Livre blanc sur la cybersécurité des réseaux électriques intelligents

Ce Livre blanc est issu des travaux du groupe de travail « REI-cyber » constitué au sein du cercle des entreprises de la SEE. *juin 2015*

Le concept de réseau électrique intelligent (REI) ou "smart grid"[1] est l'un des moyens aujourd'hui reconnus pour optimiser les performances des réseaux électriques et améliorer les services rendus au consommateur tout en le transformant en « *consom'acteur* ». Les REI permettent de répondre à des besoins nouveaux tels que l'insertion des énergies intermittentes et/ou décentralisées dans les systèmes électriques ou la gestion des parcs de véhicules électriques.

Les REI constituent également un enjeu industriel important, pris en compte par la « Nouvelle France industrielle », qui pourrait représenter d'ici 2020 dans notre pays plus de 25 000 emplois directs en France pour un chiffre d'affaires d'au moins six milliards d'euros[2].

Cependant les REI, comme tous les systèmes de collecte et de traitement de l'information, sont soumis à la menace de cyberattaques et aux risques qui en découlent, avec des conséquences qui peuvent être particulièrement dommageables, compte tenu du caractère vital des infrastructures électriques. Se protéger contre le risque cybersécuritaire est donc une nécessité. Mais le problème est difficile du fait de l'étendue et de la complexité des réseaux électriques, de l'exigence de sûreté de fonctionnement, de la nécessité de recourir à la télémaintenance pour diverses opérations, du nombre de parties prenantes et de l'émergence incessante de nouvelles formes d'attaques.

La SEE, du fait de son positionnement au carrefour entre industries électriques et électroniques et technologies de l'information et de la communication, a décidé d'élaborer, dans le cadre de son Cercle des entreprises, le présent Livre blanc.

Ce Livre blanc présente un caractère didactique : il met à la disposition des acteurs intéressés par les REI des éléments d'information essentiels sur la problématique des REI. Il analyse le risque cybersécuritaire sous différents angles et notamment au regard des risques attachés aux aspects plus traditionnels de la sécurité, sûreté de fonctionnement en particulier. Il fait le point sur la réglementation et sur les normes potentiellement applicables aux REI qui, bien qu'étant pour certaines encore en cours de finalisation, permettent à la plupart des acteurs de disposer d'un référentiel suffisant pour construire un système de gestion de la cybersécurité adapté à leurs besoins.

Au niveau français, l'autorité en matière de cybersécurité est l'Agence nationale de la sécurité des systèmes d'information (ANSSI), à l'origine notamment de la parution des décrets du 27 mars 2015 relatifs à la sécurité des systèmes d'information des opérateurs d'importance vitale (OIV). Au niveau international, le corpus norma-

[1] Selon la feuille de route des réseaux électriques intelligents établie par l'initiative gouvernementale de la Nouvelle France industrielle, et présentée au Président de la République le 7 mai 2014 les réseaux électriques intelligents (REI) ou "smart grids"visent à intégrer de manière efficiente les actions de l'ensemble des utilisateurs (producteurs et consommateurs) afin de garantir un approvisionnement électrique durable, sûr et au moindre coût. Ils font appel à des produits et services innovants ainsi qu'à des technologies d'observation, de contrôle, de communication afin de :
- faciliter le raccordement et l'exploitation de tous les moyens de production, en particulier des renouvelables en réduisant de façon significative l'impact environnemental du système électrique complet ;
- permettre au consommateur de jouer un rôle actif dans l'exploitation optimisée du système électrique ;
- optimiser le niveau de fiabilité, de sûreté et de qualité de l'électricité, et améliorer les services actuels de façon efficiente ;
- accompagner le développement d'un marché de l'électricité européen intégré ;
- augmenter la résilience du système électrique.

[2] Selon la feuille de route précitée.

tif est aujourd'hui essentiellement développé par la CEI et l'ISO, dans le cadre des normes générales ISO/CEI 27001 et 27002 et des standards CEI 62443 spécifiques aux systèmes d'automatismes et de contrôle industriel (IACS) qui, dans leur version finale, intègreront les exigences des normes ISO/CEI 27001 et 27002. Le "Technical Report" ISO/CEI TR 27019, guide d'application de l'ISO/CEI 27002 pour les systèmes de contrôle des procédés spécifiques à l'industrie de l'énergie, ainsi que la norme CEI 62351 qui vise à sécuriser les données et les communications dans les systèmes de puissance, complètent ce corpus normatif. Au niveau européen, des travaux importants ont été menés par l'ENISA et par un groupe de travail commun aux trois organismes de normalisation CEN, CENELEC et ETSI, dans le cadre du mandat M/490 qui leur a été délivré par la Commission européenne. Ces travaux[3] ont conduit à la mise au point d'un modèle fonctionnel des REI, le « *SGAM* », et d'une méthodologie dite "*framework SGIS*" permettant d'analyser les risques encourus par les systèmes ou sous-systèmes et de définir le niveau de sécurité à retenir pour leur protection.

D'autres référentiels sont également à prendre en considération dans certains pays et en particulier aux Etats-Unis où les standards CIP élaborés par le NERC ont été rendus obligatoires dans les réseaux de transport d'électricité.

Le cadre réglementaire et normatif ainsi appelé, le Livre blanc s'attache à préciser la nature des attaques et des risques auxquels les REI sont confrontés. On retrouve dans le cas des REI les attaques qui peuvent affecter n'importe quel système de collecte et de traitement d'information. Toutefois les REI présentent des vulnérabilités spécifiques du fait de leur extension géographique, de leur configuration évolutive et de la difficulté d'assurer la protection aux frontières d'un ensemble pouvant rassembler, comme en France, des dizaines de millions d'abonnés.

Les risques qui en découlent sont de trois natures principales :

- la malveillance, visant à perturber l'exploitation des réseaux et pouvant aller jusqu'à leur effondrement, liée à des attaques du type homme du milieu, injection de code malveillant, déni de service, etc.
- la fraude, liée à l'altération de données servant à la facturation des fournitures d'électricité ;
- les atteintes à la vie privée, c'est-à-dire à la « *privacité* », du fait de l'utilisation abusive de données prélevées sur les équipements en relation directe avec le mode de vie des personnes (essentiellement aujourd'hui les compteurs communicants et, dans une moindre mesure, les stations de recharge des véhicules électriques).

A l'avenir, le raccordement d'équipements de plus en plus nombreux, en aval des compteurs communicants ou des "boxes" proposées par les fournisseurs d'accès à Internet ou les agrégateurs d'effacement, élargira encore davantage la surface d'attaque et fera planer le risque de voir ces équipements manipulés à distance et de façon coordonnée.

Le Livre blanc passe en revue les principales mesures de protection qui peuvent être mobilisées pour faire face à ces menaces. La cybersécurité se construit sur la base de la combinaison de mesures techniques, organisationnelles et humaines. Ces mesures de protection doivent être conçues et mises en œuvre dans le cadre d'un programme de gestion de la cybersécurité construit de façon rationnelle en s'appuyant sur un référentiel normatif.

Les mesures techniques doivent être conçues tout d'abord au stade de la conception de l'architecture ; c'est la "security by design". Une analyse menée selon les principes du SGAM et selon la méthodologie proposée par le groupe SGIS du CEN/CENELEC/ETSI permet de hiérarchiser les niveaux de sécurité à retenir pour chaque élément constitutif de l'architecture et de jeter les bases d'une défense en profondeur. Cependant de nouveaux principes apparaissent, soutenus notamment par le Trusted Computing Group[4], s'insérant dans une réflexion plus géné-

[3] Voir :CEN-CENELEC-ETSI "SG-CG/M490/F Overview of SG-CG Methodologies", ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Methodology_Overview.pdf

[4] Voir notamment : TCG Guidance for securing IoT – Avril 2015 – http://www.trustedcomputinggroup.org/files/static_page_files/D6DED84B-1A4B-B294-D09EE5563BED7F93/TCG_Guidance_for_Securing_IoT_1_0r14-public-review.pdf

rale menée sur l'Internet Industriel des Objets (IIoT). Cette approche vise à transformer le REI en une sorte de réseau social où chaque abonné pourra converser de façon contrôlée avec les autres abonnés en fonction des droits qui lui auront été alloués.

La protection des îlots d'automatisme relève pour certains d'entre eux – pour les systèmes de contrôle de postes notamment – des méthodes classiques applicables aux systèmes de contrôle industriel. L'approche par sous-systèmes préconisée par l'ANSSI ou par zones de sécurité telles que définies par la CEI 62443, avec allocation de mesures de sécurité adaptées à chacun de ces sous-systèmes ou zones, est dans ce cas appropriée. Dans d'autres cas, des méthodes plus innovantes ont dû être imaginées, notamment pour le système de comptage *Linky* pour lequel des dispositions ont été prises au niveau du compteur et au niveau des concentrateurs dotés de modules de sécurité. Ces approches ouvrent la voie au développement de "*Trusted Platform Modules*", composants cryptographiques matériels inviolables solidaires des équipements et dans lesquels sont stockés tous les éléments, tels que les clés de chiffrement et d'authentification, relatifs à leur sécurité.

La communication entre les ilots est évidemment un point sensible sur lequel se concentrent de nombreuses attaques. Les REI, comme la plupart des systèmes de contrôle industriel, utilise encore, par héritage du passé, des protocoles faibles, souvent des protocoles applicatifs, construits au-dessus de la couche transport du modèle OSI, dont les vulnérabilités sont connues. Ces protocoles peuvent être détournés de leur objectif si l'on utilise certaines instructions pour exécuter des commandes dommageables au réseau ou pour créer des dénis de service.

La sécurisation des communications commence par la limitation des échanges à leur strict nécessaire et par l'application d'un principe de « subsidiarité » dans la gestion des informations. Pour les communications considérées comme nécessaires, il y a lieu d'homogénéiser les solutions utilisées, de façon à réduire la surface d'attaque, et de faire appel à des protocoles standardisés et reconnus comme robustes. De tels protocoles, ainsi que la technologie des réseaux privés virtuels (VPN), sont bien maîtrisés et doivent être mis en œuvre chaque fois que nécessaire, en veillant cependant à ce que cela ne porte pas atteinte aux performances du système.

Les connexions distantes, filaires ou par radiocommunications, ne sont pas à bannir de façon systématique car elles sont porteuses de gains de flexibilité et de productivité. Elles doivent cependant faire l'objet d'une analyse de risques spécifique et être utilisées avec la plus grande circonspection lorsque l'authentification de l'abonné distant ne peut pas être assurée ou lorsqu'elles pointent vers les équipements les plus sensibles des REI.

Les technologies de chiffrement et d'authentification jouent un rôle essentiel pour assurer la confidentialité et l'intégrité des données et prévenir des accès non autorisés. Elles participent également de la protection de la vie privée en évitant la divulgation d'information de caractère personnel vers des tiers non autorisés. De nombreux algorithmes, symétriques (AES 128 ou 256) ou asymétriques (RSA, courbes elliptiques), sont aujourd'hui disponibles et semblent suffisamment robustes dans l'état actuel de la puissance des ordinateurs conventionnels, en attendant la mise au point sans doute encore lointaine d'ordinateurs quantiques. Le Livre blanc met cependant l'accent sur l'intérêt de développer les techniques de chiffrement « homomorphes » qui permettent de traiter des données chiffrées sans avoir préalablement à les déchiffrer. De telles techniques seraient particulièrement intéressantes dans le cas de chaines de traitement à plusieurs niveaux telles que celles des REI.

Le Livre blanc insiste également sur la qualité des logiciels. Celle-ci est bien évidemment une condition nécessaire à l'obtention d'un niveau de sécurité fonctionnelle suffisant. Mais un logiciel mal conçu ou porteur de défauts est plus vulnérable que d'autres à des attaques cybersécuritaires. Les défauts de sécurité doivent être considérés comme des "bugs" des programmes et des outils d'analyse de code existent aujourd'hui permettant d'établir de façon semi-automatique la conformité des composants logiciels aux exigences dé cybersécurité.

En parallèle aux mesures techniques, les mesures organisationnelles sont primordiales pour construire la cybersécurité. Les exigences en matière d'organisation font l'objet de normes internationales qui sont citées en annexe 1. Elles doivent donner naissance à des procédures appropriées au rôle joué par les intervenants dans la chaine des REI : développeurs et fournisseurs de composants et de systèmes, intégrateurs, opérateurs, sociétés de services. Le Livre blanc identifie plusieurs points-clés auxquels il convient de porter attention dans le cas des REI : filtrage des communications, authentification, droits d'accès et autorisations, traçabilité, supervision et administration du système de gestion de la cybersécurité, traitement des incidents et politique de reprise.

Ce dernier point est particulièrement important dans le cas des REI. La sécurité absolue n'existe pas et il faut se résoudre à ce que certains incidents surviennent. Il faut en réduire la fréquence et en limiter les conséquences. Il faut aussi établir des règles de rétablissement du service dans des délais aussi courts que possible, en préservant les données qui permettront une analyse ultérieure de l'origine des défauts.

Parmi les mesures organisationnelles, une priorité est également donnée aux actions de formation. La cybersécurité est une « science jeune » et les compétences disponibles sur le marché sont encore rares et que les sociétés de service et de conseil absorbent une part importante du potentiel formé chaque année. La réponse aux besoins des REI pourrait être une combinaison de plusieurs approches : une formation amont combinant une « sensibilisation de masse » d'un grand nombre de personnels avec des formations plus spécifiques, au sein ou en complément de formations existantes, une formation des maitres d'ouvrage et maitres d'œuvre, des intervenants professionnels, des opérateurs et des auditeurs.

Pour l'avenir, le Livre blanc recommande d'avoir une politique de démonstrateurs REI davantage ciblée sur la cybersécurité, comme l'est le projet[5] « Postes électriques intelligents » lancé en 2013 par l'ADEME, RTE, ERDF et plusieurs industriels. Les démonstrateurs REI constituent en effet un axe important du Programme investissements d'avenir (PIA) et la cybersécurité doit y figurer avec l'importance requise.

Le Livre blanc préconise de poursuivre les travaux de certification de sécurité des REI, au niveau des principaux composants et sous-systèmes, matériels ou logiciels, politique qui constituent un complément indispensable à la politique de normalisation et de qualification des prestataires. Des ébauches de telles politiques existent dans certains pays, pour les compteurs intelligents notamment, mais ces actions sont fragmentées. La politique de certification doit être harmonisée au niveau européen tout en laissant la possibilité aux Etats de développer éventuellement des règles spécifiques correspondant à des cas d'usage particuliers dûment justifiés.

Enfin le Livre blanc recommande de poursuivre les travaux de recherche-développement dans des directions ciblées : la sécurisation des systèmes distribués, en liaison avec les travaux sur l'Internet industriel des objets (IIoT), et les méthodes de chiffrement homomorphes.

La SEE se propose d'organiser en 2016, en liaison avec la nouvelle association Smart grids France, un forum qui permettra de prendre la mesure des progrès accomplis en matière de cybersécurité et de proposer de nouvelles recommandations sur les orientations à prendre. ■

[5] Voir le dossier de presse à l'adresse http://www.presse.ademe.fr/files/2013_06_04-dossier-presse-postes-intelligents-v1.pdf

La cybersécurité des réseaux électriques intelligents

1. Introduction

1.1. Pourquoi un Livre blanc ?

Un réseau électrique intelligent (REI en abrégé et « smart grid » en anglais) est un réseau électrique dans lequel un système de collecte et de traitement de l'information vient se superposer au transport et à la distribution de l'électricité afin d'optimiser les performances du réseau et d'améliorer le service rendu au consommateur tout en permettant de répondre à des besoins nouveaux tels que l'insertion des énergies intermittentes et/ou décentralisées dans le système électrique.

L'une des manifestations les plus tangibles du développement des REI en France est le déploiement des compteurs communicants et en particulier en France du dispositif Linky promu par ERDF. Mais les ambitions des REI vont bien au-delà et doivent se traduire par une gestion du système électrique optimisée, fiable et sécurisée, répondant aux besoins des parties prenantes qu'ils soient producteurs ou consommateurs.

Cependant les REI, comme tous systèmes de traitement de l'information, sont soumis à la menace de cyberattaques et aux risques qui en découlent, avec des conséquences qui peuvent être particulièrement dommageables compte tenu du caractère vital des infrastructures électriques. Se protéger contre le risque cybersécuritaire est donc une nécessité. Mais le problème est difficile du fait de l'étendue et de la complexité des réseaux électriques, de l'exigence de sûreté de fonctionnement, de la nécessité de recourir à la télémaintenance pour diverses opérations, du nombre de parties prenantes et de l'émergence incessante de nouvelles formes d'attaques.

Des travaux importants sont en cours sur le sujet, chez les opérateurs, chez certains grands industriels, au niveau national et au niveau international. Cependant, il est apparu qu'il serait utile de donner de la cohérence à ces différentes approches en posant le problème dans sa globalité et en essayant de sérier les réponses qu'il est aujourd'hui possible de lui apporter.

Ce faisant, le but n'était pas d'écrire une encyclopédie des REI qui nécessiterait des moyens considérables et entraînerait des délais prohibitifs, avec le risque de voir le travail déjà obsolète le jour où il serait achevé. La SEE, au travers de son Cercle des entreprises, a voulu rassembler dans un seul document les informations essentielles permettant aux acteurs concernés par les REI d'user d'un vocabulaire commun et d'acquérir rapidement les données de base nécessaires au développement de leurs activités dans leurs domaines respectifs.

Les cibles de ce Livre blanc sont donc :

- les organismes publics ayant à connaître des réseaux électriques intelligents ; c'est-à-dire les parties prenantes telles que l'Administration et les organismes publics concernés : certains ministères, CRE, ANSSI, laboratoires de recherche publics, secteur académique…
- le secteur industriel y compris celui des PME et ETI (développeurs de nouveaux équipements ou services, installateurs, etc.) ;
- et bien entendu, les opérateurs qui, s'ils possèdent les compétences propres requises par la gestion des REI, pourront néanmoins faire de ce Livre blanc un trait d'union avec leurs nombreux interlocuteurs.

Ce document doit en effet permettre de développer les messages que les opérateurs et d'autres grands acteurs, publics ou privés, souhaitent promouvoir pour clarifier les enjeux de la cybersécurité des REI et faire comprendre aux parties prenantes les dispositions à prendre. C'est pourquoi le Livre blanc s'attache à :

- donner une vision prospective des REI, c'est-à-dire l'état de l'art des REI et leurs évolutions possibles ;
- identifier les risques et les menaces ainsi que la façon de les gérer ;
- présenter les solutions disponibles à différents niveaux en distinguant les contre-mesures qui existent de celles qui réclament encore des approfondissements ;
- formuler des recommandations concernant l'organisation des équipes et leurs formations, les politiques et procédures ainsi que la gestion des infrastructures.

Pour des raisons bien compréhensibles, on ne trouvera pas dans ce Livre blanc une analyse détaillée des menaces pesant sur les REI ainsi que des vulnérabilités qui pourraient être mises à profit par des attaquants éventuels. Les acteurs désireux de se prémunir contre de tels risques devront

continuer à se rapprocher des opérateurs, des agences spécialisées et de l'ANSSI[1] en particulier, en s'entourant des conseils de spécialistes du domaine.

1.2. La problématique de la cybersécurité des réseaux électriques

1.2.1. Définition de la cybersécurité

La cybersécurité peut se définir comme l'état recherché pour un système d'information lui permettant de résister à des événements d'origine malveillante, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et d'altérer en conséquence les services rendus par ce système. A cette fin, la cybersécurité met en œuvre des mesures techniques et organisationnelles de protection ainsi que des mesures de détection et de réaction face aux attaques

La cybersécurité est partie intégrante d'un concept plus vaste qui est celui de la sécurité. Cependant ce terme est ambigu et correspond, selon les contextes et les interlocuteurs, des choses différentes. Afin de lever toute ambiguïté, nous éviterons dans ce Livre blanc de l'utiliser et le terme « cybersécurité » sera préféré dans la suite du texte.

