble. Les UVTD revêtent une importance systémique pour la réalisation de leur mission première d'élimination des déchets et de leur mission secondaire d'approvisionnement en énergie de l'industrie et des ménages. La *cyber*sécurité et la *cyber*résilience font donc partie intégrante de la gestion globale des risques et constituent une thématique clé pour les décideurs.

La sécurité de l'information n'est toutefois pas uniquement l'affaire des dirigeants de l'entreprise : il est essentiel de sensibiliser l'ensemble des collaborateurs aux scénarios d'attaque toujours plus ingénieux.

La présente norme TIC poursuit un double objectif : aider les utilisateurs à dresser un état des lieux de leur environnement informatique et leur permettre de déterminer le degré de maturité de la sécurité de l'information :

- des directives ont-elles été élaborées, des processus ont-ils été définis ?
- des mesures sont-elles mises en œuvre de manière partielle ou globale ?
- si oui, sont-elles soumises à des évaluations régulières ?
- Un processus d'amélioration continue est-il mis en place ?

Des *cyber*attaques réussies peuvent considérablement perturber l'activité, et même entraîner l'arrêt des installations, ce qui a un impact économique et occasionne des dégâts d'image. Quand elles sont dirigées contre des PME du secteur privé, la survie même des entreprises peut être en jeu. Le but des prescriptions énoncées dans la présente norme (bonnes pratiques) et d'un processus d'amélioration continu est de renforcer la fiabilité de l'exploitation.

Outre le présent manuel, l'AEP propose aux entreprises actives dans la gestion des déchets un outil d'évaluation au format Excel, qui reprend les recommandations de la norme minimale TIC[6]. Cet outil est particulièrement utile pour évaluer le degré de maturité d'une entreprise ou d'un organisme. Il s'appuie sur la norme minimale pour les TIC, qui décrit la marche à suivre et apporte des éléments de réponses.

Ce manuel n'est pas une directive contraignante, son objectif étant d'inciter les acteurs du domaine de l'élimination des déchets à réfléchir aux enjeux de la *cyber*sécurité. La sécurité de l'information n'est pas un état, mais un processus. Le but de ce manuel de *cyber*sécurité est de soutenir ce processus et de faciliter sa mise en œuvre.

[6] *Lien vers l'outil Excel : Norme minimale pour les TIC (admin.ch)*

9 Principes, documents et normes

Le présent manuel tient compte de concepts, recommandations et mesures qui reposent sur diverses normes et autres documents normatifs (tableaux ci-après).

Titre	Année	Éditeur(s) et description
Mesures de protection des systèmes de contrôle industriels (SCI)	2018	Éd. : **Centre national pour la *cyber*sécurité (NCSC)** Basées sur des documents du Département américain de la sécurité intérieure (DHS), de l'Industrial *Control Systems Cyber Emergency Response Team* (ICS-CERT) et du *National Institute of Standards and Technology* (NIST), ces instructions décrivent en huit pages, de façon succincte et pragmatique, les onze mesures principales à mettre en œuvre par les exploitants de systèmes SCADA.
Analyse des risques et des vulnérabilités du sous-secteur	2015/ 2017	Éd. : **Office fédéral pour l'approvisionnement économique du pays (OFAE)** L'analyse des risques et des vulnérabilités repose sur la stratégie nationale de protection de la Suisse contre les *cyber*risques (SNPC) et sur la stratégie nationale pour la protection des infrastructures critiques (PIC). Elle a pour but d'examiner la vulnérabilité aux pannes et aux perturbations informatiques.
Guide pour la protection des infrastructures critiques (guide PIC)	2018	Éd. : **Office fédéral de la protection de la population (OFPP)** Le guide PIC constitue un instrument d'analyse et, le cas échéant, d'amélioration de la résilience des infrastructures critiques. Il est notamment conçu pour être utilisé dans des sous-secteurs critiques par les exploitants, les associations sectorielles et les autorités compétentes. Ce guide propose pour l'essentiel une procédure en matière de gestion des risques : analyse (identification des ressources, vulnérabilités, risques), évaluation, mesures (mise en œuvre, contrôle et amélioration). Il est tout à fait possible voire souhaitable d'intégrer cette procédure aux processus de gestion existants ou de baser sur eux son exécution.
Stratégie nationale pour la protection des infrastructures critiques (PIC)	2018	Éd. : **Office fédéral de la protection de la population (OFPP)** La stratégie nationale PIC définit le champ d'application, désigne les infrastructures critiques et fixe les principes directeurs de la PIC. Elle s'adresse à tous les services assumant des responsabilités dans ce domaine, en particulier aux différentes autorités compétentes, aux responsables politiques et aux exploitants d'infrastructures critiques.
Stratégie nationale de protection de la Suisse contre les *cyber*risques (SNPC)	2018	Éd. : **Unité de pilotage informatique de la Confédération (UPIC)** Vu l'intérêt majeur que revêt la protection des infrastructures informatiques contre les *cyber*risques pour la Suisse, le Conseil fédéral a chargé l'UPIC d'élaborer une stratégie nationale visant à protéger notre pays contre de tels risques. La SNPC a pour but de dresser un panorama actuel des *cyber*risques et d'indiquer les moyens dont dispose la Suisse pour y faire face, où se situent les lacunes et comment y remédier le plus efficacement possible. La SNPC identifie les structures existantes et définit des objectifs assortis de mesures ad hoc (analyses des risques et des vulnérabilités d'un sous-secteur, p. ex.).