1.2.2. Aperçu sur la cybersécurité des réseaux électriques

Le thème de la cybersécurité, s'il a pris une dimension médiatique très importante ces dernières années, n'est pas pour autant nouveau pour les responsables de la conception et de la gestion des systèmes électriques. En effet, le pilotage du réseau de transport d'électricité implique l'échange de flux d'informations importants entre les centres de production, les centres de contrôle et les postes électriques. Le nombre finalement restreint d'acteurs, tous de culture industrielle, a permis jusqu'à présent de maîtriser le risque cybersécuritaire. En particulier, la mise en œuvre d'un réseau dédié – dont les points de connexion au réseau d'entreprise via des passerelles sont peu nombreux et peuvent être surveillés en continu – conjuguée à la protection physique des sites les plus sensibles, a longtemps constitué une parade suffisamment efficace.

Depuis le début des années 2000, le fort développement du contrôle-commande numérique dans les postes électriques a fait apparaître une nouvelle classe de vulnérabilités, pas spécifique aux systèmes électriques, mais commune à l'ensemble des systèmes numériques de contrôle industriel qui a été mise en évidence par « l'épisode Stuxnet »[2]. La possibilité d'accéder au cœur de ces systèmes, facilitée par l'utilisation de systèmes d'exploitation à grande diffusion tels que Windows de Microsoft, a appelé l'attention de nombreux hackers et constitue aujourd'hui un nouveau défi. A cette occasion, une prise de conscience s'est développée quant à la nécessaire maitrise des modes opératoires et sur le fait qu'au-delà des dispositifs de protection physique et technique, la formation des opérateurs était une composante essentielle de la maîtrise de la cybersécurité.

Depuis lors, cette préoccupation est intégrée aux différents projets de démonstrateurs de REI. Ainsi en va-t-il du projet « Postes électriques intelligents », lancé en juin 2013, soutenu par l'ADEME et qui regroupe des opérateurs de réseaux et des industriels[3]. Ce projet met l'accent sur la cybersécurité et vise à doter les futurs postes intelligents de moyens innovants de sécurisation pour faire face à l'ensemble des risques liés aux nouvelles technologies.

Il reste que le déploiement à grande échelle des REI, en raison du nombre très important d'acteurs devant communiquer entre eux, fait apparaître de nouveaux types de risques qui ne pourront être approchés par les méthodes traditionnelles applicables à la protection des systèmes numériques de contrôle industriel. C'est une nouvelle approche de la cybersécurité, adaptée à l'architecture ramifiée et évolutive des REI qu'il faut développer.

Par ailleurs, si la cybersécurité d'un système électrique dépend au premier chef de l'opérateur du réseau, elle dépend aussi d'autres acteurs ayant un rôle important dans l'équilibre offre-demande. C'est aujourd'hui le cas des grands sites de production mais c'est de plus en plus le cas des producteurs décentralisés et des consommateurs qui sont amenés à participer de plus en plus à la vie du réseau pour adapter, en permanence et au moindre coût, l'offre à la demande.

C'est donc l'ensemble de l'écosystème du monde électrique qui est concerné. Les REI, dont on attend beaucoup en termes de performances techniques et économiques devront savoir répondre au défi de la cybersécurité.

---

[1] ANSSI : Agence nationale de la sécurité des systèmes d'information. L'annexe du guide publié par l'ANSSI, intitulé, « Cybersécurité des systèmes industriels, Méthode de classification et mesures principales » propose des définitions complémentaires auxquelles le lecteur pourra se reporter. Ce document est disponible à l'adresse http://www.ssi.gouv.fr/uploads/IMG/pdf/securite_industrielle_GT_methode_classification-principales_mesures.pdf

[2] On appelle « épisode Stuxnet » l'attaque mise en évidence à partir de l'été 2010, qui a ciblé les installations iraniennes d'enrichissement de l'uranium et qui s'est traduite par un dérèglement du contrôle des centrifugeuses. L'attaque a été imputée à un logiciel malveillant, dénommé Stuxnet, vraisemblablement injecté initialement dans les systèmes à l'aide de clés USB corrompues.

[3] http://www.presse.ademe.fr/files/2013_06_04-dossier-presse-postes-intelligents-v1.pdf

1.2.3. Cybersécurité et sûreté de fonctionnement

Il est utile de préciser la définition de cybersécurité au regard de celle de sûreté de fonctionnement avec laquelle des confusions sont fréquentes.

La sûreté de fonctionnement peut se définir comme l'aptitude d'un système à accomplir les fonctions qu'on en attend, dans des conditions définies et durant un intervalle de temps donné. La sûreté de fonctionnement traite en particulier les propriétés de fiabilité, maintenabilité, disponibilité et sécurité. La sécurité est entendue ici au sens de sécurité des biens et des personnes. La sûreté de fonctionnement comprend un sous-ensemble dénommé « sécurité fonctionnelle » qui s'adresse aux systèmes assurant la protection des biens et des personnes.

La cybersécurité et la sûreté de fonctionnement, si elles présentent des points communs, comme l'évaluation des risques liés à l'atteinte à l'intégrité et à la disponibilité, présentent une différence majeure : la sûreté de fonctionnement traite des risques liés aux défaillances, alors que la cybersécurité traite des risques liés à la malveillance. **La sûreté de fonctionnement s'appuie sur des calculs et des statistiques pour déterminer les risques de défaillance d'un système contrairement à la cybersécurité qui ne peut qu'estimer une vraisemblance des risques liés à la malveillance.** Enfin, la sûreté de fonctionnement ne se préoccupe pas des atteintes à certains services de sécurité tels que la confidentialité et la traçabilité, contrairement à la cybersécurité.

Néanmoins, la finalité générale reste la même. En s'appuyant sur des méthodes telles que l'AMDEC dans le cas de la sûreté de fonctionnement et EBIOS dans celui de la cybersécurité, l'objectif est d'identifier les risques pesant sur un système pour les maintenir ou les ramener à un niveau acceptable. La cybersécurité prend en compte des risques complémentaires à la sûreté de fonctionnement auxquels sont associés de nouveaux modes de défaillance.

L'atteinte à la continuité de fourniture est une problématique « inscrite dans le patrimoine génétique » des opérateurs de réseaux. De tout temps, des parades ont été mises en place pour garantir la sûreté du système opéré. Si on mesure bien la différence entre les notions de sûreté et de cybersécurité, les mesures prises pour répondre à la sûreté offrent une ouverture naturelle permettant de supporter les deux notions. L'efficience de la protection du système a toujours été assurée par des procédures métier mais le monde industriel évolue aujourd'hui vers de nouvelles technologies impliquant des échanges d'informations plus nombreux et plus fréquents. Les REI reflètent cette tendance lourde ; ils intègrent des évolutions fonctionnelles que doit prendre en compte l'opérateur pour la conduite et l'exploitation des réseaux : plus d'informations issues du terrain, des systèmes numérisés, des automatismes distribués, des communications inter-systèmes en nombre croissant… Ces ouvertures créent des vulnérabilités dans un système historiquement cloisonné. Mais l'évolution du système électrique est nécessaire et déjà enclenchée. La cybersécurité est un besoin métier que tous les opérateurs doivent à présent intégrer.

1.3. La réglementation française des REI

La cybersécurité des REI est réglementairement de la responsabilité des « opérateurs » encore appelés les « gestionnaires ». Certains peuvent être d'importance vitale et donc soumis à la réglementation relative aux Opérateurs d'Importance Vitale (OIV) définie par le code de la Défense. Ces OIV répondent à des directives nationales de sécurité (DNS) et doivent élaborer un Plan de sécurité opérateur[4]. Ce dispositif est décrit en détail dans l'Instruction générale interministérielle, relative à la sécurité des activités d'importance vitale N°6600/SGDSN/PSE/PSN du 7 Janvier 2014.

Les OIV seront également soumis aux articles concernant la cybersécurité de la loi de programmation militaire (LPM) du 18 décembre 2013[5] dont les décrets d'application ont été publiés le 27 mars 2015[6].Ces articles, parmi d'autres mesures, permettront au Premier ministre, à travers l'Agence nationale de la sécurité des systèmes d'information (ANSSI), de fixer des règles pour renforcer la sécurité des systèmes d'information critiques des OIV, de recevoir des notifications d'incidents (tentatives d'intrusion par exemple) touchant ces systèmes et de mener des contrôles pour évaluer le niveau de sécurité et vérifier la bonne application des règles fixées et, en cas d'attaque ma-

---

[4] Il s'agit de la réglementation applicable en France qui découle de la directive européenne 2008/114/CE du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

[5] Cette loi est relative à la programmation militaire pour les années 2014 à 2019 et porte diverses dispositions concernant la défense et la sécurité nationale.

[6] Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du Livre III de la première partie de la partie législative du code de la défense.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030405967&categorieLien=id
Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de la confiance pour les besoins de la sécurité nationale.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030405903

jeure, de décider des mesures à mettre en place. La France est le premier pays à adopter une telle réglementation[7].

Avant la LPM, les pouvoirs publics se sont intéressés à la question de la sécurité des REI et notamment à la sécurité des compteurs évolués (parfois appelés compteurs intelligents). L'arrêté relatif au comptage électrique du 4 janvier 2012[8] intègre des éléments relatifs à la cybersécurité puisqu'il prévoit, dans son article 4, que « *Les dispositifs de comptage mentionnés au présent article sont conformes à des référentiels de sécurité approuvés par le ministre chargé de l'énergie. Cette conformité est vérifiée par une évaluation et une certification conformément aux dispositions du décret du 18 avril 2002 susvisé*[9] ». A l'avenir cette approche pourrait être étendue aux textes réglementaires (arrêtés) définissant par exemple les exigences pour pouvoir raccorder des équipements sur le réseau de distribution.

Enfin, la réglementation relative à la protection de données personnelles[10] s'applique également. En effet, les REI ont pour vocation d'irriguer jusqu'au consommateur final, à l'intérieur du domicile des particuliers, via notamment les compteurs évolués. Des équipements domestiques relevant de la vie de tous les jours, tels que les chauffe-eau, radiateurs, éclairage, équipements électroménagers et domotiques, etc., qui véhiculeront très certainement des données à caractère personnel, communiqueront avec les compteurs évolués. Cet aspect est traité par la CNIL qui a publié avec la FIEEC, à la suite des réflexions d'un groupe de travail, un « *Pack de conformité Smart grids et données personnelles »*[11] pour les compteurs évolués. Ce pack formule des recommandations sur les conditions de collecte et de traitement des données personnelles relatives à la consommation électrique par des appareils installés par les usagers en aval des compteurs électriques et vise à assurer une étanchéité complète entre les données aval et amont du compteur.

1.4. Travaux européens sur la cybersécurité des réseaux électriques intelligents

Au niveau européen, de nombreuses initiatives ont été lancées sur le sujet de la cybersécurité des Réseaux électriques intelligents (REI). Parmi celles-ci, l'attention doit être portée sur trois documents intéressants :

- le rapport "*Smart Grid Threat Landscape and Good Practice Guide*" de l'ENISA[12] ;
- le rapport "*Proposal for a list of security measures for smart grids*" de l'ENISA et de l'Expert Group 2 (EG2) de la Smart Grid Task Force de la Commission européenne[13];
- le rapport "*Smart Grid Information Security"* du Groupe de travail"Smart Grid Coordination Group (SG-CG/SGIS)" du CEN-CENELEC-ETSI[14].

Certains de ces documents utilisent le Smart Grid Architecture Model (SGAM)[15] qui est un modèle générique des REI développé par un groupe de travail du CEN, du CENELEC et de l'ETSI, dans le cadre du mandat M/490 de la Commission européenne, afin de parvenir à un référentiel commun permettant de faire progresser plus facilement les travaux de normalisation. Ce modèle n'est pas spécifique à la cybersécurité mais son utilisation permet aux acteurs concernés par la cybersécurité de positionner leur problème par rapport à un référentiel commun et de l'analyser de façon méthodique.

Le modèle SGAM est fondé sur la notion de "Smart Grid Plane" qui décompose le plan d'un REI selon deux dimensions (figure 1) :

- la composante « Domain » allant de la "Bulk generation" aux « Customers Premises » en passant par la « Transmis-

[7] Aux Etats-Unis, l'Executive Order 13636 du 12 février 2013 du Président Obama vise également à renforcer la cybersécurité des infrastructures critiques. Les travaux ont été confiés au NIST (National Institute of Standards and Technology) dont les conclusions figurent dans le rapport disponible à l'adresse suivante :
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
Ces travaux encouragent les opérateurs à renforcer le niveau de cybersécurité des infrastructures critiques qu'ils opèrent en suivant le guide établi dans le rapport précédemment cité.

[8] Arrêté du 4 janvier 2012 pris en application de l'article 4 du décret n° 2010-1022 du 31 août 2010, relatif aux dispositifs de comptage sur les réseaux publics d'électricité, pris par le ministre de l'économie, des finances et de l'industrie, de l'énergie et de l'économie numérique.

[9] Décret n° 2002-535 du 18 avril 2002, relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

[10] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[11] http://www.cnil.fr/linstitution/actualite/article/article/innovation-dans-le-pilotage-energetique-du-logement-un-pack-de-conformite-pour-les-compteurs-c

[12] ENISA, "Smart Grid Threat *Landscape and Good Practice Guide*"
https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/sgtl/smart-grid-threat-landscape-and-good-practice-guide/at_download/fullReport

[13] ENISA et groupe de travail (EG2) de la Commission européenne, "*Proposal for a list of security measures for smart grids*".
https://ec.europa.eu/energy/sites/ener/files/documents/20140409_enisa_0.pdf

[14] CEN-CENELEC-ETSI, "SG-CG/M490/H Smart Grid Information Security"
ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf

[15] CEN-CENELEC-ETSI "SG-CG/M490/F Overview of SG-CG Methodologies", ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Methodology_Overview.pdf

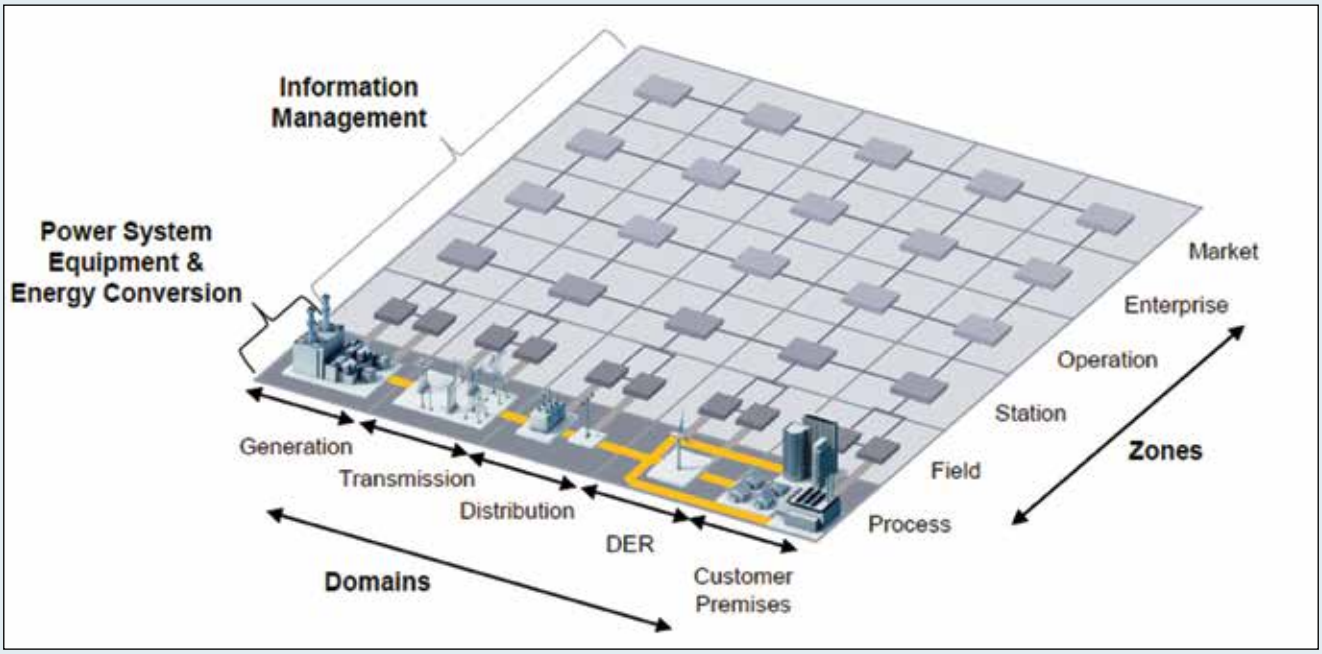

Figure 1 : Smart Grid Plane – Source : CEN-CENELEC-ETSI.

sion », la « Distribution » et les « DER : Distributed Electrical Resources » ;

- la composante « Zones » qui correspond grosso modo aux niveaux de la pyramide CIM[16] dite de Purdue, allant du "Process" au "Market" en passant par le "Field", la "Station", « l'Opération », et « l'Entreprise ».

La figure 1 illustre la notion de "Smart Grid Plane" en faisant apparaître les îlots correspondant au découpage selon ces deux axes.

Les fonctionnalités assurées par chacun de ces îlots peuvent être analysées en « niveaux d'interopérabilité » un peu à l'image du séquencement proposé dans le domaine des communications par le modèle OSI. Cinq couches sont ainsi proposées : "Component" "Communication", "Information", "Function", "Business", ce qui conduit au modèle à trois dimensions de la figure 2.

Le rapport "*Smart Grid Threat Landscape and Good Practice Guide*" établit un panorama des menaces liées aux REI et des bonnes pratiques qui peuvent être utilisées pour s'en protéger. Il propose une cartographie des équipements utilisés dans les REI en utilisant le SGAM. Il fournit une liste d'équipements et de menaces. Les équipements

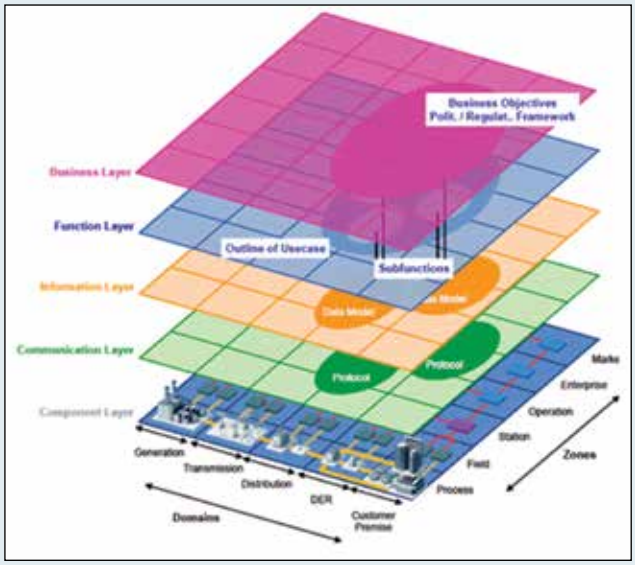

Figure 2 : Les cinq couches du SGAM – Source : CEN-CENELEC-ETSI.

sont ensuite liés aux menaces et les menaces aux bonnes pratiques.

Le rapport "*Proposal for a list of security measures for smart grids*" propose un catalogue de 45 mesures regroupées en 11 domaines. Son objectif est d'aider les acteurs des REI à identifier parmi les mesures proposées celles à mettre en œuvre pour gérer les risques qu'ils auront identifiés au travers d'une analyse de risques.

Le rapport du SG-CG/SGIS "*Smart Grid Information Security*" s'inscrit dans le cadre du mandat M/490 que la Commission européenne a adressé aux organisations de

[16] Le modèle de Purdue ou "Purdue Enterprise Reference Architecture (PERA)" a été développé dans les années 90 par Theodore J. Williams et des membres de "l'Industry-Purdue University Consortium" pour servir de référence Computer Integrated Manufacturing. Il sert donc de base à ce qu'on appelle usuellement la pyramide CIM et se trouve dans les standards, tels que l'ISA88 et l'ISA95, traitant de l'intégration des processus industriels.

Niveau	Désignation	Critères au regard de la stabilité du réseau européen
1	Très critique	Perte possible de plus de 10 GW – Incident pan-européen
2	Critique	Perte possible de 1 à 10 GW – Incident national ou européen
3	Elevé	Perte possible de 100 MW à 1 GW – Incident régional ou national
4	Moyen	Perte possible de 1 MW à 100 MW – Incident urbain ou régional
5	Faible	Perte possible de moins de 1 MW– Incident local ou urbain

Tableau 1 : Description des niveaux de sécurité proposés par le rapport « M/490-SGCG-SGIS ».

normalisation européennes pour supporter le déploiement des REI en Europe. Il s'appuie sur le SGAM et sur la notion de "Smart Grid Information Security-Security Levels (SGIS-SL)". Ces niveaux de sécurité, au nombre de cinq, sont établis de façon à refléter l'impact que peut avoir une défaillance sur la stabilité du réseau européen (tableau 1).

Le rapport analyse un ensemble de normes reconnues dans le domaine de la cybersécurité et en établit une cartographie en utilisant le SGAM en identifiant pour chacune de ces normes les îlots de l'architecture SGAM où leur application est pertinente.

De façon similaire, le rapport positionne dans un tableau de bord ("dashboard") les mesures proposées dans le rapport "*Proposal for a list of security measures for smart grids*" sur l'architecture SGAM en définissant pour chacune d'elles les îlots SGAM auxquels elles s'appliquent, avec trois niveaux de priorité fonctions du SGIS-SL.

Cette approche permet, pour un cas d'usage donné, de le modéliser en utilisant le SGAM, d'identifier grâce à une table de référence, le niveau de sécurité à retenir (SGIS-SL) pour ce cas d'usage, d'identifier les normes pouvant être utilisées et de définir des priorités dans le déploiement des mesures de cybersécurité à mettre en œuvre. Des exemples de cas d'usage sont donnés et une méthodologie en six étapes, un "framework", est proposé pour conduire de façon rationnelle une analyse de risques et pour définir le plan d'action pour y faire face.

Enfin ce rapport traite de la question de la protection de la vie privée qui est abordée à la section 2.5. du présent Livre blanc.

1.5. La réglementation aux Etats-Unis

Aux Etats-Unis, la Federal Energy Regulatory Commission (FERC) a désigné en 2007 la North American Electric Reliability Corporation (NERC) comme Energy Regulatory Office (ERO) en application de l'Energy Policy Act de 2005. En conséquence, les standards de fiabilité du NERC (CIP: Critical Infrastruture Protection) sont devenus obligatoires aux Etats-Unis. Ces standards qui traitent de la cybersécu-

- **CIP-001:** Covers sabotage reporting;
- **CIP-002:** Requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System;
- **CIP-003**: Requires that responsible entities have minimum security management controls in place to protect Critical Cyber Assets;
- **CIP-004:** Requires that personnel with authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness;
- **CIP-005:** Requires the identification and protection of the Electronic Security Perimeters inside which all Critical Cyber Assets reside, as well as all access points on the perimeter;
- **CIP-006:** Addresses implementation of a physical security program for the protection of Critical Cyber Assets;
- **CIP-007:** Requires responsible entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeters;
- **CIP-008:** Ensures the identification, classification, response, and reporting of cybersecurity incidents related to Critical Cyber Assets; and
- **CIP-009:** Ensures that recovery plans are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practice.

Tableau 2 : Les standards NERC-CIP (2015).

rité des réseaux de transport électriques sont actuellement au nombre de neuf et sont listés dans le tableau 2. Des standards additionnels sont en cours d'élaboration[17].1

1.6. Certification des réseaux électriques intelligents

Selon l'organisme d'accréditation français COFRAC, « La certification est une procédure par laquelle une tierce partie, l'organisme certificateur, donne une assurance écrite qu'un système d'organisation, un processus, une personne, un produit ou un service est conforme à des exigences spécifiées dans une norme ou un référentiel ».

La certification s'emploie abondamment dans le domaine de la sûreté de fonctionnement mais plus rarement encore dans le domaine de la cybersécurité.

L'ENISA a publié en décembre 2014 un rapport préliminaire sur la certification des REI en Europe1. Ce rapport contient des informations sur les différentes démarches de certification à travers l'Union européenne et formule des recommandations visant à la mise en place de pratiques harmonisées de certification de sécurité des réseaux intelligents. Le rapport souligne la nécessité de traiter le problème de certification dans la globalité de la chaine de conception, d'installation et d'exploitation des REI, y compris celle des constituants, afin d'atteindre le niveau de confiance recherché. La pluralité des intervenants et des constituants rend évidemment la tâche complexe.

Pour les prestataires de service, il existe en France un schéma de qualification des prestataires de confiance. La qualification atteste que le prestataire répond à un référentiel d'exigences. L'ANSSI délivre de telles qualifications pour des prestataires d'audit, prestataires de « cloud », prestataires de détection d'incidents de sécurité et prestataires de réponse aux incidents de sécurité. D'autres familles de prestataires compléteront la liste, en particulier dans le domaine des systèmes industriels. Les référentiels sont consultables sur www.ssi.gouv.fr . Ces référentiels peuvent également être appliqués aux équipes internes des industriels opérant des REI.

Les éventuels futurs schémas de certification pour les composants devront s'inscrire dans le cadre de l'accord reconnaissance mutuelle du SOG-IS (Senior Officers Group for Information Systems)[18] afin d'être reconnus au niveau européen par les signataires de cet accord.

[17] Pour connaitre le détail de la situation de chacun des standards CIP, se référer au site du NERC : http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[18] L'accord SOG-IS, mis à jour en 2010, est un accord de reconnaissance mutuelle des procédures d'évaluation de la sécurité des systèmes d'information fondées sur les critères communs. Les participants de cet accord sont des organisations gouvernementales ou des agences gouvernementales des pays de l'Union européenne ou de l'AELE (Accord européen du libre-échange) représentant leur(s) pays http://sogis.org/

Une première étape, très concrète, est de définir des cibles de sécurité ou profils de protection, décrivant pour un composant donné (Intelligent Electronic Device (IED), automate, disjoncteur, etc.), les objectifs de sécurité auxquels il doit satisfaire. De tels profils ont été récemment publiés par l'ANSSI3[19] pour des automates. Ces cibles permettent ensuite de procéder à une évaluation de la sécurité du composant, quel que soit le schéma de certification choisi.

L'identification des principaux composants d'un REI pourrait être menée dans le cadre de travaux ultérieurs puis complétée par la définition, pour chaque composant, d'un profil de protection en s'appuyant sur ceux publiés par l'ANSSI, issus du groupe de travail sur la cybersécurité des systèmes industriels.

De manière générale, les REI mettant en œuvre à la fois des systèmes de types industriels et d'information classique (IT), il semblerait essentiel de s'appuyer autant que possible sur un seul schéma de certification et une seule famille de normes ou standards. Le risque de mettre en œuvre des schémas spécifiques (industriel d'une part et IT d'autre part) est de ne pas couvrir correctement les interfaces entre les différents types de systèmes et de ne pas employer de méthode d'analyse de risques unifiée. Une approche de gouvernance par les risques permettrait de mettre en perspective de nouveaux développements à ce sujet.

2. Menaces, vulnérabilités et risques

2.1. Quelques définitions

La construction et la gestion d'un système de protection contre le risque cybersécuritaire font classiquement appel à trois notions complémentaires mais souvent confondues : les menaces, les vulnérabilités et les risques.

Une **menace** est une attaque possible d'un individu ou d'un élément naturel sur des biens (des composants, matériels ou logiciels, des données, un savoir-faire) entraînant des conséquences potentielles négatives. Les menaces sont caractérisées par une expertise de l'attaquant, ses ressources disponibles et sa motivation. Exemple : un développeur modifie le code source en vue de détournement de l'usage d'un compteur…

Une **vulnérabilité** est une caractéristique du système d'information, dans son ensemble ou au niveau de l'un de ses constituants, qui peut constituer une faiblesse de nature à permettre à une menace de se réaliser. Les vulnérabilités peuvent être organisationnelles (politique de sécurité incomplète…), humaines (manque de formation

[19] Voir www.ssi.gouv.fr/systemesindustriels.

des personnels…), logicielles ou matérielles (utilisation de produits peu fiables ou non testés…).

L'aboutissement d'une attaque provoque un impact qui peut être exprimé en perte de disponibilité, danger pour les hommes, détérioration de l'image de marque, perte financière ou autre, en fonction du contexte.

Les vulnérabilités internes, comme les menaces, peuvent être d'origine humaine. Par exemple un agent qui devient vulnérable, car mécontent de l'entreprise, peut, s'il fait l'objet de pressions sur sa personne, devenir une vulnérabilité du fait de son expertise et des droits qui lui ont été donnés.

Le **risque** est la combinaison de la probabilité de réalisation d'une menace avec la valorisation de l'impact qu'elle peut engendrer, c'est-à-dire la combinaison de la potentialité de l'exploitation d'une vulnérabilité par un élément menaçant avec l'impact qui peut en résulter.

2.2. Les menaces dirigées vers les REI

Le métier des opérateurs de réseaux a évolué de systèmes cloisonnés vers des systèmes connectés où la donnée doit être disponible pour différents sous-systèmes de l'entreprise où elle est traitée pour créer de la valeur. Ces interconnexions massives sont indissociables des technologies de l'information et de la communication (TIC). Mais il peut s'avérer que tout en apportant des améliorations significatives, la présence accrue des TIC ouvre la voie à de nouvelles menaces et génère de nouveaux risques Le sentiment est aujourd'hui partagé que la présence croissante des TIC conduit à une fragilité au sein des réseaux et une vulnérabilité face à des « cyberattaques » dont la diversité, l'ampleur et la technicité ne font que croître.

Les REI, en tant que systèmes de collecte et de traitement de l'information, sont sujets à toutes les menaces que l'on rencontre dans le domaine des TIC. Il serait vain de chercher à les énumérer et nous contenterons ici d'en citer quelques-unes qui peuvent prendre les REI comme cibles préférentielles. Ces menaces peuvent se combiner entre elles et conduire à des scénarios d'attaque complexes :

- détournement d'information en provenance ou en direction des compteurs communicants ;
- interception ou brouillage de communications sans fil en direction ou provenance des compteurs ou des IED ;
- accès distants non autorisés ;
- attaques non-invasives telles que l'analyse des radiations électromagnétiques émises par un équipement électronique isolé ;
- attaques de l'homme du milieu dans les chaînes de transmission de données ; manipulation d'information et altération de données ou d'instructions ; transmission d'informations erronées aux opérateurs et envoi de commandes corrompues vers les équipements ;
- attaques en déni de service (ICMP[20] ou autre), sur les équipements sensibles notamment et à différents niveaux ;
- attaques par canal auxiliaire sur différents équipements ;
- attaques par rejeu sur messages ;
- attaques utilisant les faiblesses de certains protocoles ou l'absence d'activation des mesures de sécurités, notamment sur les liaisons à distance et les liaisons sans fil ;
- attaques de stations opérateurs ou ingénieurs par harponnage ("spear phishing"), création de portes dérobées, injection de code malicieux (trojans, vers, virus, APT : advanced persistent threats…) ;
- attaques locales synchronisées ;
- etc.

2.3. Les vulnérabilités propres aux REI

Comme pour les menaces, beaucoup de vulnérabilités affectant les REI sont communes à tous les systèmes d'information. Cependant certains aspects particuliers doivent être soulignés. Jusqu'à présent, en effet, les centres de contrôle et les centres de calcul constituaient les principaux éléments sensibles d'un système électrique. Le déploiement de solutions décentralisées, dont le projet « Postes électriques intelligents » est une illustration, fait apparaître de nouvelles classes d'éléments critiques qui peuvent avoir à affronter de nouveaux types de menaces et s'y avérer vulnérables.

Au niveau de la production, il devient nécessaire de contrôler et de gérer des moyens de plus en plus nombreux répartis sur l'ensemble du territoire et de s'assurer en particulier de leur disponibilité.

Au niveau du transport et de la distribution, une attention particulière doit être portée aux postes électriques au fur et à mesure du déploiement de solutions numériques permettant d'améliorer la sécurité d'alimentation grâce à un échange d'information temps réel entre différents points du réseau. Quant à la gestion de la demande, elle implique les utilisateurs finaux et les équipements plus ou moins intelligents qui seront raccordés en aval des compteurs intelligents. Les équipements actifs des particuliers, commerces ou petites entreprises, capables de répondre à un signal externe par exemple pour ajuster automatiquement leur consommation – phase la plus aboutie de l'émergence du « consom'acteur »

[20] Les attaques ICMP (Internet Control Message Protocol) consistent à envoyer des paquets inoffensifs en très grand nombre dans le but de mettre hors-service une machine.

– doivent être également pris en compte dans l'analyse de risques. Des attaques a priori localisées sont susceptibles d'être reproduites à plus grande échelle si elles sont programmées pour se déclencher à un instant donné.

La gestion de la demande implique également les opérateurs des services d'effacement qui disposent en général d'une gestion centralisée permettant d'activer des effacements de consommation qui demain seront du même ordre de grandeur qu'un site de production nucléaire ou thermique. Une défaillance dans leur système est donc susceptible de provoquer un déséquilibre important du système électrique.

Les fournisseurs de service peuvent être à l'origine de nouveaux points de vulnérabilité du fait d'une part de leur recours à des solutions numériques très avancées et de leur impact potentiel sur les grands équilibres du système électrique et d'autre part de leur dépendance envers d'autres acteurs pour leur fournir connectivité et informations fiables pour prendre les décisions appropriées.

Sur un plan plus technique, se pose la question de la robustesse des réseaux de communication utilisés par les REI. Les cyberattaques résultent nécessairement d'une intrusion volontaire dans le système à un stade ou à un autre de son histoire. La sécurité des réseaux de communication est donc un point central. Certains réseaux ont été conçus à une époque où les problèmes de cybersécurité n'étaient pas à l'ordre du jour et peuvent présenter des vulnérabilités intrinsèques, notamment des faiblesses en termes d'authentification et de chiffrement permettant à des acteurs malintentionnés de dérouter les mécanismes demande/réponse (ou maître/esclave) à la base de ces protocoles pour les utiliser afin de collecter des informations sur la configuration ou sur l'état du système, d'exécuter des commandes non autorisées ou d'inonder les équipements par un flot de messages déclenchant un déni de service.

La plupart des protocoles sont des protocoles « de couche application » installés au-dessus des couches transport du modèle OSI (TCP ou UDP), ce qui ouvre la voie à la possibilité de véhiculer des commandes au travers de ports non standardisés ou d'injecter de façon subreptice via des ports officiels des commandes dans un trafic autorisé.

La migration vers des protocoles systématiquement basés sur IP peut être à l'origine de vulnérabilités accrues. Elle peut *a contrario* être l'occasion de repenser de bout en bout la cybersécurité de l'infrastructure de communication en assurant à tous les niveaux et pour tout type de communication (H2M, M2M) un contrôle des accès utilisant aussi bien les méthodes tirées du monde de l'information que celles du monde industriel.

Un autre point d'attention concerne les mécanismes de synchronisation horaire, s'ils devaient se développer dans les REI comme c'est le cas dans les réseaux de télécommunication. En effet, de récents articles ont mis en évidence un ensemble de vulnérabilités sur les protocoles tels que Network Time Protocole (NTP) utilisé pour synchroniser, via un réseau informatique, l'horloge locale d'un équipement sur une référence d'heure. Une attaque sur ce type de fonctionnalité pourrait alors probablement provoquer des perturbations importantes dans un REI.

2.4. Les risques encourus par les REI

L'aboutissement d'une attaque sur un REI peut avoir des conséquences de nature diverse. La première a trait à la mise hors service ou à l'altération du fonctionnement de certains équipements, y compris les systèmes d'alarme, dotés de capacités informatiques : compteurs intelligents, actionneurs télécommandés et autres IED, RTU, DMS (Distribution Management Systems), voire EMS (Energy Management Systems). Les conséquences de telles défaillances peuvent être plus ou moins importantes selon qu'elles conserveront un caractère local ou se propageront à l'ensemble du REI et, à l'extrême, à l'ensemble du réseau paneuropéen. La sévérité de ces incidents d'exploitation est reflétée par les cinq niveaux de sécurité proposés par le SG-CG/SGIS dans son rapport précédemment cité "*Smart Grid Information Security*" (tableau 1).

Un autre facteur essentiel d'appréciation du risque réside dans le délai de rétablissement du service. Une coupure du réseau électrique, quelle que soit son ampleur, ne sera pas vécue de la même façon selon qu'elle est brève ou prolongée. Aux côtés des mesures de protection, les mesures visant à faciliter l'identification des causes d'une défaillance et à permettre le rétablissement rapide du service constituent un élément essentiel d'un système de management de la cybersécurité des REI.

Un autre type de risque est celui de la fraude. La fraude la plus élémentaire est celle qui pourrait affecter les compteurs intelligents s'il était possible de manipuler les informations qu'ils collectent ou d'altérer les mécanismes de facturation. Un tel risque ne deviendrait critique que s'il était susceptible d'être reproduit à grande échelle.

Il faut enfin mentionner les risques sur la vie privée que fait courir l'accès par des personnes non autorisées aux informations utilisées par un REI et leur divulgation vers des destinataires qui n'ont pas à en connaître. Des études ont en effet montré que ces données peuvent être utilisées pour reconstruire tout ou partie de la vie privée des usagers : leurs habitudes, leurs heures de présence et

d'absence, leurs heures de travail et leurs heures de loisirs, etc. Aujourd'hui ce risque pourrait être associé à l'utilisation abusive des données en provenance des compteurs communicants et, dans une moindre mesure, des stations de recharge des véhicules électriques. Mais il pourrait à l'avenir prendre une ampleur plus importante avec l'extension au domaine de l'énergie des fonctionnalités des boxes. La protection de ces informations privées doit donc être assurée, même si leur divulgation éventuelle reste sans incidence sur le réseau, Des dispositions appropriées ont été prises sur les compteurs évolués comme Linky, suite aux recommandations de la CNIL, afin de maîtriser ce risque.

2.5 Construire la cybersécurité

Construire la cybersécurité d'un REI est un travail important qui doit s'appuyer sur une analyse aussi précise et lucide que possible des menaces, des vulnérabilités et des risques. De cette analyse, résultera un système de gestion de la cybersécurité qui exposera face aux risques ainsi encourus les dispositions prises pour les limiter (c'est la phase de « mitigation ») ou pour y faire face dans le cas où ils viendraient à se matérialiser.

Il n'est pas possible de décrire au niveau de ce Livre blanc le plan-type applicable à un REI ou à l'un de ses constituants. En effet, le cycle de vie à retenir dépend fondamentalement du rôle joué par le responsable considéré qui peut être l'opérateur du REI, un intégrateur, un fournisseur de composant, un fournisseur de services, un installateur, etc. Pour concevoir le système de gestion de la cybersécurité adapté à sa fonction, le responsable pourra s'appuyer sur un référentiel plus amont formé du corpus réglementaire applicable dans le pays considéré et des normes pertinentes dans le cas d'espèce parmi celles listées en annexe 1.

Dans tous les cas, un tel système de gestion de la cybersécurité devra traiter des grands sujets qui conditionnent la confiance que l'on peut porter à un système ou à l'un de ses constituants et en particulier des trois domaines-clés identifiés par la norme générique ISO/CEI 27001 : disponibilité, intégrité, confidentialité, qui doivent être complétés par la traçabilité et la non-répudiation des actions ainsi que par la « privacité » ou respect de la vie privée.

• ***Disponibilité***

Un REI devant répondre à des exigences de fonctionnement en temps réel, la disponibilité est une propriété fondamentale à assurer. Les menaces visant la disponibilité sont nombreuses, depuis les attaques physiques contre les objets connectés jusqu'aux attaques en déni de service visant le système d'information, en passant par les attaques contre l'infrastructure de communication. Ces attaques peuvent être d'origine interne aussi bien qu'externe.

• ***Intégrité***

Les attaques en intégrité peuvent cibler divers composants du REI et avoir des objectifs variés. La modification illicite de données peut conduire à des facturations erronées, à un fonctionnement anormal des actionneurs. La modification de composants du système (contrôleurs et calculateurs, etc.) peut quant à elle conduire à un fonctionnement anormal, masquant notamment les alarmes ou alertes éventuelles, etc.