Tableau 8 : Bases et documents

Titre	Année	Éditeur(s) et description
Loi fédérale sur l'approvisionnement économique du pays (loi sur l'approvisionnement du pays, LAP)	État 2016	Éd. : **Assemblée fédérale de la Confédération suisse** La LAP régit les mesures visant à garantir l'approvisionnement du pays en biens et services vitaux lors d'une pénurie grave à laquelle les milieux économiques ne peuvent pas faire face par leurs propres moyens. La Confédération peut encourager, dans les limites des crédits autorisés, des mesures prises par des entreprises de droit privé ou public pour garantir l'approvisionnement économique du pays si ces mesures contribuent à renforcer substantiellement les préparatifs nécessaires pour garantir les systèmes d'approvisionnement et infrastructures vitaux en cas de pénurie grave. Le présent manuel constitue l'une de ces mesures.

Tableau 8 : Bases et documents

Le tableau ci-après répertorie une série de normes internationales prises en considération dans le présent manuel.

Titre	Éditeur(s) et description
ISO 27001 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences	Éd. : **Organisation internationale de normalisation (ISO)** Cette norme détaille les exigences relatives à un système de gestion de la sécurité de l'information (SGSI). Les normes ISO 27000 ss. constituent une série de *normes concernant la sécurité de l'information,* dont les suivantes présentent un intérêt ici :
ISO 27002 Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information	• 27000 Vue d'ensemble et vocabulaire ; • 27001 Exigences (principes de base avec contrôles et objectifs de contrôle en annexe) ; • 27002 Code de bonne pratique pour le management de la sécurité de l'information ; • 27003 Systèmes de management de la sécurité de l'information – Lignes directrices (pour la mise en œuvre) ; • 27005 Gestion des risques liés à la sécurité de l'information • 27019 Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie. Largement appliquées à l'heure actuelle, les normes ISO 27000 ss. devraient s'imposer comme le principal cadre de référence dans les années à venir. Les observer déjà aujourd'hui constitue donc la bonne approche. Contrairement à d'autres normes ou cadres, elles ne sont pas trop détaillées, sont modulables et peuvent être continuellement améliorées et développées sur une longue période. Le SGSI et le contenu des mesures doivent être adaptés et mis en œuvre en tenant compte des spécificités du secteur.
ISO 22301 *Security and resilience – Business continuity management systems – Requirements*	Éd. : **Organisation internationale de normalisation (ISO)** Cette norme détaille les exigences relatives aux systèmes de gestion de la continuité d'activité.
ISO 31000 Management du risque	Éd. : **Organisation internationale de normalisation (ISO)** Cette norme définit des lignes directrices décrivant les modalités de gestion des risques au sein d'une organisation. L'application de ces lignes directrices peut être adaptée à l'environnement spécifique de chaque entreprise. La norme constitue une approche très générale, qui n'est pas spécifique à une industrie ou à un secteur et qui reste applicable à tout type de risque. Elle peut en outre être utilisée tout au long de la vie d'une entreprise et être implémentée à tous les niveaux de l'entreprise ainsi que dans le processus de prise de décision.
ISO27005 Gestion des risques liés à la sécurité de l'information	Éd. : **Organisation internationale de normalisation (ISO)/ Commission électrotechnique internationale (IEC)** Cette norme définit des lignes directrices pour une gestion des risques systématique et axée sur les processus qui, le cas échéant, soutient également la mise en conformité avec les exigences de gestion des risques prévues par la norme ISO/CEI 27001.