Il convient également de prendre en compte l'intégrité de l'information remontée. Une information fausse, ou dont la transmission est retardée, peut également induire des déséquilibres importants avec un faible effort de la part de l'attaquant. Il est possible de faire un parallèle entre cette situation et celle du routage dans le réseau Internet

• ***Confidentialité***

L'interception d'informations critiques, telles que des codes d'accès ou des clés de chiffrement, peut permettre une intrusion dans les réseaux de transfert d'informations et le développement d'attaques « homme du milieu » avec des conséquences opérationnelles très graves. Il en va de même pour les données de traçage collectées qui doivent rester impérativement confidentielles.

• ***Traçabilité et non-répudiation des actions***

Enfin, en complément des trois aspects principaux évoqués ci-dessus, il convient également, d'aborder, dans le cas des REI, la question de la traçabilité et de la non-répudiation (également cités par la norme ISO 27001). En effet, chaque acteur émet et reçoit des informations des autres acteurs. Il traite ces informations en fonction de sa politique interne. Il peut avoir intérêt à ne pas fournir certaines informations à l'extérieur ou ne pas avoir la possibilité de vérifier les informations reçues.

Il est important pour pouvoir piloter un réseau en temps réel et, s'il y a lieu, procéder aux investigations nécessaires en cas d'incident, de disposer des données nécessaires et de s'assurer de leur origine.

• ***« Privacité »***

Dans le cas du réseau REI, une préoccupation d'une autre nature que celles qui précèdent doit être prise en compte : la protection de la vie privée, mentionnée précédemment dans la section consacrée aux risques et que nous désignons par le néologisme de « *privacité* ». Les données collectées par les objets connectés peuvent en effet être sensibles du point de vue de la « privacité », c'est-à-dire de la protection des données à caractère personnel.

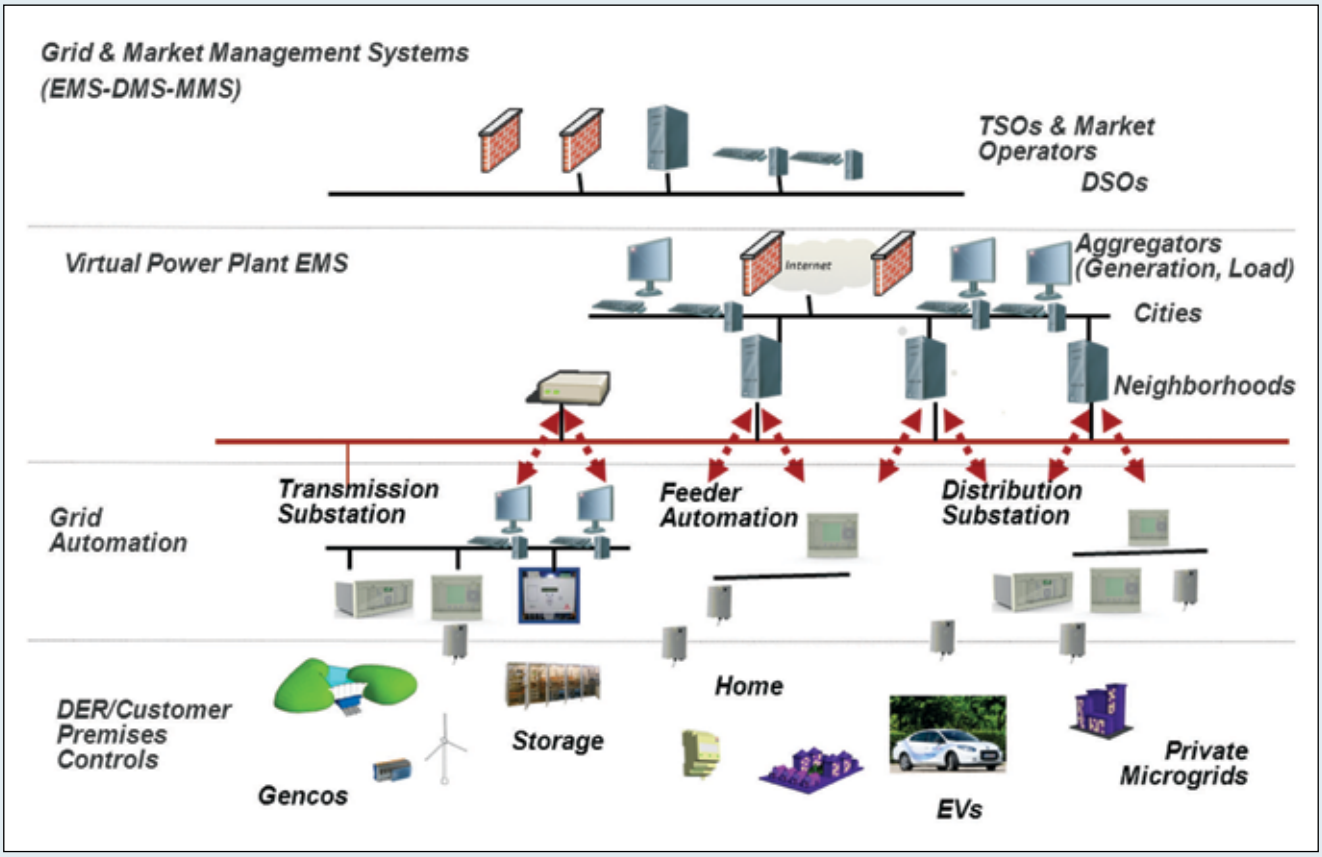

Figure 3 : Schéma-type d'un réseau électrique intelligent – Source : Alstom Grid.

Cette question est abordée en détail dans le rapport du SG-CG/SGIS "*Smart Grid Information Security*" précédemment cité. Elle est traitée au niveau européen dans le cadre de la "*General Data Protection Regulation (GDPR)*"[21] en cours d'élaboration par les instances européennes et qui se substituera à la Directive 95/46/EC. Ce règlement, susceptible d'être approuvé en 2015, s'imposera aux Etats membres et impactera toutes les entreprises collectant, gérant, ou stockant des données et aura pour but principal de simplifier et harmoniser la protection des données dans les 28 pays de l'Union européenne.

Ce texte aura un impact sur les REI, dans la mesure notamment où il visera à promouvoir un marché européen unique dans le domaine des REI et de leurs constituants. Aujourd'hui, les deux principaux segments concernés sont ceux des compteurs communicants et des systèmes de gestion des véhicules électriques. A l'avenir, la généralisation du concept de bâtiment intelligent générera de nouvelles sources de données qui devront être protégées.

3. De la cybersécurité des installations industrielles à celle des REI

Les REI constituent une variété de systèmes industriels. A ce titre, beaucoup de dispositions, réglementaires, normatives ou techniques, qui sont applicables aux installations industrielles trouvent leur place dans le domaine des REI. Toutefois les REI présentent des particularités qui les différencient des systèmes industriels et appellent sur certains aspects une approche spécifique.

Les REI, comme l'illustre la figure 3, regroupent des équipements et sous-systèmes de toute nature et manipulent un ensemble de données hétérogènes. Ils mettent en œuvre pour cela des moyens de communication s'appuyant sur des réseaux de communication, publics ou non, et sur des systèmes de traitement et de stockage de l'information importants et performants.

La dynamique des procédés électriques est rapide, typiquement le ¼ de période (5 ms), comparable à celle des

[21] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012PC0011&from=en

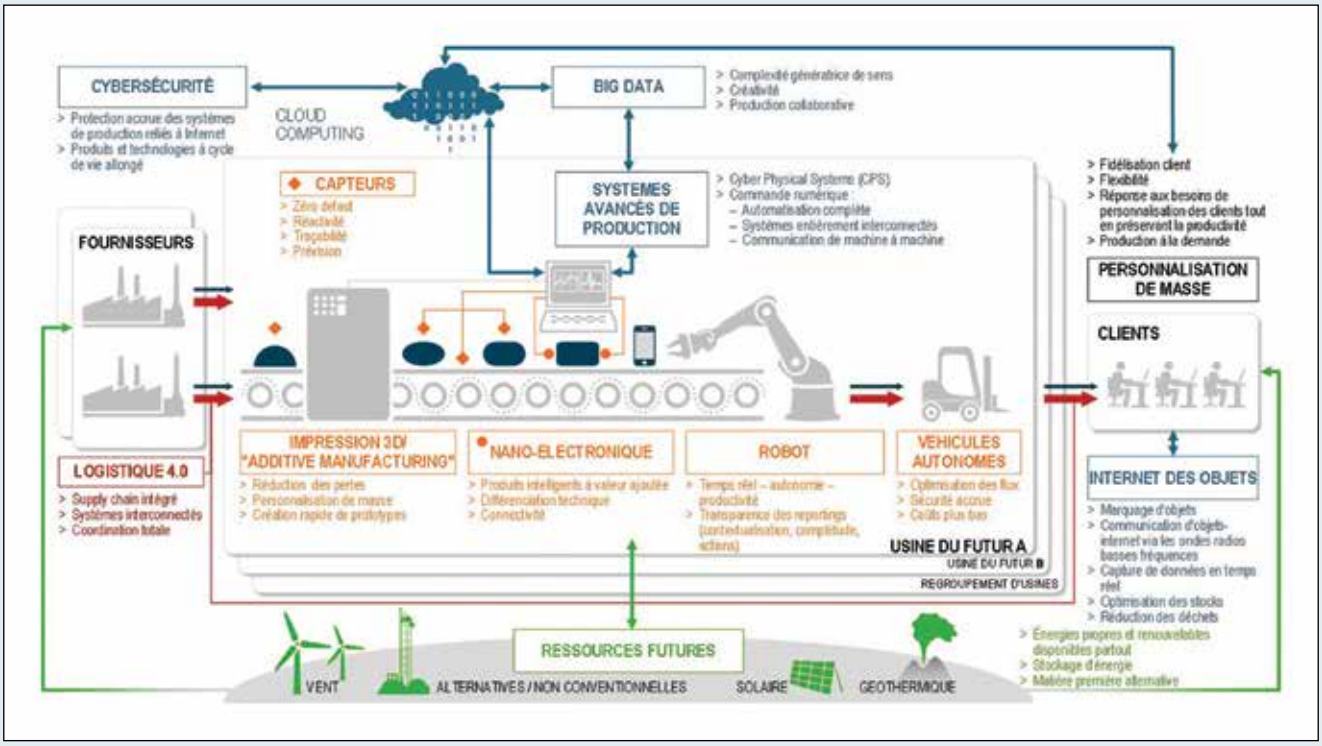

Figure 4 : Le concept d'Industrie 4.0 – Source : Industrie 4.0 – Les leviers de la transformation – Gimelec (septembre 2014).

systèmes d'automatismes et de contrôle industriel (IACS)[22] dits « temps réel » ou « temps critique », mais moins exigeante cependant que celle de procédés plus rapides tels que la métallurgie ou l'imprimerie.

Les REI utilisent des contrôleurs et des calculateurs similaires à ceux de l'industrie avec des consoles de programmation et des stations de supervision. Ils s'appuieront également de plus en plus sur des technologies issues du monde de l'informatique – telles que le *cloud computing*, les *big data* ou encore l'*Internet des objets (IoT)* – auxquelles l'industrie a, elle aussi, de plus en plus recours.

Les REI s'apparentent donc aux futures « usines intelligentes » qui constituent le cœur de « l'Industrie 4.0 »[23] (figure 4). L'utilisation abondante des nouvelles technologies et la mise en réseau des sous-systèmes constitutifs peuvent fragiliser la résilience d'un tel système.

Les problématiques sont également similaires à celle des IACS puisqu'une perte d'intégrité des données ou leur indisponibilité peut entraîner des défaillances importantes.

Une différence majeure réside cependant dans le fait qu'une usine dispose d'un périmètre physique bien maîtrisé et contrôlable, ce qui paraît hors de portée pour des REI déployés à l'échelle d'un pays comme la France. Les REI associent un très grand nombre d'acteurs, plus de 30 millions de consommateurs dans le cas du réseau de distribution, et ce périmètre est quotidiennement évolutif et il est impossible d'en assurer à tout instant la protection rapprochée. Cette remarque conduit, dans le cas des REI, à s'interroger sur les limites de la défense périmétrique qui reste, avec la défense en profondeur, à la base de la cybersécurité des installations industrielles.

Par ailleurs, si les REI peuvent être vus comme une architecture intégrée, ils sont en fait des « **systèmes de systèmes** » comme le montre le modèle du SGAM. Les systèmes élémentaires, ou sous-systèmes, sont interconnectés entre eux ; ils échangent des informations mais n'ont pas pour autant besoin de les partager toutes. Il existe donc une certaine autonomie au niveau de chaque sous-système, autonomie qui a vocation à devenir totale, au moins de façon temporaire, en cas de marche dégradée. Ces sous-systèmes sont de nature très différente : ils vont des grands systèmes informatiques constitutifs des EMS jusqu'à l'îlot

[22] IACS : Industrial Automation and Control Systems – Cette notion inclut les SCADA dédiés au contrôle d'installations distantes via des RTU (Remote Terminal Units).

[23] Le concept d'Industrie 4.0 correspond à une nouvelle façon d'organiser les moyens de production : l'objectif est la mise en place d'usines dites « intelligentes » (« smart factories ») capables d'une plus grande adaptabilité dans la production et d'une allocation plus efficace des ressources, ouvrant ainsi la voie à une nouvelle révolution industrielle. Ce concept est né en Allemagne et est à présent promu en France par de grands industriels et par l'organisme professionnel du GIMELEC.

local que constitue un compteur communicant et un équipement de consommation finale qui lui est raccordé. Chacun de ces sous-systèmes peut être analysé selon la grille classique des systèmes d'automatisme, en y distinguant les différents niveaux du modèle de Purdue mais l'ensemble du système est d'un degré de complexité supérieur.

D'autres différences tiennent à la non-adaptation de certaines mesures de protection classiques, notamment celles qui sont directement transposées du monde des systèmes d'information. Par exemple des procédures de chiffrement ou d'authentification complexes pourront s'avérer trop lourdes, au regard de la taille des équipements ou de la dynamique exigée. Les protocoles IPsec, utilisés notamment pour réaliser des réseaux privés virtuels (VPN), pourront s'avérer trop lourds à certains niveaux de l'architecture. Il pourra en aller de même des dispositifs évolués de pare-feu (dotés de l'inspection en profondeur des trames) et a fortiori des plates-formes de sécurité mises à jour en temps réel et associant divers critères de détection.

La miniaturisation de ces solutions nouvelles de protection, afin de les rapprocher de plus en plus des équipements à protéger, et l'assurance de leur mise à jour en temps réel sans arrêt du service, constitue l'un des défis importants de la recherche-développement.

4. Les mesures de protection

4.1. Aperçu général

Pour faire face aux menaces qui pèsent sur les REI et aux risques qui s'ensuivent, il existe deux grandes familles de mesures de protection :

- **les mesures d'ordre technique**, comportant des aspects structurels (architectures, protection des îlots d'automatisme, protection des réseaux de communication) et des aspects technologiques (cryptographie, authentification & identification, sécurité des logiciels, surveillance temps réel) ;
- **les mesures d'ordre organisationnel**, correspondant à ce qu'on appelle dans le jargon normatif international « *les policies and procedures* », y compris « *l'hygiène cybersécuritaire* ».

Nous aborderons tout d'abord les solutions d'ordre technique, en mettant l'accent sur les points particuliers propres aux REI et donc sans la prétention de dresser un catalogue exhaustif des protections susceptibles d'être mises en œuvre. Nous distinguerons les mesures ayant trait à l'architecture – que l'on peut qualifier comme relevant de la "security by design" –, celles relatives à la protection des sous-systèmes ou « îlots d'automatisme », celles relatives à la sécurisation des réseaux avant de donner quelques coups de projecteur sur quelques technologies-clés.

Nous aborderons ensuite les mesures organisationnelles.

Quelles que soient les mesures considérées, il doit être souligné que les protections ou contremesures ne doivent pas porter atteinte à la disponibilité et aux performances du système ce qui, comme on l'a vu dans la section qui précède, peuvent rendre inappropriées certaines mesures d'emploi courant dans le domaine de l'informatique de gestion voire des systèmes industriels.

4.2. La sécurisation des architectures

4.2.1. La "security by design" et la défense en profondeur

La plupart des systèmes d'information sont fondés sur une architecture qui a été définie pour des raisons fonctionnelles et sur laquelle des primitives ou fonctions de sécurité ont été implantées : on retrouve ainsi la protection périmétrique (empêcher les intrusions avec des sas, pare-feux, anti-virus, etc.) assortie d'un dispositif de surveillance par des IPS (Intrusion Prevention Systems), des IDS (Intrusion Detection Systems) ou d'autres dispositifs. On peut également assimiler à ce type de protection, les systèmes dits « multi-barrières » consistant en une protection périmétrique utilisant des approches et des matériels indépendants.

Initialement développées dans un contexte militaire pour assurer la confidentialité des informations, des architectures « en couches » ont également été développées pour permettre une défense en profondeur. L'idée de base est qu'une couche traite des informations d'un niveau de classification donné et que la communication entre les couches est soit interdite, soit strictement contrôlée (diodes logicielles ou matérielles). Ce type d'architecture se retrouve dans les IACS avec généralement un cœur de système de pilotage supposé totalement déconnecté et validé.

Dans le cas des REI, ces approches, si elles demeurent pertinentes, ne peuvent plus être considérées comme suffisantes. Elle sont en effet battues en brèche par l'élargissement considérable de la surface d'attaque des systèmes due principalement à leur extension et à leur décentralisation, par l'augmentation de la compétence des attaquants, par le ciblage de plus en plus précis des attaques et enfin par l'accroissement des moyens à disposition des attaquants.

L'architecture des REI, architecture de système de systèmes, est fondée sur des sous-systèmes ou îlots d'automatismes, reliés entre eux par des réseaux, situés soit à la tête du REI, soit près du terrain, soit aux niveaux intermédiaires, correspondant à des niveaux de criticité variables selon leur positionnement.

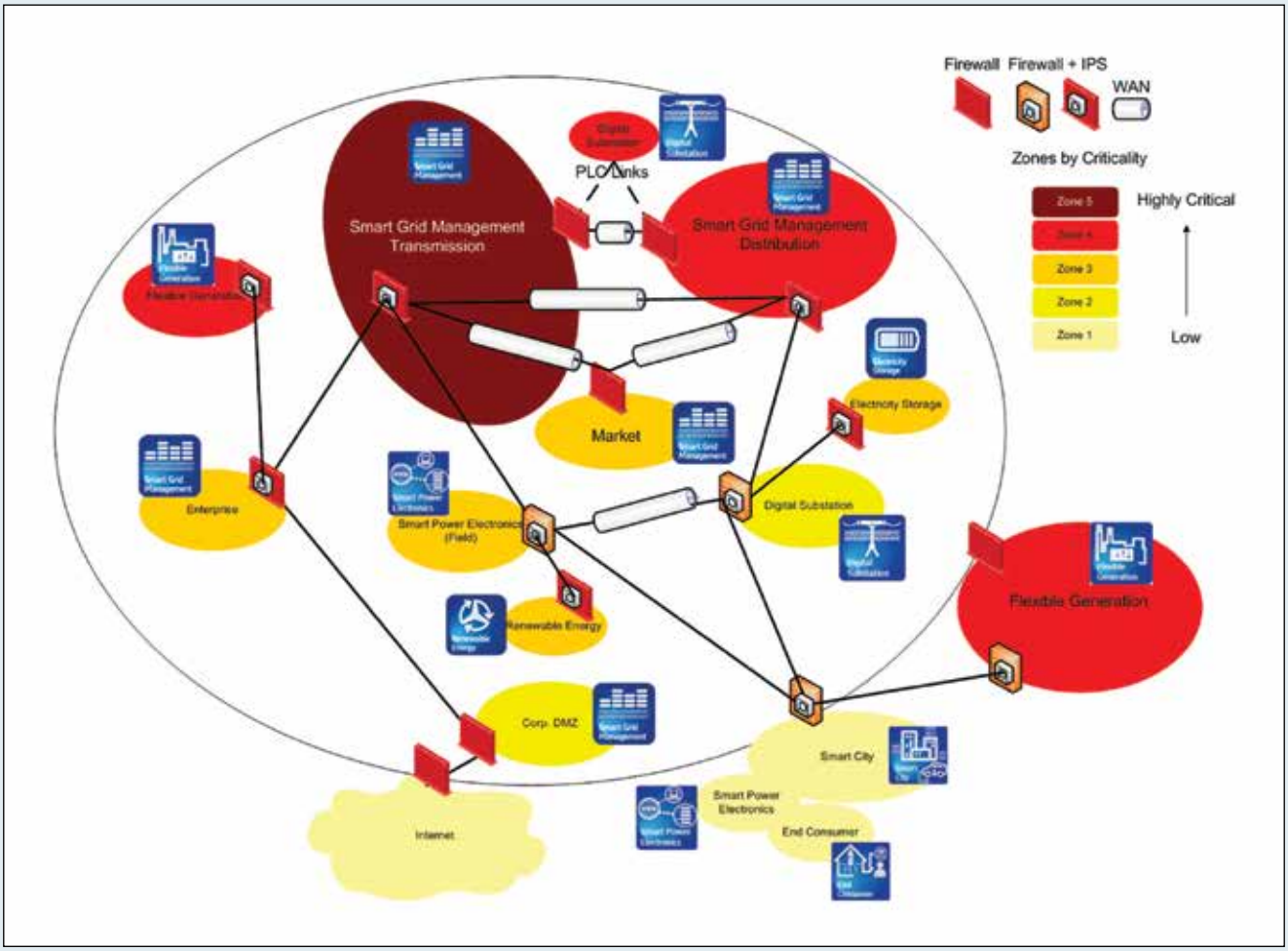

Figure 5 : Architecture REI avec différents niveaux de sécurité – Source : Alstom Grid.