Tableau 9 : Normes nationales et internationales relatives à la sécurité informatique

Titre	Éditeur(s) et description
ISO 27019 Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie	Éd. : **Organisation internationale de normalisation (ISO)** Cette norme concerne les systèmes et les réseaux de contrôle, de régulation et de surveillance des processus servant à contrôler et surveiller la génération/production, le transport, le stockage et la distribution de l'électricité, du gaz, du pétrole et de la chaleur. Cela inclut les systèmes de commande et d'automatisation, les systèmes de protection et de sécurité ainsi que les systèmes de mesure, y compris les technologies de communication. La norme les englobe sous l'appellation de contrôle-commande des processus. Contrairement à la norme ISO/CEI 27002, l'accent est mis ici sur les infrastructures critiques nécessaires à une exploitation sûre et fiable, et dont il faut par conséquent tenir compte dans les processus de gestion (disponibilité et intégrité des données).
CEI 62264 ss. Intégration des systèmes entreprise-contrôle	Éd. : **Commission électrotechnique internationale (CEI)** Cette série compte quatre normes relatives à l'intégration des systèmes informatiques d'entreprise et de contrôle-commande.
CEI 62443 ss. Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes	Éd. : **Commission électrotechnique internationale (CEI)** Cette série compte treize normes de sécurité et spécifications techniques applicables aux systèmes d'automatisation de commande industriels (*industrial automation and control systems,* IACS). Les normes CEI 61508 ss. (principes fondamentaux régissant la sécurité des IACS), qui englobent le thème de la sécurité de l'information, couvrent de manière complète et indépendante la thématique des IACS. Quatre aspects ou niveaux de sécurité de l'information différents sont retenus : • les aspects généraux (concepts, terminologie, unités de mesure, etc.) : CEI 62443-1-x ; • la gestion de la sécurité informatique : CEI 62443-2-x ; • le niveau « système » : CEI 62443-3-x ; • le niveau « composants » : CEI 62443-4-x. À relever que cette série de normes couvre également l'architecture de réseau et l'architecture zonale, alors que d'autres normes ne le font pas, ou alors de manière moins détaillée. Cette série de normes est en train de devenir une prescription normative fondamentale dans le contexte des normes du CENELEC (EN 50126, entre autres) en matière de fiabilité, de disponibilité, de maintenabilité et de sécurité (FDMS).
BDEW Livre blanc *Anforderungen an sichere Steuerungs- und Telekommunikationssysteme*	Éd. : ***Bundesverband der Energie- und Wasserwirtschaft*** **(BDEW),** ***Österreichs E-Wirtschaft*** Le livre blanc de la BDEW pointe les mesures de sécurité fondamentales touchant aux systèmes de commande et de télécommunication de l'industrie de l'énergie. L'objectif stratégique de ce document est d'influencer favorablement le développement de produits destinés aux systèmes susmentionnés, sous l'angle de la sécurité informatique, et de renforcer la compréhension de la branche eu égard aux enjeux de la protection de ces systèmes. Dans la région D-A-CH (Allemagne, Autriche, Suisse), le livre blanc de la BDEW est devenu un document de référence pour la passation de marchés dans le domaine du courant de traction. Il est complété par des recommandations d'exécution.

Tableau 9 : Normes nationales et internationales relatives à la sécurité informatique

Titre	Éditeur(s) et description
Guide to Industrial Control Systems (ICS) *Security* SP 800-82	Éd. : ***National Institute of Standards and Technology*** **(NIST)** Ce guide donne une vue générale des typologies et architectures SCADA, identifie les menaces et les vulnérabilités, et énonce des recommandations concernant les contre-mesures et l'atténuation des risques. Il présente en outre des contrôles spécifiques SCADA fondés sur le cadre NIST 800-53.
Framework for Improving Critical Infrastructure Cybersecurity	Éd. : ***National Institute of Standards and Technology*** **(NIST)** Ce cadre fait suite à un décret présidentiel américain de 2013 intitulé « *Improving Critical Infrastructure Cybersecurity* » (améliorer la *cyber*sécurité des infrastructures critiques). Il propose une synthèse de différentes lignes directrices visant à dresser l'état des lieux d'une entreprise dans le domaine de la *cyber*sécurité et à définir une feuille de route pour améliorer les pratiques en la matière, en se référant à d'autres cadres et normes (ISO 27001, ISA 62443, NIST 800-53, COBIT, etc.).
Recommended Practice: Improving Industrial Control System Cybersecurity with Defense in Depth Strategies	Éd. : ***Industrial Control Systems Cyber Emergency Response Team*** **(ICS-CERT) du Département américain de la sécurité intérieure (DHS)** Ce document constitue une introduction générale à la stratégie de défense en profondeur des systèmes de contrôle industriels.
IT-Grundschutz-Kompendium – Werkzeug für Informations-sicherheit	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik*** **(BSI)** Ce compendium est la publication de référence en matière de protection informatique de base (*IT-Grundschutz*). Il constitue, avec les normes édictées par le BSI, une base solide pour appréhender la thématique de la sécurité de l'information. Le document détaille les différentes composantes de la protection informatique de base. Les menaces potentielles sont présentées dans une première partie, suivies des exigences fondamentales en matière de sécurité. Les composantes de la protection informatique de base sont réparties en dix sous-catégories thématiques allant des applications (APP) à la gestion de la sécurité (SGSI) en passant par l'informatique industrielle (IND). Différents niveaux de protection sont systématiquement examinés.
Normes BSI	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik*** **(BSI)** Les normes BSI sont une composante clé de la méthodologie relative à la protection informatique de base. Elles comprennent des recommandations sur les méthodes, les processus et les procédures ainsi que sur les marches à suivre et les mesures touchant aux différents aspects de la sécurité de l'information. Quelques exemples de normes BSI : 200-1 (SGSI), 200-2 (marche à suivre concernant la protection informatique de base), 200-3 (analyse des risques fondée sur la protection informatique de base) et 100-4 (analyse détaillée de la gestion des situations d'urgence sous la forme d'un guide pratique).
BSI-Zertifizierung nach ISO 27001 *auf der Basis von IT-Grundschutz*	La mise en place et le contrôle du dispositif de sécurité peuvent être réalisés selon les modalités de la protection informatique de base définies par le BSI, mais aussi selon les normes ISO 27000 ss. Ces deux approches sont compatibles. Toutes deux permettent de mettre en place et d'exploiter un SGSI, autrement dit d'identifier les risques en matière de sécurité de l'information et de les réduire à un niveau acceptable grâce à des mesures appropriées.

Tableau 9 : Normes nationales et internationales relatives à la sécurité informatique

Titre	Éditeur(s) et description
Zuordnungstabelle ISO *zum modernisierten IT-Grundschutz*	La norme BSI 200-2 relative à la protection informatique de base interprète les exigences et les mesures prévues par les normes ISO 27001 et 27002. Le tableau de correspondance aide les utilisateurs dans la transposition du contenu de ces deux normes ISO.
Industrielle Steuerungs- und Automatisierungssysteme (ICS) – *Allgemeine Empfehlungen*	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik*** **(BSI)** Le compendium est un ouvrage de référence destiné à permettre d'appréhender facilement la sécurité informatique des systèmes SCADA. Il présente les principes généraux de l'automatisation et précise les spécificités et les normes pertinentes dans ce domaine. Il contient en outre un ensemble de mesures et une marche à suivre pour la mise en œuvre. Des outils techniques supplémentaires sont proposés aux utilisateurs sur le site internet du BSI.
Tableau de correspondance – Mapping of Dependencies to International Standards	Éd. : **Agence de l'Union européenne pour la *cyber*sécurité (ENISA)** Ce rapport analyse les dépendances et les interactions entre les opérateurs de services essentiels (operators of essential services, OES) et les fournisseurs de services numériques (*digital service providers,* DSP), et propose une série d'indicateurs en vue de leur évaluation. Ces indicateurs sont mis en regard de normes et conditions-cadre internationales (ISO/CEI 27002, COBIT 5, mesures de sécurité du groupe de coopération SRI et NIST *Cybersecurity Framework*).
Communication Network Dependencies for ICS/SCADA *Systems*	Éd. : **Agence de l'Union européenne pour la *cyber*sécurité (ENISA)** Ce rapport se penche sur les réseaux de communication, sur l'intercommunication entre les SCI ou systèmes SCADA, sur l'identification des vulnérabilités, des risques et des menaces, et sur l'impact des systèmes *cyber*physiques sur la sécurité. Il comprend également une série de recommandations sur l'atténuation (*mitigation*) des risques identifiés. L'étude préliminaire a permis d'établir une liste de pratiques et de lignes directrices éprouvées visant à limiter autant que possible la vulnérabilité des SCI ou systèmes SCADA. Ce document vise principalement à donner un aperçu des interdépendances des réseaux de communication (SCI ou systèmes SCADA), et à identifier les ressources critiques sous l'angle de la sécurité, ainsi que les scénarios d'attaque et les menaces concrètes contre ces réseaux de communication.
Paysage des menaces de l'ENISA (taxonomie)	Éd. : **Agence de l'Union européenne pour la *cyber*sécurité (ENISA)** Ce document donne une vue d'ensemble des menaces et des tendances actuelles ou émergentes. Basé sur des données publiques, il offre une vision indépendante des menaces identifiées, de leurs auteurs et des tendances qui se dessinent. La taxonomie catégorise les menaces de façon systématique.