Cette problématique appelle des solutions nouvelles, pour partie héritées des architectures classiques des IACS et pour partie fondées sur des concepts nouveaux.

La cybersécurité des REI peut ainsi se concevoir suivant une approche à deux niveaux :

Dans un premier temps, il est vital de renforcer la sécurité des îlots principaux c'est-à-dire des sous-systèmes constitutifs des nœuds du réseau. La forte connectivité de ces nœuds avec le monde extérieur ainsi que leur forte numérisation, telles que celles des sous-stations électriques numériques, les rendent vulnérables aux attaques informatiques. Ces nœuds sont similaires à des IACS, présentant les caractéristiques habituelles de ces systèmes : contraintes de sûreté de fonctionnement, d'environnement « non informatique » et de « temps réel » en exigeant des temps de réponse rapides (l'ordre de grandeur des trames Goose[24] véhiculant des asservissements dans les sous-stations est de quelques millisecondes).

[24] Les "gooses" (Generic Object Oriented Substation Events) sont, comme décrit dans le standard IEC 61850, des types de trame mises en œuvre pour assurer les asservissements d'équipements électriques des sous-stations.

Dans un deuxième temps, il est nécessaire de sécuriser les moyens de communication entre ces nœuds afin de garantir l'intégrité, la disponibilité et, pour certaines d'entre elles, la confidentialité des données échangées. Les mécanismes classiquement utilisés dans le domaine de la sécurité des systèmes d'information peuvent être utilisés mais il faut s'assurer qu'ils répondent à la demande. De nouvelles méthodes pour contrôler et valider les échanges apparaissent aujourd'hui. Elles sont encore « à la limite de la recherche-développement » et sont résumées à la fin de cette section.

Le challenge réside dans le découpage et la définition du périmètre des systèmes et sous-systèmes constituant les REI afin de délimiter les domaines de responsabilités mais aussi les exigences et les objectifs à atteindre en fonction des risques propres à chaque système. Tous les systèmes de contrôle composant les îlots n'appellent pas les mêmes niveaux de criticité. Il est important d'adapter les mesures aux enjeux en classant les systèmes en fonction des risques.

Le recours au modèle SGAM et à la méthodologie proposée par le SG-CG/SGIS permet d'apporter de la rationa-

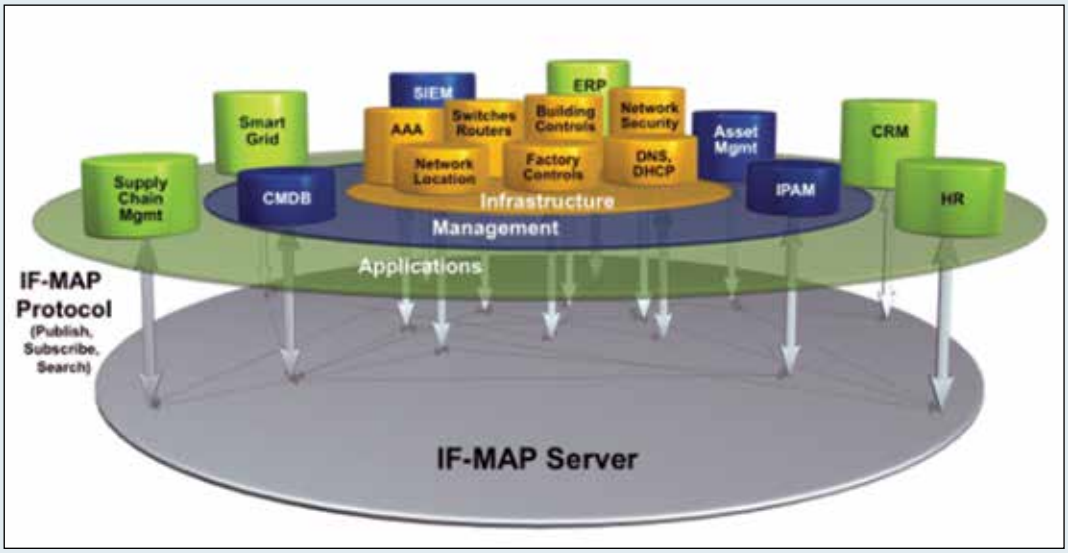

Figure 6 : Le serveur IF-MAP agrège automatiquement, corrèle et distribue les données en provenance ou à destination des différents sous-systèmes – Source : TCG.

lité à l'analyse. Si l'on adopte les cinq niveaux de sécurité proposés par ce groupe de travail, il est possible de réaliser un mapping tel que celui de la figure 5 entre les principaux constituants d'un REI et ses cinq niveaux.

Les travaux menés autour de la cybersécurité des systèmes industriels comme les guides de recommandations publiés par le groupe de travail piloté par l'ANSSI apportent[25] une aide précieuse pour la détermination des mesures de protection à mettre en place, notamment au niveau de la méthode retenue pour une analyse approfondie des risques encourus suite aux menaces et vulnérabilités identifiées.

Le guide cybersécurité des systèmes industriels[26] « Méthode de classification et mesures principales », propose une méthodologie pour cela. Ses recommandations peuvent d'ores et déjà être testées sur les différents démonstrateurs nationaux de REI et notamment ceux dédiés aux stations électriques.

Une vision standardisée de telles installations est cependant illusoire et chaque cas doit faire l'objet d'une analyse spécifique. Le processus d'homologation[27], préconisé, voire imposé dans les démarches habituelles de cybersécurité des systèmes d'information (classiques et industriels) ne semble pas approprié à l'échelle d'un REI. En revanche, il peut être appliqué au niveau des sous-systèmes contrôlant les nœuds des réseaux. Le recours à des produits et services certifiés[28] (au sens de la cybersécurité) apportera des garanties supplémentaires quant au niveau de sécurité des systèmes opérés. Celles-ci apparaissent indispensables compte tenu de la complexité du sujet.

4.2.2. Orientations nouvelles

Récemment sont apparues des solutions de *gestion des événements et des informations de sécurité* (en anglais "Security Information and Event Management" : SIEM) destinées à collecter des données à partir des équipements, réseaux et applications puis à les corréler. Ces plates-formes hautement sécurisées identifient les risques et les menaces par l'analyse de données internes et externes et à partir des informations qu'elles collectent.

D'autres solutions introduisent la notion de système intrinsèquement sûr, c'est-à-dire intégrant des primitives de contrôle d'intégrité avec une vérification permanente. L'exemple le plus connu est sans doute celui des architectures proposées par le Trusted Computing Group[29] utilisant le protocole IF-MAP (Interface for Metadata Access Points).

Dans cette architecture, les communications sont gérées par un serveur IF-MAP qui collecte toutes informations rela-

[25] http://www.ssi.gouv.fr/systemesindustriels

[26] http://www.ssi.gouv.fr/IMG/pdf/securite_industrielle_GT_methode_classification-principales_mesures.pdf

[27] L'homologation permet à un responsable d'attester aux utilisateurs d'un système d'information que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés. Il s'agit d'un préalable à l'instauration de la confiance dans les systèmes d'information et dans leur exploitation.

[28] Des certifications de produits et de prestataires de service sont délivrées en France par l'ANSSI. http://www.ssi.gouv.fr/fr/certification-qualification/ Au moment où ce Livre blanc est écrit, des travaux sont en cours pour étendre ces certifications au monde industriel : PLC, IED, disjoncteurs, etc. pour les produits et prestataires d'intégration et de maintenance pour les prestataires de service.

[29] Le Trusted Computing Group est une organisation à but non lucratif dont l'objet est de développer et promouvoir des standards industriels ouverts neutres commercialement permettant de réaliser des architectures de confiance interopérables – http://www.trustedcomputinggroup.org

tives à la sécurité et autorisent les transactions en fonction des droits de chacun et des informations dont il peut disposer (figure 6).

Chaque équipement est doté d'un module, dénommé Trusted Platform Module (TPM) qui est un composant cryptographique matériel réputé inattaquable solidaire de l'équipement et par exemple soudé sur la carte mère, dans lequel sont stockés de façon passive tous les éléments relatifs à la sécurité tels que les clés de chiffrement. L'idée de base est d'avoir un contrôle d'intégrité permanent reposant sur l'utilisation de primitives cryptographiques (signatures, fonctions de hachage) dont les éléments critiques sont stockés dans ce module de confiance inattaquable (ou difficilement attaquable). Des actions de recherche sont en cours pour intégrer à cette approche une vérification de l'intégrité hardware (par exemple dans le projet européen Holistic Approaches for Integrity of ICT-Systems – HINT : http://www.hint-project.eu).

Le but ultime est de transformer les REI en une sorte de réseaux sociaux dont les membres peuvent dialoguer entre eux, sans qu'il y ait aucun doute sur leur identité, sans que les messages soient altérés et dans le respect des règles fixées pour le dialogue entre abonnés.

4.3. La sécurisation des îlots d'automatisme

4.3.1. Généralités

Nous avons vu que les îlots d'automatisme étaient localisés à différents niveaux de l'architecture (figure 3). Leur criticité et donc le niveau de sécurité à leur assurer varie selon le rôle qui leur est assigné. On peut cependant définir pour chacun d'eux une méthodologie d'analyse cybersécuritaire fondée sur des principes communs qui sont ceux applicables aux IACS, sachant que seules devront être retenues les notions pertinentes au regard des fonctionnalités assurées.

Chaque système d'automatisme équipant ces îlots peut être divisé en quatre niveaux, en s'inspirant du modèle de Purdue. Tous les niveaux ne sont pas nécessairement présents dans chaque îlot d'automatisme :

- le niveau 4 est le niveau « entreprise » qui connecte différents sites. Ce niveau intègre le système de gestion de l'entreprise et de ses usagers ;
- le niveau 3 est le niveau de gestion de l'unité opérationnelle. Il comprend le système de supervision global et de prise de décision ;
- le niveau 2 supporte les fonctions de contrôle. Il permet de contrôler et de superviser les procédés opérationnels ;
- le niveau 1 est le niveau de terrain. Il comprend l'ensemble des objets connectés de type capteurs et actionneurs.

Le système doit être décomposé en sous-ensembles (appelés zones de sécurité ou sous-systèmes) correspondant à des fonctionnalités données et donc homogènes sur le plan des exigences de sécurité. Ces exigences de sécurité sont définies en fonction des impacts que provoquerait une atteinte à l'intégrité, à la disponibilité ou la confidentialité sur le fonctionnement de la zone ou du sous-système considéré.

Un sous-système correspond rarement à un seul niveau. Il est en effet difficile de dissocier les capteurs et actionneurs (niveau 1) de l'automate (niveau 2) qui assure les asservissements. Dans certains cas, le sous-système comporte des éléments situés au niveau 3, tels que l'émission d'ordre de commande, dont la compromission provoquerait des dégâts importants sur le sous-système.

Le découpage d'un îlot d'automatismes en sous-systèmes est une étape souvent complexe, où les erreurs sont fréquentes. Il est important d'être vigilant sur cette étape. Les mesures de sécurité à déployer dépendent du niveau mais le besoin de sécurité porte bien sur l'ensemble du sous-système et sur la fonction (ou service) qu'il assure. Les normes et guides (cf. annexe 1) pourront apporter une aide utile quant à la définition de ces mesures.

D'une façon générale, on peut considérer que les niveaux 3 et 4 posent des problèmes de sécurité "classiques" de systèmes d'information d'entreprise. Les mesures de sécurité qui en découlent, doivent, sous réserve d'une analyse de risques, intégrer les fonctionnalités suivantes :

- contrôle d'accès des utilisateurs :
  - authentification des utilisateurs autorisés à accéder au système d'information, y compris des usagers ;
  - gestion des autorisations des utilisateurs en fonction de leurs rôles dans le système d'information et des règles de séparation des tâches,
- filtrage des communications du réseau d'entreprise et des réseaux de production via le déploiement de pare-feux sur IP et configuration de ces pare-feux conformément à la politique d'entreprise ;
- supervision pour détecter les intrusions contre le réseau d'entreprise et les réseaux de production via le déploiement de systèmes de détection et de prévention des intrusions (IDS et IPS) ainsi que de gestion des événements de sécurité (SIEM) ;
- journalisation des événements de sécurité et de gestion des alarmes de sécurité ;
- mise en œuvre de protocoles permettant de protéger les communications avec les utilisateurs distants via l'ouverture de VPN.

Le niveau 2 pose des problèmes de sécurité spécifiques aux systèmes industriels de type « IACS ». Les mesures de

sécurité à ce niveau doivent en conséquence intégrer les fonctions suivantes :

- contrôle d'accès des utilisateurs et gestion de l'authentification et des autorisations ;
- filtrage des communications du réseau de commande/contrôle via le déploiement de pare-feux de filtrage des protocoles utilisés ;
- supervision pour détecter les intrusions contre le réseau de contrôle commande via des IDS et des IPS dédiés et remontée des événements de sécurité vers des SIEM dédiés aux réseaux de contrôle commande ;
- journalisation des événements de sécurité et de gestion des alarmes de sécurité.

Le niveau 1 concerne les réseaux de terrain qui relient l'ensemble des objets connectés. Les mesures de sécurité à ce niveau doivent intégrer les fonctions suivantes :

- contrôle d'accès aux objets connectés notamment pour contrôler les procédures de mises à jour des configurations des capteurs et des actionneurs ;
- filtrage des communications entre le système de commande contrôle et les objets connectés via le déploiement de pare-feux de filtrage des protocoles du réseau de terrain ;
- supervision pour détecter les intrusions contre le réseau de terrain et les objets connectés via des IDS et des IPS dédiés et remontée des événements de sécurité vers les SIEM du système de contrôle commande ;
- sécurité pour contrôler l'insertion ou le retrait d'un objet connecté dans le réseau de terrain ;
- chiffrement des données émises par les capteurs dans le cas où ces données sont sensibles ;
- redondance des fonctions pour assurer la disponibilité du réseau de terrain en cas de défaillance des communications principales ou des objets connectés.

Il est important de souligner que les mesures de sécurité des niveaux 1 et 2 se trouvent aujourd'hui renforcées car des besoins d'échange de plus en plus importants sont apparus entre ces niveaux et les niveaux 3 et 4 de l'architecture. Il est souhaitable qu'à l'avenir les niveaux 1 et 2 les plus critiques soient basés sur une architecture intrinsèquement sûre de type « Trusted Computing » intégrant un contrôle d'intégrité et d'authenticité renforcé.

4.3.2. Le cas des installations terminales

Les installations de domotique ou de « maisons intelligentes » vont jouer un rôle important dans la gestion de l'énergie à domicile. En effet, outre la télérelève des compteurs permettant d'assurer un suivi de la consommation, d'autres équipements télécommandés installés au domicile permettront d'ajuster la consommation à la variabilité des tarifs à venir et aux éventuels pics de consommation zonés et d'intervenir dans les mécanismes d'effacement des agrégateurs équivalents à une extension dynamique du système heures creuses.

Ces divers équipements seront connectés soit au compteur communicant installé par le distributeur, Linky dans le cas d'ERDF et des équivalents pour les entreprises locales de distribution (ELD), pour réagir automatiquement à des plans tarifaires spécifiques, soit à des boxes installées par les fournisseurs d'accès à Internet (FAI) ou à des points d'accès dédiés connectés au réseau Internet. C'est au travers de ce type de connexion que les agrégateurs d'effacement constitueront leurs « blocs» qu'ils valoriseront par ailleurs auprès des fournisseurs ou sur les marchés.

Concernant la télérelève des compteurs, il est d'ores et déjà possible techniquement de connecter un lecteur d'index positionné sur les compteurs électroniques et de remonter au rythme souhaité des informations de consommation globale au travers d'Internet.

Bien évidemment, ces dispositifs doivent faire l'objet d'un maximum de précautions afin d'éviter de nouvelles formes d'attaques : intrusion sur les réseaux, manipulation

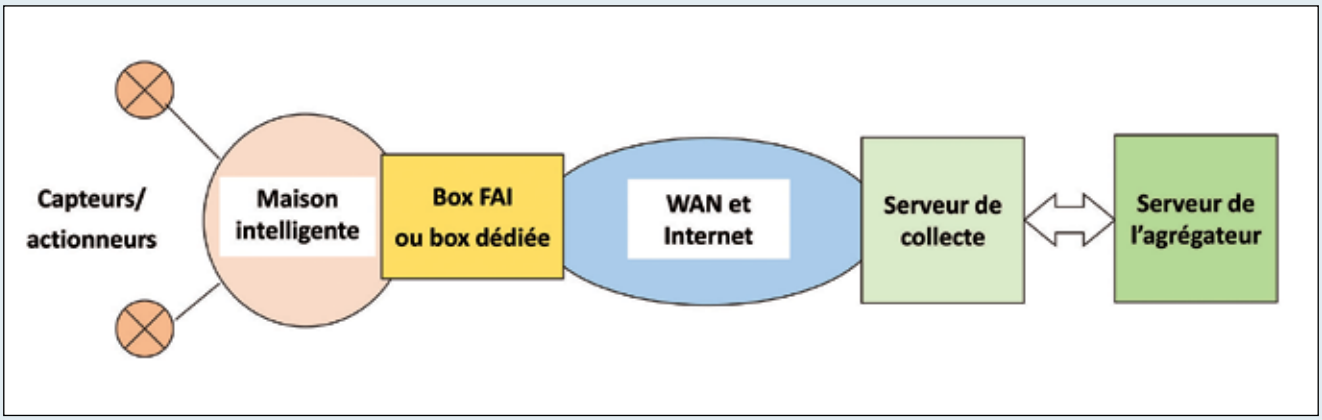

Figure 7 : Chaine de transmission des données au travers d'une box FAI ou d'une box dédiée.

En France, l'arrêté de 4 janvier 2012 prévoit que les dispositifs de comptage évolué doivent être conformes à un référentiel de sécurité certifié par l'ANSSI. Le compteur communiquant Linky installé par ERDF, est conforme à ce référentiel.

Les recommandations de la CNIL et de la CRE[1] ont également été prises en compte lors de la concertation sur les spécifications du compteur. Des règles strictes ont été établies concernant la précision des mesures enregistrées, la durée de stockage des données, les règles de communication à des tiers et la protection de l'ensemble du système.

Les principes de base qui sous-tendent l'architecture du système Linky sont les suivants :

- les informations sont et demeurent la propriété du consommateur ;
- elles ne peuvent être communiquées à des tiers sans l'accord du consommateur ;
- les courbes de charge ne peuvent être calculées à un pas de temps inférieur à 10 minutes.