Tableau 9 : Normes nationales et internationales relatives à la sécurité informatique

10 Exigences réglementaires relatives à l'élimination des déchets

Les réglementations et normes nationales et internationales suivantes s'appliquent en matière de gestion des déchets :

Bases juridiques nationales

Responsabilité des organes en vertu de l'art. 754 du code des obligations
RS *220* – Loi fédérale du 30 mars 1911 complétant le Code civil suisse (Livre cinquième : Droit des obligations) (admin.ch)

Loi fédérale du 7 octobre 1983 sur la protection de l'environnement (loi sur la protection de l'environnement, LPE) ; RS *814.01*
RS *814.01* – Loi fédérale du 7 octobre 1983 sur la protection de l'environnement (loi sur la protection de l'environnement, LPE) (admin.ch)

Ordonnance du 4 décembre 2015 sur la limitation et l'élimination des déchets (ordonnance sur les déchets, OLED) ; RS *814.600*
RS *814.600* – Ordonnance du 4 décembre 2015 sur la limitation et l'élimination des déchets (ordonnance sur les déchets, OLED) (admin.ch)

Ordonnance du 22 juin 2005 sur les mouvements de déchets (OMoD) ; RS *814.610*
RS *814.610* – Ordonnance du 22 juin 2005 sur les mouvements de déchets (OMoD) (admin.ch)

Ordonnance du DETEC du 18 octobre 2005 concernant les listes pour les mouvements de déchets (RS *814.610.1*)
RS *814.610.1* – Ordonnance du DETEC du 18 octobre 2005 concernant les listes pour les mouvements de déchets (admin.ch)

Ordonnance du 20 octobre 2021 sur la restitution, la reprise et l'élimination des appareils électriques et électroniques (OREA) ; RS *814.620*
RS *814.620* – Ordonnance du 20 octobre 2021 sur la restitution, la reprise et l'élimination des appareils électriques et électroniques (OREA) (admin.ch)

Ordonnance du 5 juillet 2000 sur les emballages pour boissons (OEB) ; RS *814.621*
RS *814.621* – Ordonnance du 5 juillet 2000 sur les emballages pour boissons (OEB) (admin.ch)

Ordonnance du 7 septembre 2001 relative au montant de la taxe d'élimination anticipée sur les bouteilles en verre pour boissons (RS *814.621.4*)
RS *814.621.4* – Ordonnance du 7 septembre 2001 relative au montant de la taxe d'élimination anticipée sur les bouteilles en verre pour boissons (admin.ch)

Ordonnance du DETEC du 28 novembre 2011 sur le montant de la taxe d'élimination anticipée pour les piles (RS *814.670.1*)
RS *814.670.1* – Ordonnance du DETEC du 28 novembre 2011 sur le montant de la taxe d'élimination anticipée pour les piles (admin.ch)

Ordonnance du 26 août 1998 sur l'assainissement des sites pollués (ordonnance sur les sites contaminés, OSites) ; RS *814.680*
RS *814.680* – Ordonnance du 26 août 1998 sur l'assainissement des sites pollués (ordonnance sur les sites contaminés, OSites) (admin.ch)

Ordonnance du 26 septembre 2008 relative à la taxe pour l'assainissement des sites contaminés (OTAS) ; RS *814.681*
RS *814.681* – Ordonnance du 26 septembre 2008 relative à la taxe pour l'assainissement des sites contaminés (OTAS) (admin.ch)

Loi du 21 mars 2003 sur l'énergie nucléaire (LENu) ; RS *732.1*
RS *732.1* – Loi du 21 mars 2003 sur l'énergie nucléaire (LENu) (admin.ch)