Le système Linky intègre un très haut niveau de sécurité :

- au sein du Programme Linky, une équipe est totalement dédiée à la sécurité (SI, matériel et télécommunications) ;
- la protection du système se situe à la fois au niveau du compteur, du concentrateur et du système d'information centralisé :
  - les données qui circulent dans le système d'information Linky font l'objet d'un chiffrement dès leur envoi, et ce sur toute la chaîne. Le système de chiffrement intègre les technologies les plus modernes ;
  - des pare-feux protègent chaque brique du système d'information Linky de toute intrusion ;
  - les serveurs du Système d'Information Linky sont placés dans des zones de sécurité (ZSE), espaces dédiés et protégés, avec restriction d'accès et système d'authentification.
  - les terminaux mobiles servant à programmer les différents éléments clés de la protection du système, comportent des certificats d'authentification ou des clés de chiffrement mis à jour régulièrement.

[1] CNIL : Commission Nationale Informatique et Liberté – CRE : Commission de Régulation de l'Energie.

Encadré 1 : Sécurisation du système de compteurs communicants Linky.

d'équipements à distance ("botnets") et de façon coordonnée, par exemple en déni de service.

En ce qui concerne les communications depuis les boxes des FAI ou des agrégateurs vers les équipements participants au pool d'effacement, un niveau particulier de sécurité doit être assuré dans la remontée des données même si ce n'est pas sur la base de ces éléments que la facturation annuelle et contractuelle est établie.

Les mécanismes de sécurité mis en œuvre dans ce cas sont :

- l'identification et l'authentification certifiée des capteurs/lecteurs d'index par le serveur de collecte ;
- le chiffrement des échanges de données entre le capteur et le serveur de collecte sécurisé situé dans le réseau internet. La « box » FAI est alors transparente à ce chiffrement ;
- la reconnaissance par la « box » du serveur de collecte l'autorisant à dialoguer avec le capteur qui lui est raccordé.

Ces mécanismes associés à des mécanismes de « caches » en cas de rupture de communication permettent de fournir un service fiable de suivi de consommation. Mais la criticité de ces données ne met pas en péril l'équilibre du réseau électrique.

Par contre l'impact des agrégateurs d'effacement (et de modulation) sur l'équilibre du système électrique peut être crucial. Il est donc indispensable d'analyser et de définir les besoins de sécurité auxquels ils devront répondre selon les différentes architectures possibles et les différents tronçons des réseaux de télécommunication mis en œuvre. Ces exigences devront être définies par le pouvoir réglementaire.

4.4. La sécurisation des réseaux de communication

4.4.1. Aperçu général

Comme expliqué à la section 2.3, les réseaux de communication sont porteurs d'une grande part des vulnérabilités qui affectent les REI. Il est donc essentiel de veiller à leur protection.

Une des particularités des REI est qu'ils mettent en œuvre de nombreux supports de radiocommunication (cellulaires, Wi-Fi, 802.15.4, bientôt, peut-être, LoRa). Le niveau de cybersécurité intrinsèque de ces solutions est très hétérogène et ne suffit pas à protéger les données.

En premier lieu, une attention particulière doit être portée à la sécurité des médias utilisés pour les communications entre îlots d'automatisme (réseaux WAN, CPL, GSM…). Cette sécurité, même si elle est déléguée à un opérateur tiers, doit être placée sous le contrôle de l'opéra-

teur du REI. Les points de connexion doivent être surveillés et, chaque fois que nécessaire, les communications doivent être authentifiées, chiffrées et auditables.

Même si les opérateurs, telecom ou FAI, proposent des offres de services « sécurisés », il est de la responsabilité des utilisateurs d'assurer une protection de « bout en bout » pour les données transmises. Lorsque les protocoles applicatifs mis en œuvre (couches hautes du modèle OSI) n'intègrent pas de sécurité, deux options se présentent :

1 – remplacer ces protocoles par des protocoles mettant en œuvre des mécanismes cryptographiques pour assurer l'intégrité, l'authenticité et la confidentialité. Un exemple classique est le remplacement de HTTP par HTTPS.

2 – encapsuler ces protocoles dans un tunnel sécurisé de type VPN assurant la sécurité des données transmises. La mise en œuvre des VPN s'appuie sur les protocoles IPSec ou TLS. Une note technique de l'ANSSI détaille les avantages et inconvénients de chacun d'eux. Les notes techniques et autres recommandations sont disponibles librement sur http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

4.4.2. Techniques de protection des données transmises sur les réseaux

Dans le cadre des REI il faut distinguer la sécurité « intra-site » et la sécurité du service de communication « inter-site ».

- au sein d'un site la protection du réseau s'appuie en général sur la confidentialité des données transmises sur le support physique. Selon la nature du support physique (radio, CPL, fibre optique), il faut ou non chiffrer les informations, ce qui n'exclut pas une protection de plus haut niveau (réseau privé virtuel VPN chiffrant, applicatif) ;
- en intersite, il est indispensable de mettre en place des services de type VPN chiffrés tels qu'ils sont en général proposés par les opérateurs Télécom ;
- une mesure conservatoire serait de créer des VPN de bout-en-bout pour s'affranchir de la dépendance aux opérateurs Télécom

La technologie VPN se situe au niveau 3 du modèle de référence OSI, c'est à dire au niveau de la couche IP qui assure la connectivité. C'est à dire que les couches TCP, UDP et au-dessus communiquent grâce au service VPN. Les services VPN s'appuient sur les standards IPsec (*Internet Protocol Security*), défini par l'IETF (Internet Engineering Task Force) comme un cadre de standards ouverts destiné à assurer des communications privées et protégées sur des réseaux IP grâce à l'utilisation de services de sécurité cryptographiques.

IPsec autorise plusieurs méthodes d'authentification et de chiffrement et donc, en tant que standard ouvert, peut être personnalisé pour un REI donné. De plus, IPsec est totalement indépendant des applications (couche 7 du modèle OSI) donc les utilisateurs n'ont pas besoin de configurer chaque application en fonction des standards IPsec. Ce qui n'exclut pas cependant de mettre en œuvre au niveau des applications des fonctions de sécurité et confidentialité complémentaires.

Le mode tunnel est utilisé pour créer des réseaux privés virtuels permettant la communication de réseau à réseau (entre deux sites distants), d'hôte à réseau (accès à distance d'un utilisateur) ou bien d'hôte à hôte (messagerie privée).

IPsec établit des « connexions » ou « tunnels » entre les points d'accès du VPN. Lors de l'établissement d'une connexion IPsec, plusieurs opérations sont effectuées :

1. Un échange des clés grâce à un canal d'échange de clés, sur une connexion UDP (ISAKMP pour Internet Security Association and Key Management Protocol). Le résultat est la constitution d'une association de sécurité (Security association) qui définit aussi l'usage du AH (Authentification Header) et de l'encapsulation de la charge utile d'un paquet. Une association de sécurité (SA) est donc l'établissement d'informations de sécurité partagées entre deux entités de réseau pour protéger le contenu de la communication.
2. Le transfert des données qui s'opère sur ces tunnels chiffrés dans deux champs de message : AH qui assure l'intégrité et l'authentification des paquets, ou ESP (Encapsulating Security Payload) qui assure en plus la confidentialité par cryptographie.

4.4.3. Quels protocoles ?

L'homogénéisation des systèmes de contrôle commande et/ou d'acquisition de signaux permet de réduire la surface d'attaque et de faciliter la mise en œuvre de systèmes de protection génériques. Cette homogénéisation passe par l'utilisation de standards tant dans les matériels déployés que dans les protocoles de communication utilisés. Ces protocoles doivent être basés sur des standards ouverts afin de limiter le taux de dépendance avec des solutions propriétaires industrielles et de faciliter les évolutions technologiques et le processus de maintenance par des équipes techniques variées.

Les protocoles applicatifs rencontrés dans les REI dépendent de l'endroit où l'on se situe. Sans être exhaustif, on peut citer :

- la norme CEI 61850 qui est la norme internationale pour la modélisation des données et des échanges internes

aux postes électriques. Elle permet d'intégrer toutes les fonctions de protection, de contrôle, de mesure et de surveillance dans un poste et fournit les moyens nécessaires aux applications de protection rapide des postes, de verrouillage et de télédéclenchement. Elle sera donc mise en œuvre pour les communications dans les sous-stations électriques. La spécification n'intègre pas de mécanismes de sécurité ;

- la norme CEI 62351, dédiée à la sécurité des communications dans les REI, qui vise à apporter une surcouche à la CEI 61850 pour sécuriser les données échangées lorsque les contraintes opérationnelles le permettent ; elle permet aussi de sécuriser les communications avec les RTU utilisant le protocole CEI 60870-5-104.
- la norme CEI 62056 issue de la spécification COSEM/DLMS[30], qui s'applique aux compteurs. Des mécanismes de sécurité sont prévus dans les spécifications du protocole.
- La norme CEI 62541 qui définit les mécanismes d'échange connus sous l'acronyme d'OPC-UA. Elle intéresse de nombreuses applications, qu'elles soient industrielles ou tertiaires. Ce protocole tend à devenir interopérable entre tous les constructeurs et couvre de nombreux besoins. Le standard prévoit des mécanismes de cybersécurité qui peuvent être implémentés ou non. Il convient de bien vérifier les configurations mises en œuvre afin qu'elles correspondent aux besoins de sécurité identifiés.

4.4.4. Les connexions distantes

Les connexions à distance font souvent débat dans le monde industriel comme dans celui des REI : d'un côté il est clair qu'elles tendent à accroître la surface d'attaque mais d'un autre elles permettent de développer des services, en particulier des services de télégestion et de télémaintenance, qui non seulement concourent à l'amélioration de l'efficacité mais peuvent aussi, s'ils sont bien conçus et bien gérés, rendre des services sur le plan de la gestion de la cybersécurité.

Avant de mettre en œuvre des connexions distantes, il est nécessaire d'identifier et d'apprécier le besoin auquel on entend répondre. Est-ce pour réaliser des opérations de télémaintenance ? Est-ce pour remonter des informations vers un centre de supervision centralisé ? Est-ce pour permettre à des équipes techniques de réaliser plus facilement des diagnostics en cas de panne ? Seuls les besoins réels devront être retenus.

En conformité avec les réglementations applicables et dans le cadre du référentiel normatif retenu, il est indispensable de conduire une analyse de risques spécifique à ces connexions. Les résultats de cette analyse de risques permettront de décider :

- si une connexion à distance est justifiée compte tenu des risques qu'elle présente au regard des avantages qu'elle procure ;
- dans le cas où une connexion apparaît justifiée, de définir avec quel niveau de protection il faut la concevoir et l'exploiter.

Dans l'analyse de risques, le niveau de sécurité des points d'accès en entrée et en sortie sera évidemment un élément déterminant. La connexion à distance avec un équipement d'un REI dont le haut niveau de sécurité doit être préservé, pourra être considérée comme interdite

S'agissant des points d'entrée distants, les connexions peuvent être de différente nature :

- accès depuis une zone physiquement maîtrisée ;
- accès depuis des postes nomades utilisés par exemple par des équipes d'intervention.

Si dans le premier cas, il est envisageable de déployer une solution offrant un niveau de sécurité correct, il est en revanche délicat d'envisager la même chose pour le deuxième.

En effet, des produits permettent aujourd'hui d'établir des connexions sécurisées entre deux entités. Il est recommandé, pour cela, d'employer des produits de confiance et de faire auditer régulièrement la solution mise en œuvre. De plus le contrôle d'accès physique des locaux depuis lesquels seront opérés les accès distants permettra de s'assurer que les personnes se connectant à distance sont bien légitimes. Mais aucun produit ne permet de garantir que les personnes qui utilisent un poste nomade sont bien légitimes. Les moyens d'authentification peuvent être dérobés et réutilisés par un attaquant. Autoriser des accès permanents depuis des postes nomades n'est donc pas recommandé. Lorsqu'il n'est pas possible de procéder autrement, ces accès doivent être ouverts à la demande et pendant une fenêtre temporelle limitée, ceci afin de limiter la surface d'exposition.

Les connexions distantes peuvent proposer plusieurs fonctionnalités :

- permettre des actions à distance (des télécommandes, des réglages, des modifications de configurations) ;
- limiter les accès à de la lecture seule.

Dans ce dernier cas, il sera possible de rendre la solution très sécurisée en mettant en œuvre des serveurs « miroirs » recevant, au travers d'une diode réseau, les éléments nécessaires au diagnostic.

[30] COSEM: Companion Specification for Energy Metering – DLMS: Device Language Message Specification.

4.5. Quelques technologies-clés

4.5.1. La cryptographie

L'état de l'art

La cryptographie désigne l'ensemble des techniques utilisées afin d'assurer le chiffrement des informations, c'est-à-dire leur transformation en un ensemble indéchiffrable par un acteur, humain, matériel ou logiciel, ne disposant pas des clés ayant servi au chiffrement.

La cryptographie est une technologie fort ancienne qui a connu des progrès continus au fur et à mesure que se développaient des algorithmes de chiffrement de plus en plus robustes mais aussi des techniques de déchiffrage de plus en plus performantes.

L'usage de la cryptographie dans les systèmes industriels et a priori dans les REI soulève les questions suivantes :

- comment mettre à la clé les équipements (insertion de la première clé) ? Si celle-ci est compromise, toutes les autres clés qui seront générées ou dérivées seront compromises ;
- comment changer les clés dans des environnements fonctionnant en continu 24/7, ce qui est le cas pour certains systèmes des REI ?
- comment révoquer les clés en cas de compromission ?
- comment stocker de manière sécurisée les clés maîtresses dans les composants, dont certains sont facilement accessibles et sur lesquels des attaques physiques permettraient de les extraire ?

Les **algorithmes de chiffrement symétrique** se fondent sur une même clé pour chiffrer et déchiffrer un message. L'un des problèmes de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre. La mise en œuvre peut s'avérer difficile, surtout avec un grand nombre de correspondants car il faut autant de clés que de correspondants.

L'algorithme le plus courant a été pendant longtemps le Data Encryption Standard (DES) pour lequel il existe de nombreux circuits disponibles intégrables dans la plupart des équipements. Son emploi n'est plus recommandé aujourd'hui, du fait de son espace de clés trop petit (56 bits) permettant une attaque systématique en un temps raisonnable. L'Advanced Encryption Standard ou AES (soit « standard de chiffrement avancé » en français), est le nouveau standard de chiffrement né aux Etats-Unis en 2000 et approuvé par la National Security Agency (NSA). Il est aujourd'hui largement utilisé, avec des clés de 128, 192 ou 256 bits, dans de nombreux protocoles de communication, tels que le Wi-Fi (niveau WPA2) ou les protocoles basés sur l'IEEE 802.15.4 (ZigBee, ISA100.11a).

Les **algorithmes de chiffrement asymétriques** (à clé publique qui est diffusée et à clé privée qui est gardée secrète par l'une des parties) permettent le chiffrement et la signature. La protection de la partie secrète est plus aisée que dans les algorithmes symétriques. Le plus connu est le RSA (nommé à partir des initiales de ses trois inventeurs : Rivest, Shamir, Adleman) est très utilisé dans le commerce électronique. Basée sur des exponentiations entières de grands nombres, cette technique est gourmande en calcul et mémoire et de ce fait moins aisément implantable dans des équipements « bas coût » ou dotés de faible capacité de traitement ou de mémoire. De ce fait, de nombreuses variantes sont développées et les préférences actuelles vont vers l'utilisation de solutions cryptographiques basées sur les courbes elliptiques ou ECC (Elliptic Curve Cryptography) et fondées sur la difficulté du problème du logarithme discret dans le groupe correspondant à une courbe elliptique.

L'échange de clés Diffie-Hellman, est une méthode par laquelle deux entités se mettent d'accord sur un nombre (qu'ils vont utiliser comme clé pour chiffrer la conversation suivante éventuellement avec un algorithme symétrique) sans qu'il soit possible de découvrir le nombre, même en ayant écouté tous leurs échanges Elle permet donc d'éviter la distribution de clé secrète (ou publique) préalable. Cette technique est utilisée dans Internet (par exemple dans le protocole HTTPS). La partie d'échange de clé est aussi basée sur des grands nombres et donc requiert des capacités de calcul.

Les mécanismes cryptographiques permettent aussi d'assurer l'intégrité et l'authenticité d'un message transmis en « clair ».

Les annexes B du Référentiel général de sécurité RGS publié par l'ANSSI (http://www.ssi.gouv.fr/rgs) fournissent les recommandations quant à l'utilisation des mécanismes cryptographiques. Sans une bonne connaissance du sujet et une bonne gestion des paramètres (choix des algorithmes, taille des blocs, des clés, etc.), les avantages de la cryptographie peuvent être réduits à néant. Des clés trop courtes ou mal protégées ainsi que des mauvaises implémentations offriront aux attaquants la possibilité de contourner les mécanismes de sécurité.

Beaucoup d'experts considèrent qu'il est recommandé de s'appuyer sur des solutions existantes et standardisées plutôt que de réinventer des solutions dont le niveau de sécurité sera plus faible faute de retours d'expérience suffisants. Faire appel à des experts pour mettre en œuvre la cryptographie est essentiel, de même que le recours à des produits labellisés (se référer au site de l'ANSSI).

En outre, le développement d'algorithmes et de protocoles cryptographiques dédiés, lorsque nécessaire, doit reposer sur une équipe, voire un écosystème, d'un haut niveau d'expertise pour éviter certaines erreurs passées. Cela est d'ailleurs vrai pour l'ensemble de la cybersécurité au regard de la complexité technique, de la multidisciplinarité des sujets et de l'évolution rapide du domaine.

Les développements nouveaux : les crypto-systèmes homomorphes

Depuis quelques années, se développe la théorie des crypto-systèmes dits pleinement homomorphes, permettant de réaliser des calculs arbitrairement complexes directement sur des données chiffrées, c'est à dire de « crypto-calculer ». Ces crypto-systèmes fournissent les fondements nécessaires pour la mise en œuvre de services préservant intrinsèquement la confidentialité des données. Ce domaine de recherche se caractérise par un large potentiel applicatif ainsi que par les progrès extrêmement rapides réalisés ces dernières années en matière de performances qui permettent d'envisager l'intégration de cette technologie dans de premiers prototypes industriels.

Dans un contexte de REI, une telle capacité de calcul en aveugle sur données cryptées permettra de répondre à plusieurs enjeux :

- celui des infrastructures de distribution de clefs qui pourront être largement simplifiées si certains nœuds du réseau ont la capacité de traiter des données sans avoir de capacité de déchiffrement ;
- celui de l'interaction sans divulgation entre données et algorithmes en préservant la confidentialité des données (privées ou sensibles sur le plan de la propriété industrielle) ;
- celui de la protection intrinsèque de données sur plates-formes connectées.

Bien que des cryptosystèmes homomorphes restrictifs (exclusivement additifs ou multiplicatifs) existent depuis des années, et possèdent de nombreuses applications (par exemple en traitement du signal), la théorie des crypto-systèmes pleinement homomorphes est encore récente et pose plusieurs challenges, notamment en termes de performances. L'annexe 4 fournit un état de l'art sur les techniques de cryptographie homomorphe et leur degré d'applicabilité.

4.5.2. Authentification et identification

Dans les systèmes informatiques, identification et authentification sont généralement liées. L'utilisateur doit être identifié (avec les droits qui lui sont associés), et authentifié pour activer ces droits.

L'authentification des utilisateurs ou plus généralement des entités se décline généralement à partir de trois éléments :

- ce que l'entité connait : typiquement un couple login/password, un PIN code (Personal Identification Number), etc.
- ce que l'entité possède : typiquement un objet physique, carte à puce, badge, dongle, les générateurs de mots de passe et notamment d'OTP (One Time Password) utilisables une seule fois, etc.
- ce que l'entité est : typiquement une caractéristique de l'entité, si possible unique et infalsifiable, par exemple la biométrie.

Les systèmes d'authentification sont hiérarchisés en fonction de leur résistance aux attaques. On parle d'authentification forte quand plusieurs de ces éléments sont mixés : par exemple, une carte à puce activée via un PIN code, un OTP complété par un PIN personnel, etc.

Une authentification forte est recommandée pour s'assurer qu'un utilisateur a bien le droit d'effectuer des opérations critiques sur un système informatique.

Il faut noter que ce principe peut également s'appliquer aux composantes matérielles d'un système et pas uniquement aux utilisateurs. Une clef cryptographique peut ainsi être assimilée à une connaissance de l'entité, un composant de sécurité (de type TPM) peut être assimilé à une possession de l'entité et la technologie émergente des PUF (Physical Unclonable Function) peut être assimilée à une caractéristique intrinsèque d'un composant du système.

Comme pour tout système de sécurité, le niveau d'authentification requis dépend de l'application et des conditions dans lesquelles cette authentification est réalisée : un environnement ouvert et incontrôlé requerra une authentification forte, le même système dans un environnement contrôlé pourra se contenter d'une authentification faible.

L'annexe 5 fournit des compléments sur la façon dont l'authentification peut être assurée selon l'acteur concerné.

4.5.3. La qualité des logiciels

La qualité des logiciels est une étape indispensable pour disposer de logiciels robustes susceptibles de résister à des attaques informatiques. Les attaques par débordement de tampon (« buffer overflow ») ou injection de code restent encore importantes. Pourtant l'application de règles simples de bonne programmation permettrait de les éviter. Il existe également des guides de « secure coding » pour rendre les développements plus sécurisés mais leur application nécessite néanmoins un apprentissage et de la rigueur de la part des développeurs.

La qualité est nécessaire à la sécurité afin de pouvoir garantir que les programmes informatiques utilisés dans des applications sensibles assurent trois propriétés essentielles :

• la confidentialité des données ;
• l'intégrité des données et des codes (programmes) ;
• la disponibilité des services.

Concrètement, les défauts de sécurité sont des "bugs" des programmes. Les approches traditionnelles face à cette problématique, fondées sur des audits d'exhaustivité variable mais jamais complète, ne constituent qu'une réponse partielle à ce problème. La garantie de l'absence absolue de défaut dans des logiciels reste un objectif poursuivi depuis longtemps qui ne semble atteignable qu'à travers des approches pragmatiques concernant à cerner le problème afin de limiter l'espace d'analyse de sécurité. La problématique de la détection de failles de sécurité est alors similaire à celle de la démonstration de la sûreté de fonctionnement d'une application logicielle.

Des outils d'analyse de code source sont déjà développés et mis en exploitation, depuis plusieurs années, dans ce domaine de la sûreté logicielle. Leur méthodologie d'application consiste à définir des familles de risques, puis à définir pour ceux-ci des familles de bugs dans les logiciels en les associant à des structures et schémas types de codage. Ensuite, la méthodologie se traduit de manière technologique par un paramétrage des outils d'analyse et le développement de bibliothèques dédiées afin d'assurer à la fois la correction des résultats et la performance des analyses.

L'enjeu actuel est donc l'adaptation de ces outils aux problématiques de sécurité pour établir de manière semi-automatique la conformité de certains éléments logiciels critiques à des exigences de sécurité, en particulier :
• invulnérabilité aux attaques de type débordement de tampon ;
• confidentialité des informations sensibles ;
• étanchéité totale entre les processus d'une part, le logiciel et les fonctions du matériel d'autre part ;
• surveillance automatique et optimisée des exécutions de composants (monitoring).

La mise en place de ces développements pourra s'effectuer selon trois axes, combinant :
• conduite de recherche technologique permettant l'élaboration de vérifications de sécurité complexes ;
• cas d'usage à impact industriel pour la démonstration d'applicabilité des analyses les plus mûres ;
• activités de dissémination notamment auprès des instances de normalisation.

Analyse des failles logicielles

La mise en place de référentiels de sécurité dans le domaine informatique nécessite de pouvoir démontrer la qualité et la sécurité des composants logiciels utilisés. Il s'agit, en pratique, non seulement d'assurer la conformité aux normes de codage, mais aussi l'absence d'opérations non définies (division par zéro, accès à des zones mémoires invalides, etc.) pouvant mener à des erreurs à l'exécution du code. Les référentiels préconisent également d'effectuer le test unitaire de façon à assurer que tous les cas sont testés et rejoignent le domaine des règles de codage en recommandant la détection et l'élimination du code inatteignable.

Les outils d'analyse de code réalisent une approximation de comportement des programmes dont ils veulent vérifier les propriétés. Une analyse est complète lorsque, malgré cette approximation, elle trouve et signale implacablement toute instruction du programme qui viole la propriété examinée. Par exemple, si une analyse complète valide la propriété « ce logiciel ne génère pas d'erreurs à l'exécution », alors le logiciel examiné est assuré de ne pas rencontrer d'erreurs à son exécution, quelles que soient les conditions opérationnelles. De même, si une analyse complète valide la propriété « cette fonction ne contient pas de code inatteignable », alors toute instruction de cette fonction pourra être exécutée en opération. En d'autres termes, une analyse complète ne se contente pas de chercher des bugs : elle en garantit l'absence. Cette propriété, techniquement complexe à mettre en œuvre pour les concepteurs des analyseurs, est caractéristique des outils de nouvelle génération comme Astrée, Frama-C[31] ou Polyspace pour le langage C.

L'analyse des codes des systèmes industriels et leur certification doit pouvoir s'appuyer sur un outillage performant, permettant de fournir des garanties formelles de sécurité des logiciels telles que :
• absence d'erreurs à l'exécution, des défauts de programmation à l'origine d'une large majorité des attaques connues ;
• respect de politiques de sécurité prédéfinies, spécifiant les comportements fonctionnels sécuritaires et hérités des politiques systèmes ;
• contrôle des flux d'information à travers les traitements numériques, préservant l'intégrité et la confidentialité de ceux-ci.

4.6. Les mesures organisationnelles

4.6.1. Généralités

La cybersécurité ne dépend pas seulement des solutions techniques mises en œuvre : la sensibilisation, la formation

[31] La société TrustInSoft, créée en 2013, propose des solutions de prévention des cyberattaques sur la base de l'outil d'analyse de code en open-source Frama-C. Son offre comporte d'une part, un analyseur de logiciel diffusé en ligne ou directement sur des machines chez les clients, et, d'autre part, des kits de validation pour des composants logiciels dédiés très répandus, dans lesquels les vulnérabilités ont des conséquences économiques majeures.

et la motivation des personnels, l'efficacité des organisations, la répartition des responsabilités, la clarté des « politiques & procédures » et leur respect sont des facteurs essentiels de prévention des risques et de réactivité face à une attaque couronnée de succès,

Il existe des référentiels normatifs appropriés pour élaborer, dans le cadre d'une organisation donnée, un programme de gestion de la cybersécurité incluant notamment les politiques et des procédures applicables aux organisations et aux personnels qui les composent. Ces référentiels sont cités en annexe 1. La norme la plus connue est sans doute l'ISO/CEI 27002 qui constitue un catalogue de 133 mesures dites "best practices" (bonnes pratiques en français), destinées à être mises en œuvre, si la sécurité des systèmes le requiert, par tous ceux qui sont responsables de la mise en place ou du maintien d'un système de management de la cybersécurité. Ce texte sera repris et complété dans le volet 2-1 de la norme CEI 62443, en cours de finalisation, plus spécifiquement applicable aux systèmes industriels, et qui retient pour les « politiques et procédures » les 11 catégories d'exigences organisationnelles issues de l'ISO/CEI 27002 auxquelles il faut répondre dans un système de gestion de la cybersécurité. Nous nous contenterons ici de souligner certains aspects propres aux REI. L'ISO/CEI 27002 est accompagnée du Technical Report ISO/CEI TR 27019 applicable aux systèmes de contrôle de procédés spécifiques à l'industrie de l'énergie. Ce "Technical Report" est important pour les REI car il propose des mesures supplémentaires à l'ISO/CEI 27002 spécifiques aux systèmes des industries de l'énergie.

4.6.2. Les politiques et les procédures

Les différents composants d'un REI requièrent des opérations critiques, que ce soit en phase de conception, d'installation, d'exploitation ou de maintenance. Ces différentes opérations doivent être contrôlées via la définition de « **politiques** » de cybersécurité conforme à un référentiel normatif que l'on aura préalablement choisi. Les politiques de cybersécurité doivent inclure l'expression des exigences à satisfaire pour contrôler l'exécution et la réalisation de ces opérations critiques.

Chacune de ces exigences donne ensuite naissance à des « **procédures** » fixant dans le détail les règles, techniques et organisationnelles à observer afin d'assurer le respect de ces exigences. L'ensemble constitue un **système de gestion de la cybersécurité**. Un tel système peut être établi à différents niveaux de l'organisation d'un opérateur de réseau à condition que les politiques et procédures applicables aux différents niveaux de l'organisation soient cohérentes entre elles.

Les politiques de cybersécurité dans les REI doivent inclure a minima les composantes suivantes :

- **Politique d'authentification** spécifiant les exigences d'identification et d'authentification des personnes en charge de réaliser les opérations critiques. La politique d'authentification peut notamment spécifier que certaines opérations critiques, pour être réalisées, nécessitent une authentification forte. La politique de d'authentification peut également spécifier des exigences de contrôle d'accès physiques, par exemple à un bâtiment, un local, une machine ou des équipements spécifiques du REI. Ces exigences sont notamment importantes pour contrôler les opérations de maintenance et de mise à jour des configurations des équipements du REI.
- **Politique d'autorisation** spécifiant les droits ainsi que les interdictions des personnes et des processus. Cette politique d'autorisation peut être définie en fonction des rôles affectés aux personnes dans le REI conformément au modèle de contrôle d'accès RBAC (Role Based Access Control). L'affection des rôles peut passer par une procédure d'habilitation des personnels. La politique d'autorisation doit pouvoir s'adapter dynamiquement aux changements de l'environnement de risque du REI, par exemple en cas de situation d'urgence ou de passage dans un mode de fonctionnement dégradé.
- **Politique de filtrage** des communications spécifiant les flux autorisés entre les composants matériels et logiciels du REI. Cette politique de filtrage sera déployée sur les composants en charge d'assurer les contrôles de sécurité du REI tels que routeur, pare-feu système et applicatif, système de détection d'intrusion, VPN, etc. (Cf section 4.4.2).
- **Politique de traçabilité** spécifiant les exigences permettant de tracer et auditer la réalisation des opérations critiques. La politique de traçabilité doit spécifier toutes les données, telles que paramètres des opérations critiques, données temporelles ou données contextuelles, qu'il convient d'auditer pour détecter d'éventuelles violations de la politique de sécurité et déterminer les responsabilités en cas de violation.
- **Politique de supervision et d'administration** spécifiant les exigences pour contrôler le bon fonctionnement du système et détecter les incidents ou accidents ayant des causes accidentelles ou malveillantes. La politique de supervision et d'administration doit contrôler la génération des alertes et spécifier les moyens logiciels et humains pour corréler ces alertes. Elle doit également inclure les procédures à suivre pour traiter les alertes. Lorsque la cause de la défaillance n'est pas accidentelle mais est au contraire intentionnellement malveillante, la politique de

supervision et d'administration doit également spécifier les procédures pour faire face et réagir à cette action malveillante. Ces procédures peuvent conduire, lorsque cela s'avère nécessaire, à mettre à jour la politique de sécurité.

- **Politique de reprise** après panne ou défaillance (voir section 4.6.3.).
- **Politique de mise à jour des logiciels** spécifiant les exigences pour gérer ces modifications et assurer la cohérence globale lors de la mise en place des nouvelles versions.

La politique de sécurité permet donc de contrôler les éléments de base de la sécurité décrits précédemment (authentification et autorisation des utilisateurs, audits, détection d'intrusion, filtrage des communications, etc.) mais également des aspects organisationnels relatifs à l'affectation de droits particuliers critiques à des personnes (formation, habilitation, accréditation, etc.). Ces aspects organisationnels sont généralement regroupés dans la thématique « gestion de la sécurité » et des normes décrivent des méthodes et organisations efficaces (ISO/CEI 27001&2 ISO/CEI TR 27019 et CEI 62443-2-x).

Il est également souhaitable qu'une politique définisse les règles de spécification et de conception des infrastructures. La sécurité se doit d'être intégrée dès l'origine des projets : cela passe par l'expression des besoins en cybersécurité spécifiée dans les cahiers des charges pour clairement identifier les budgets nécessaires au durcissement des systèmes et permettre aux intégrateurs, constructeurs et éditeurs d'adapter leurs solutions. Ces besoins doivent se référer aux normes, référentiels métiers et contraintes nationales. Les architectures doivent être conçues pour être intrinsèquement résilientes et présenter des caractéristiques de défense en profondeur.

De nombreuses infrastructures sont dépendantes de tiers pour les communications. Un soin particulier doit être apporté quant au choix des fournisseurs de services et des technologies qu'ils utilisent et des règles de sélection doivent être définies. En tout état de cause, les opérateurs des REI doivent considérer les moyens de communication mis à leur disposition par des tiers comme non sûrs et doivent bâtir leur propre sécurisation de communications au-dessus des moyens fournis.

Les opérateurs des REI doivent veiller à la mise en œuvre d'une organisation capable d'analyser les informations de flux sous des angles techniques et métier, à réagir aux tentatives d'intrusion et à analyser les nouvelles menaces et leurs parades. Des solutions de type SOC (Security Operation Center), bâties au-dessus de solutions de collecte et de corrélation d'évènement SIEM permettent de vérifier l'application des politiques définies.

4.6.3. Le traitement des incidents

Parmi les mesures organisationnelles importantes figure le traitement d'incident. Dans un contexte comme celui des REI, il est illusoire de penser que les mesures préventives suffiront à empêcher totalement la survenance d'incidents. Or les REI sont des systèmes qui sont conçus pour fonctionner en mode 7 jours sur 7 et 24 heures sur 24. Si les pannes et défaillances sont des événements exceptionnels, elles doivent être prévues dans le plan de continuité de service du système. Ce plan de continuité doit être décliné dans une politique de reprise d'activité après panne ou défaillance, qui spécifie les procédures à suivre pour remettre le système en état de marche, ainsi que les modes opératoires de contournement pour continuer à fonctionner pendant la reprise système qui peut durer plusieurs jours. La politique de traçabilité, vue précédemment, doit être conçue en tenant compte de la politique de reprise après panne ou défaillance, de manière à auditer toutes les données nécessaires pour assurer la reprise du système en cas de panne ou défaillance.

Il est en outre impératif de pouvoir s'exercer régulièrement, à la manière de ce qui se pratique dans le domaine de la lutte contre l'incendie.

Dans le domaine de la cybersécurité, des prestataires de réponse aux incidents offrent des services pour aider les opérateurs. Ce sujet peut en effet demander des compétences spécifiques dont ne disposent pas les opérateurs. Des travaux pour qualifier ce type de prestataires sont actuellement en cours, car lors d'un incident, il est important de pouvoir s'appuyer sur des entreprises et intervenants de confiance afin de ne pas surexposer les systèmes à de nouvelles attaques informatiques et de nouveaux risques.

Des assureurs proposent des services intégrant le traitement d'incidents. Le mouvement est apparu aux Etats-Unis il y a quelques années déjà. En France, des compagnies d'assurance s'associent avec des entreprises spécialisées dans le domaine de la cybersécurité pour proposer des offres complètes en ce sens.

Comme cela est souvent nécessaire – et pour les OIV c'est une obligation résultant de l'article 22 de la loi de programmation militaire – des mesures d'urgence doivent être prévues. Ces mesures, préparées en amont et dont les effets ont été analysés, peuvent être activées sur demande pour limiter les effets d'une attaque informatique. Par exemple, désactiver les accès distants permet de réduire la surface d'exposition des systèmes lors d'épisodes tels que les attaques virales ; activer les équipes d'astreinte permet d'intervenir plus rapidement et de basculer sur des modes dégradés dépendant moins des systèmes.

4.6.4. La supervision de la cybersécurité

La supervision de la cybersécurité des REI doit s'appuyer sur un réseau informatique spécialisé qui centralise les informations remontées par des sondes du ou des réseaux supervisés. Les informations remontées par ces sondes réseaux doivent être significatives des activités :

- informations concernant la cartographie des réseaux (éléments connus et détection en temps réel d'éléments connectés non identifiés, par exemple détection d'adresse IP inconnue) ;
- informations concernant les flux échangés (capacité des sondes en mode d'apprentissage de remonter à la supervision un comportement « normal ») ;
- informations concernant les flux illégitimes ou déviants par rapport à un comportement normal.

Les capacités d'analyse permettant de détecter des comportements malveillants, pourront selon le degré de complexité des systèmes soient être intégrés aux sondes dans le réseau industriel en mode passif, soit dans le réseau de supervision cyber, la communication des sondes avec le réseau de supervision cyber se faisant au travers de diodes matérielles assurant une étanchéité entre les réseaux afin de garantir la non compromission de la supervision cyber en cas d'attaque sur les réseaux industriels.

4.6.5. La formation : formations existantes et formations nécessaires

Malgré une offre de formation importante en nombre et en volume (annexe 3), il apparaît que la difficulté à trouver les compétences « sur le marché » persiste. Cela peut provenir du fait que tous les diplômés ne débutent pas leur carrière dans le domaine de la sécurité et qu'une part importante sinon majoritaire est absorbée par les sociétés de service et de conseil, d'autre part certaines sont ciblées vers des besoins sectoriels (paiement, réseau…). Il est important qu'une fraction de ces formations soit davantage orientée vers les besoins des REI.