Ordonnance du 10 décembre 2004 sur l'énergie nucléaire (OENu) ; RS *732.11*
RS *732.11* – Ordonnance du 10 décembre 2004 sur l'énergie nucléaire (OENu) (admin.ch)

Ordonnance du 25 mai 2011 concernant les sous-produits animaux (OSPA) ; RS *916.441.22*
https://www.fedlex.admin.ch/eli/cc/2011/372/fr

Ordonnance du 16 décembre 1985 sur la protection de l'air (OPair)
https://www.fedlex.admin.ch/eli/cc/1986/208_208_208/fr#app7ahref0

Ordonnance du 28 octobre 1998 sur la protection des eaux (OEaux)
https://www.fedlex.admin.ch/eli/cc/1998/2863_2863_2863/fr

Loi fédérale du 19 juin 1992 sur la protection des données (LPD)
https://fedlex.data.admin.ch/eli/cc/1993/1945_1945_1945/fr

Ordonnance du 22 juin 1994 sur la radioprotection (ORaP)
https://www.fedlex.admin.ch/eli/cc/1994/1947_1947_1947/fr

Ordonnance sur la radioprotection, nouvelle version uniquement en PDF
https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/2017/502/20210101/fr/pdf-a/fedlex-data-admin-ch-eli-cc-2017-502-20210101-fr-pdf-a.pdf

Normes nationales et recommandations

Office fédéral de la santé publique (OFSP), Élimination de substances radioactives, page d'aperçu
https://www.bag.admin.ch/bag/fr/home/gesund-leben/umwelt-und-gesundheit/strahlung-radioaktivitaet-schall/radioaktive-materialien-abfaelle/entsorgung-von-radioaktiven-abfaellen.html#193585208

Élimination de substances radioactives, directive de l'OFSP, PDF
https://www.bag.admin.ch/dam/bag/fr/dokumente/str/str-wegleitungen/abfaelle/artikel-114.pdf.download.pdf/201021_V1_Strahlenschutz_Wegleitung_Art-114_FR.pdf

IEEE802.11i *Network Standards*
https://standards.ieee.org/products-services/index.html

Avoir un comportement sûr dans le *cyber*espace
https://www.s-u-p-e-r.ch/fr/

Norme minimale pour améliorer la résilience informatique – Partie principale
https://www.bwl.admin.ch/dam/bwl/fr/dokumente/themen/ikt/broschuere_minimalstandard.pdf.download.pdf/IKT_FR_2018_Web.pdf

Norme minimale TIC – Outil d'évaluation (Excel)
Norme minimale pour les TIC (admin.ch)

Norme minimale pour les TIC – Électricité (en allemand uniquement)
https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/minimalstandard_strom.html

Norme minimale pour les TIC – Eaux usées (en allemand uniquement)
https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/abwasser.html

Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement du chauffage et du froid à distance
https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/fernwaerme-und-fernkaelteversorgung.html

Mots de passe sécurisés
https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-private/aktuelle-themen/schuetzen-sie-ihre-konten.html

Réglementations internationales

Évaluation de haut niveau à mi-parcours du processus européen Environnement et santé
https://www.euro.who.int/__data/assets/pdf_file/0011/294779/EHTF-MTR-Haifa-Report-fr.pdf

WHO *World Health Assembly 2015 resolution*
https://www.euro.who.int/en/health-topics/environment-and-health/air-quality/news/news/2015/05/air-quality-and-health-resolution-adopted-at-the-sixty-eighth-world-health-assembly

ISA-62443-1-1, *Security for industrial automation and control systems*
https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

NIST, *Cybersecurity Framework*
https://www.nist.gov/cyberframework

Glossaire

Terme	Description
Awareness	Prise de conscience, perception, sensibilisation
Résilience	Capacité de résistance psychique – aptitude à surmonter des situations difficiles sans subir de préjudice durable
POLYCOM	Polycom est un réseau de radiocommunication suisse basé sur Tetrapol.
Téléphonie SIP	Par « téléphonie SIP », on entend les appels téléphoniques passés via le protocole Internet.
ESXi	VMware ESXi (anciennement ESX) est un hyperviseur bare metal qui s'installe simplement sur votre serveur et le subdivise en plusieurs machines virtuelles.
Compétence inconsciente	Lorsqu'une personne est expérimentée au point que ses compétences relèvent quasiment d'une seconde nature, elle peut solliciter cet acquis à tout moment, de manière répétée, sans grand effort de concentration. N'ayant pas conscience de ces compétences, la personne aura du mal à les transmettre facilement. Les gens dotés de compétences inconscientes agissent de manière intuitive, mais n'ont plus la capacité d'analyser leurs actes.
Shop Floor	Atelier et production

Se référer au glossaire du NCSC (référentiel) pour d'autres définitions : https://www.ncsc.admin.ch/ncsc/fr/home/glossaire.html

Liste des abréviations utilisées

Abréviation	Description
API	Automate programmable industriel
ASED	Association suisse des exploitants d'installations de traitement des déchets
BIA	Bilan d'impact sur l'activité
BSI	*Bundesamt für Sicherheit in der Informationstechnik* (Allemagne)
CEI	Commission électrotechnique internationale (normes et standards)
CNA	*Corporate Network Access*
DCS/PLS	*Distributed Control System* (système numérique de contrôle-commande), système de commande
DCS ou ICS	Système de contrôle industriel, unités de pilotage pour la production industrielle tels qu'API
DECT	*Digital Enhanced Cordless Telecommunications*
DEP	*Device Enrollment Program* (programme d'inscription des appareils)
DMZ	*Demilitarized Zone,* zone démilitarisée (réseau)
FLR	Régulateur de combustion
GCA/BCM	Gestion de la continuité d'activité/*Business Continuity Management*
GSM	*Global System for Mobile Communications*
IHM	*Interface* homme-machine
IT	*Information Technology* (technologie de l'information), infrastructure bureautique classique
KPI	*Key Performance Indicator* (indicateur clé de performance)
LPD	Loi sur la protection des données
MDE	Maintenance de l'exploitation
NCSC	Centre national pour la *cyber*sécurité
NFC	*Near Field Communication* (communication en champ proche)
NIST	*National Institute of Standards and Technology*
OEaux	Ordonnance sur la protection des eaux
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFPP	Office fédéral de la protection de la population
OFSP	Office fédéral de la santé publique
OLED	Ordonnance sur la limitation et l'élimination des déchets (ordonnance sur les déchets)
OPair	Ordonnance sur la protection de l'air
ORaP	Ordonnance sur la radioprotection
OS	*Operating System,* système d'exploitation

Abréviation	Description
PCE	Processus clé « Élimination des déchets »
PDCA	*Cycle* PDCA (Plan-Do-Check-Act ou méthode de gestion de la qualité), *cycle* de Deming
PGJA	Parlement, gouvernement, justice, administration
PIC	Protection des infrastructures critiques
PLC, API	Programmable Logic Controller ou automate programmable industriel
PME	Petites et moyennes entreprises
SCADA	*Supervisory Control and Data Acquisition,* système de commande
SCI	Système de contrôle de l'information
SGE	Système de gestion énergétique
SGSI	Système de gestion de la sécurité de l'information (*Information Security Management System,* ISMS)
SIP	*Session Initiation Protocol*
SLA	*Service Level Agreement* (accord de niveau de service)
SMS	*Short Message Service*
TIC	Technologies de l'information et de la communication (acception globale)
TO	Technologie opérationnelle, infrastructure réseau pour système de commande
UE	Union européenne
UTD	Décharge souterraine
UVTD	Usine de valorisation thermique des déchets
VLAN	*Virtual Local Area Network*
WLAN	*Wireless Local Area Network*
WSUS	*Windows Server Update Services*

Table des illustrations

Liste des tableaux

11 Annexe

11.1 Bilan d'impact sur l'activité (BIA)

Sous sa forme adaptée au thème de l'élimination des déchets, le BIA décompose les processus critiques identifiés comme vecteurs d'attaque dans le cadre du Tableau 3 « Processus critiques dans les UVTD ». Les informations obtenues peuvent ainsi être facilement intégrées dans le BIA (voir exemple en annexe). Les critères d'évaluation financière varient selon les installations, raison pour laquelle les totaux des matrices de risque n'ont qu'une valeur indicative.

Le résultat du BIA traduit le risque résiduel que l'on est prêt à prendre nonobstant les mesures déjà prises.

Matrices de risque avec ordres de grandeur

Processus Élimination (déchets) rapporté à la situation globale						
E Événements entraînant une interruption prolongée de l'activité (> 1 jour)	E1	E2	E3	E4	E5	E6
D Événements entraînant une interruption prolongée de l'activité (< 1 jour)	D1	D2	D3	D4	D5	D6
C Événements entraînant une brève interruption de l'activité (< 12 h)	C1	C2	C3	C4	C5	C6
B Événements entraînant une restriction minime de l'activité	B1	B2	B3	B4	B5	B6
A Événements ayant des conséquences négligeables	A1	A2	A3	A4	A5	A6

Processus Infrastructure (GI)						
E > 60 mio CHF	E1	E2	E3	E4	E5	E6
D 30-60 mio CHF	D1	D2	D3	D4	D5	D6
C 10-30 mio CHF	C1	C2	C3	C4	C5	C6
B 1-10 mio CHF	B1	B2	B3	B4	B5	B6
A < 1 mio CHF	A1	A2	A3	A4	A5	A6

Processus Conduite de l'entreprise						
E > 60 mio CHF	E1	E2	E3	E4	E5	E6
D 30-60 mio CHF	D1	D2	D3	D4	D5	D6
C 10-30 mio CHF	C1	C2	C3	C4	C5	C6
B 1-10 mio CHF	B1	B2	B3	B4	B5	B6
A < 1 mio CHF	A1	A2	A3	A4	A5	A6

	Très faible	Faible	Limitée	Accrue	Élevée	Très élevée
sur 10 ans	< 5 %	5-25 %	15-30 %	50-75 %	> 75-90 %	> 95-100 %
	1	2	3	4	5	6
			Probabilité			

Figure 14 : Matrices de risque avec ordres de grandeur

Détails de l'analyse

	Risques						Mitigation (atténuation)				Mesures correctrices
N°	Catégorie de risque	Détail de la catégorie de risque	Description détaillée	Processus Élimination	Processus Infrastructure (GI)	Conduite de l'entreprise (administration des affaires)	Risque	Processus Élimination	Processus Infrastructure (GI)	Conduite de l'entreprise (administration des affaires)	Mesure
1a	Global	Communication des informations	Panne des communications, des données ; pas de données de processus pour la facturation et la maintenance, PLS non concernés								
1b	Global	Communication des informations	Panne des communications, messages vocaux, internet, téléphone, radio et internet perturbés								
2a	Global	Facteur humain	Fausse manipulation, surmenage, inattention, sous-occupation								
2b	Global	Facteur humain	Insatisfaction, sabotage								
2c	Global	Facteur humain	Victime involontaire (phishing, ingénierie sociale)								
3a	Télémaint. IT/ TO	Télémaintenance par des prestataires externes	Modification incontrôlée de programmes et de la conduite de processus								
3b	Télémaint. IT/ TO	Télémaintenance par des prestataires externes	Interruption des accès de télémaintenance								
4a	Télémaint. IT/ TO	Données d'exploitation	Écoulements incontrôlés, modifications, effacements								
4b	Télémaint. IT/ TO	Données d'exploitation	Perte d'accès aux données d'exploitation								
5	Télémaint. IT/ TO	Mises à jour automatiques	Mises à jour incorrectes, source de mise à jour invérifiable								
6	Télémaint. IT/ TO	Développement	Défaillance du système de maintenance, développement et adaptation du système productif (à cœur ouvert)								
7a	Télémaint. IT/ TO	Backup, sauvegardes TO	Sauvegardes manquantes, corrompues ou non plausibles								

Figure 15 : Détails de l'analyse selon le Tableau 3 Processus critiques dans les UVTD

Le document BIA peut être téléchargé via ce lien :

https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/abfallentsorgung.html

Auteurs et experts ayant contribué à la première édition :

Prénom, Nom	Organisation	Fonction
Hans-Peter Käser	OFAE	Chef de projet
Sven Peter	OFAE	Expert, assurance qualité
Sandra Rüfenacht	OFPP	Experte, assurance qualité
Ariane Stäubli	ASED	Cheffe de projet à l'ASED, experte, assurance qualité
Patric Imhof	Eniwa	Expert, assurance qualité
Thomas Bücherer	EWB	Expert, assurance qualité
Andreas Tschanz	EWB	Expert, assurance qualité
Christoph Beleda	IWB	Expert, assurance qualité
Bruno Hottinger	KVATG	Expert, assurance qualité
Marco Weber	KVATG	Expert, assurance qualité
Martin Muheim	Renergia	Expert, assurance qualité
Jonas Tschudi	SAIDEF	Expert, assurance qualité

Impressum et contact

Éditeur
Office fédéral pour l'approvisionnement économique du pays OFAE
Bernastrasse 28, CH-3003 Berne
www.ofae.admin.ch, info@bwl.admin.ch

Associations consultées :
Association suisse des exploitants d'installations de traitement des déchets (ASED)