D'autre part la sécurité est un sujet excessivement vaste et la protection d'un système d'information, d'un réseau d'entreprise, d'objets communicants, de systèmes monétiques, la gestion de la formation et l'habilitation des personnels… mobilisent des champs de connaissances larges et des compétences variées. La sécurité est fortement liée aux systèmes informatiques (y compris embarqués), la formation à la sécurité implique des prérequis solides en systèmes d'exploitation, en gestion des systèmes, en réseau et nécessite des compétences rares sur le marché. La réponse aux besoins des opérateurs des REI peut être une combinaison de plusieurs approches de formation :

- Formation amont
  - Une sensibilisation de masse permettant à un grand nombre de personnels de tous niveaux de se sensibiliser à la sécurité, en comprendre les enjeux et les premiers éléments techniques. Le développement d'un ou plusieurs MOOC (Massive Online Open Course) permettrait d'atteindre rapidement un large public professionnel dont le niveau peut aller de Bac à Bac+2 (BTS, DUT, Licence pro…) avec expérience informatique. L'implication des acteurs de l'électricité dans la conception (programme) et l'illustration du cours donnera crédibilité et confiance. L'efficacité nécessite de toucher tous les personnels à former qui sont autant chez les opérateurs, que chez les constructeurs voire chez les utilisateurs. Il faudra aussi que ceux-ci incitent leurs agents à utiliser ces ressources (y compris dans le cadre du droit individuel à la formation ou de la formation continue).
  - Expliciter les besoins spécifiques du secteur de l'énergie en matière de sécurité autour des REI (architectures SCADA, composants, systèmes d'information de gestion de l'énergie, home distribution, multi-entreprise…) et favoriser la prise en compte de ces problématiques dans les formations existantes ou au sein de nouvelles formations.
- **Formation des maîtres d'ouvrage, des concepteurs et des maîtres d'œuvre** afin que la sécurité soit incluse tout au long de la chaine de conception et réalisation des composants matériels et surtout logiciels du système électrique intelligent. Outre les techniques propres à la sécurité ce sont les éléments de la politique de sécurité des REI qui doivent être connues.
- **Formation des intervenants :** il faut développer une formation professionnelle de la branche destinée à qualifier les intervenants professionnels. Elle est indispensable dans le cadre d'une politique de sécurité associant qualification et rôle.
- **Formation des opérateurs :** une politique orientée rôle nécessite que les opérateurs doivent être capables de piloter en temps réel la production et la distribution. Il est indispensable d'introduire dans leur formation une capacité de type "Security Operating Center" (SOC) leur permettant d'inclure les alertes informatiques dans leurs processus de décision.
- **Formation des auditeurs :** les auditeurs de systèmes informatiques traditionnels connaissent mal les besoins spécifiques de sécurité des infrastructures industrielles. Par exemple, les protocoles utilisés dans le monde des SCADA (Modbus, DNP3, EthernetIP, Profinet…) ne sont pas ou peu enseignés dans les parcours informatiques. Les architectures matérielles spécifiques de ces

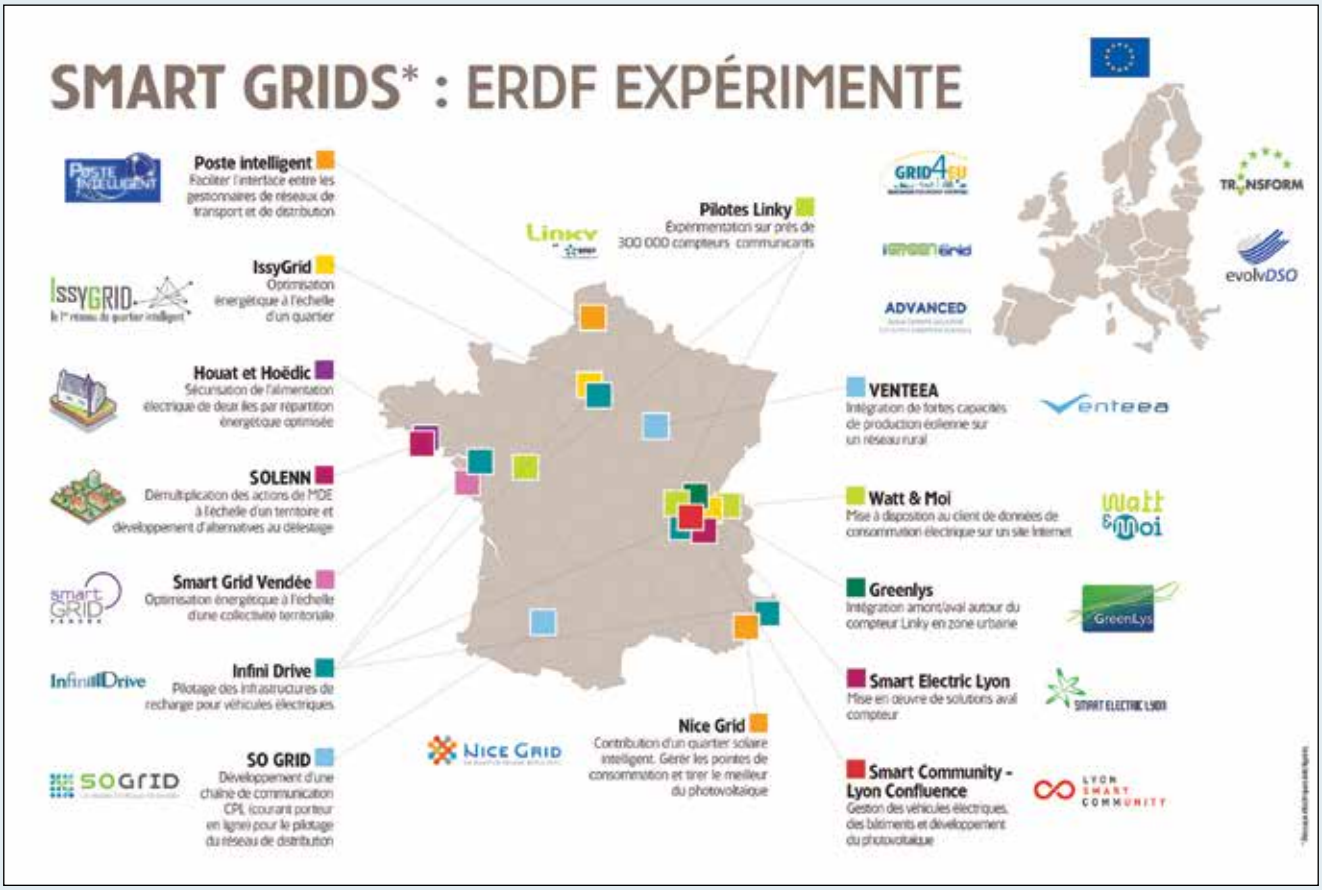

Figure 8 : Carte des démonstrateurs REI en France – Source : ERDF.

environnements sont également souvent ignorées. Il apparaît donc nécessaire de développer une filière de type binôme, constitué par un spécialiste en sécurité de systèmes informatiques et un autre en contrôle industriel. Il conviendrait également de former des auditeurs orientés vers ces environnements.

Ces formations peuvent se concevoir sous l'égide de la branche tout en étant mises en œuvre avec des partenaires académiques disposant des compétences et forces de formation. Dans ce contexte l'alternance devrait être privilégiée. Le modèle de l'ISTP qui associe branche industrielle et école d'ingénieurs spécialisés dans la formation à la sûreté nucléaire est intéressant à cet égard.

L'évolution continue des risques et la rareté de réalisation de certaines actions nécessitent un entretien et une mise à jour des savoirs et des compétences pilotées par les professionnels. Le modèle de formation mis en œuvre dans le secteur santé est particulièrement exemplaire à cet égard.

5. Les démonstrateurs

Après avoir décidé le financement de 16 projets sur la thématique des « Réseaux électriques intelligents », l'Etat a complété en 2015 ce soutien à l'innovation par un nouvel appel à manifestations d'intérêt (AMI), géré par l'ADEME dans le cadre du Programme Investissements d'Avenir (PIA)[32]. Cet appel est ouvert jusqu'au 11 septembre 2015.

Ces projets, pilotés par plusieurs consortiums rassemblant de nombreux partenaires couvrent les différents enjeux de la transition énergétique et les différentes composantes des REI tout en permettant aux opérateurs de réseaux de valider sur le terrain la pertinence technique et économique des solutions innovantes testées.

Ces démonstrateurs sont soumis, pour la protection et la transmission des données, à la règlementation de la CRE pour les informations commercialement sensibles (ICS) et à la règlementation de la CNIL pour les données à caractère personnel (DCP).

La problématique de cybersécurité est présente dans tous les démonstrateurs REI et est traitée systématiquement en utilisant une méthodologie structurée et rationnelle par les acteurs des projets.

[32] http://www.presse.ademe.fr/2014/04/un-nouvel-appel-a-projets-pour-les-reseaux-electriques-intelligents-html

A titre d'exemple, ERDF utilise le modèle de référence SGAM pour identifier puis formaliser les cas d'usage des démonstrateurs REI d'une façon technologiquement neutre. Ce modèle propose une approche normalisée bien adaptée à la complexité des REI. Il introduit clairement les aspects d'interopérabilité et comment ces derniers sont pris en compte entre les différents composants REI via des domaines, des zones et une décomposition en couches (voir section 1.4.).

Dans le domaine de la distribution, ce sont principalement les domaines "Distribution", "DER" "Customer Premise" et les zones "Process" 'Field" "Station" "Operation" qui sont explorés.

Pour répondre à la problématique de cybersécurité des démonstrateurs REI les plus récents, ERDF décline la méthodologie décrite dans le rapport "*Smart Grid Information Security*" issue des travaux menés par le Smart Grid Coordination Group (SG-CG/SGIS) du CEN-CENELEC-ETSI dans le cadre du mandat M/490 de la Commission européenne.

ERDF a utilisé, dans l'ensemble des démonstrateurs REI, les normes internationales, dont l'ISO 27001 pour les systèmes d'information d'entreprise et la CEI 62443-2-1 pour les systèmes d'information industrielle, comme cadre de gestion de la cybersécurité.

Sur le plan technique, l'approche d'ERDF consiste dans un premier temps à identifier les besoins de sécurité « métier » à partir des cas d'usage des démonstrateurs, puis à réaliser les analyses de risque, les menaces et les mesures étant considérées d'un point de vue technique, processus et humain.

A ce jour, les premiers retours d'expérience des démonstrateurs REI renforcent le besoin que la cybersécurité prenne en compte une approche globale de gestion des risques « entreprise » et « industriels ». Il sera important de tirer les enseignements de ces démonstrateurs et de partager les retours d'expérience. Les premiers retours confirment que le thème de la cybersécurité doit être considéré comme l'un des objectifs essentiels de tout démonstrateur.

6. Conclusions et recommandations

Le développement des réseaux électriques intelligents est une tendance forte de l'évolution des systèmes électriques. L'enjeu pour la France est double :

- d'une part les REI constituent l'un des moyens de faciliter, dans le domaine de l'énergie électrique, l'adéquation entre les ressources et la demande par une adaptation mutuelle et la promotion de formes d'énergie décentralisées. La loi sur la transition énergétique et la croissance verte reconnait l'importance des REI en en faisant l'un des volets de la programmation pluriannuelle de l'énergie ;
- d'autre part les REI constituent un véritable enjeu industriel, pris en compte par la « Nouvelle France industrielle », qui pourrait représenter d'ici 2020, plus de 25 000 emplois directs en France pour un chiffre d'affaire d'au moins six milliards d'euros.

Cependant, dans un contexte marqué par une intensification des cyberattaques, le développement des REI s'accompagne d'un élargissement des surfaces d'attaque donnant prise à des menaces dont les impacts, si elles aboutissaient, pourraient être dommageables aux réseaux et par conséquent aux populations et au tissu économique qu'ils desservent. La responsabilité d'y faire face et d'assurer en permanence l'équilibre offre/demande implique l'ensemble des gestionnaires des réseaux de transport et de distribution.

ERDF et RTE ont investi dans le domaine et organisé leur système de manière à assurer la meilleure prise en compte des contraintes de cybersécurité dans un contexte en forte transformation. Mais le système électrique s'étend à des acteurs toujours plus nombreux : opérateurs, industriels ou sociétés de service et consommateurs, bientôt transformés en « consom'acteurs » grâce aux REI. Toutes ces parties prenantes interagissent entre elles par des canaux multiples en mettant en œuvre des équipements ou des composants, matériels ou logiciels, d'origine diverse.

Il est donc absolument indispensable que le développement des REI s'accompagne d'une prise en considération, par tous les acteurs, des problématiques de cybersécurité, dès la conception des services/logiciels/équipements et pendant toute leur durée de vie.

Le cadre normatif des REI n'est pas achevé mais il est très avancé. Il s'élabore au niveau européen et dans les instances internationales de standardisation. En France, l'ANSSI joue son rôle de prescripteur et de conseil, en émettant des guides et recommandations techniques et en servant de support à l'action réglementaire, ponctuée récemment (le 28 mars 2015) par la parution de deux décrets essentiels sur « la sécurité des systèmes d'information des opérateurs d'importance vitale » et sur « la qualification des produits de sécurité et des prestataires de service de la confiance pour les besoins de la sécurité nationale ».

En parallèle, les technologies de protection progressent rapidement et les capacités des processeurs et des mémoires permettront à l'avenir de rapprocher les dispositifs de protection des équipements auxquels ils s'adressent.

Cependant le monde de la cybersécurité des REI reste très complexe et la cybersécurité a un coût. Le présent Livre blanc s'efforce de faciliter la prise en compte de la cybersécurité par l'écosystème des REI en dressant un panorama

d'ensemble de la problématique cybersécuritaire. Chaque intervenant doit cependant faire l'effort d'analyser son cas particulier afin de déterminer quel est le bon niveau de protection à mettre en place compte tenu des risques encourus et quelles sont les bonnes solutions et les bonnes pratiques à mettre en œuvre.

Le Livre blanc met en évidence quelques voies d'approfondissement.

En s'appuyant sur le cadre normatif international, il est souhaitable de mettre en place, en France comme au niveau européen, des procédures de certification de sécurité des constituants des REI, qui permettront de donner aux parties prenantes une confiance suffisante dans le respect des exigences de sécurité découlant de ces normes.

Il est également indispensable de mieux afficher la cybersécurité en tant qu'objectif majeur dans les démonstrateurs futurs ou en cours d'expérimentation dans le cadre de la politique de soutien menée par les pouvoirs publics. De telles opérations, ciblées sur des contraintes d'usage soigneusement préparés avec les opérateurs et les diverses parties prenantes, permettront de tirer des enseignements utiles sur la pertinence des normes et des mesures de protection qui seront ainsi testées.

Bien entendu, compte tenu de la complexité du sujet et du nombre d'intervenants concernés, il est nécessaire de renforcer sensiblement les actions de formation et de sensibilisation. Certains acteurs peuvent se contenter d'une formation générale sur les enjeux et les techniques de la cybersécurité ; d'autres ont besoin d'une formation plus approfondie qui doit être considérée comme un volet de la formation « métier » qui leur est dispensée. Un système de qualification des personnels et des entreprises doit être mis en place en aval de ces formations.

La recherche et développement doit être encouragée : il existe de nouvelles approches du traitement de la cybersécurité d'architectures distribuées telles celles des REI. La philosophie en est proche de celle applicable à l'Internet industriel des objets (IIoT) pour lequel les questions de cybersécurité font l'objet de nouveaux paradigmes visant à assimiler le réseau à une sorte de réseau social dans lequel chaque abonné dispose de droits et obligations. Les progrès des technologies matérielles et logicielles permettent également d'envisager des protections de plus en plus rapprochées des composants sensibles grâce au développement de plates-formes de sécurité intégrées sur des chipsets et remplissant les fonctions-clés de la protection. Enfin, les travaux sur les méthodes de cryptographie homomorphes permettant de traiter des données chiffrées sans avoir à les déchiffrer sont d'un intérêt primordial pour les REI de façon à pouvoir acheminer et manipuler sans risque les informations quelles qu'en soient l'origine et la destination.

Il est à noter que, dans une logique duale civile-militaire, le ministère de la défense, la région Bretagne, l'INRIA, le CNRS et neuf écoles et universités mettent en place dans le cadre du pôle d'excellence Cyber un « accord général de partenariat recherche cyber » regroupant 200 chercheurs, y compris dans le domaine juridique, pour travailler de concert, à l'écoute des besoins industriels, sur les différents points durs de la cybersécurité.

Le travail réalisé dans le cadre de ce Livre blanc ne doit pas rester sans suite et la SEE continuera à suivre attentivement l'évolution des travaux dans ce domaine. Elle se propose d'organiser en 2016, en liaison avec la nouvelle association Smart grids France, un forum qui permettra de proposer de nouvelles recommandations en fonction des avancées en matière de cybersécurité.

Annexes

Annexe 1 : Normes et guides

Plusieurs référentiels (normes et guides) sur la cybersécurité des systèmes électriques intelligents ont été élaborés ces dernières années Que ce soit, au niveau européen ou international, les principaux aspects de ce sujet y sont étudiés. Les enjeux, les acteurs concernés, les menaces, les mesures de sécurité y sont présentés d'une manière plus ou moins détaillée. La liste suivante présente une sélection de ces référentiels. Certains présentent un caractère normatif (voire réglementaire), fixant des exigences sans imposer des solutions, d'autres constituent des guides ou des recommandations de nature à faciliter le respect de ces exigences.

Normes

- ISO/CEI 27000 : la famille des standards ISO/CEI 27000 traite de la sécurité des informations sur un plan général. Les plus connus de ces standards sont l'ISO/CEI 27001 qui définit les exigences applicables aux systèmes de management de la sécurité de l'information (SMSI), l'ISO/CEI 27002 qui définit les bonnes pratiques applicables

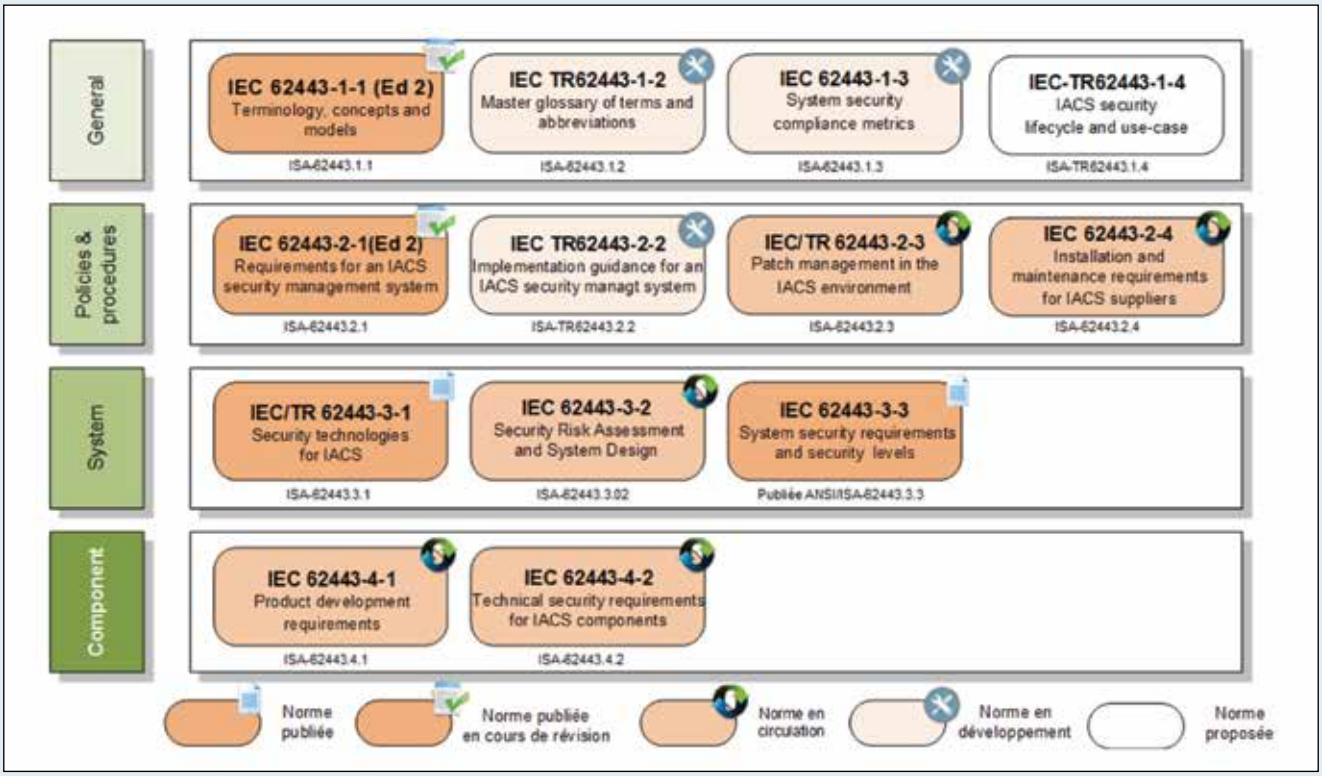

Figure 9 : Plan documentaire des normes et rapports techniques de la CEI 62443.
NB : Certains documents ne sont pas normatifs mais ont le statut de Technical Reports.

aux SMSI et l'ISO/CEI 27005 applicable à la gestion des risques liés à la sécurité de l'information.

- CEI 62443 : La famille des normes CEI 62443 "*Security for Industrial Automation and Control Systems*", résulte des travaux menés au sein du comité ISA-99. C'est un ensemble de normes et de rapports techniques spécifiquement destinée aux systèmes de contrôle industriel et notamment aux SCADA. Les documents constitutifs sont répartis en quatre niveaux, le document 62443-2-1 (nouvelle version) intègre les prescriptions de l'ISO 27002.
- CEI 62351 : La norme CEI 62351 vise à sécuriser les données et les communications dans les systèmes de puissance. Elle vient au-dessus de normes régissant les communications telles que la CEI 60870, la CEI 61850, la CEI 61968 et la CEI 61970.
- Les standards NERC-CIP (rendus obligatoires aux Etats-Unis) constituent un ensemble de prescriptions visant à protéger les actifs vitaux afin d'assurer un fonctionnement fiable du réseau de transport électrique nord-américain. (voir la liste à la section 1.5).

Réglementations

Arrêté du 4 janvier 2012 pris en application de l'article 4 du décret n° 2010-1022 du 31 août 2010 relatif aux dispositifs de comptage sur les réseaux publics d'électricité

Guides et rapports techniques

- ISO/CEI TR 27019 : Technologies de l'information – Techniques de sécurité – Lignes directrices de management de la sécurité de l'information fondées sur l'ISO/CEI 27002 pour les systèmes de contrôle des procédés spécifiques à l'industrie de l'énergie. Le document reprend la structure de l'ISO/CEI 27002 tout en y intégrant les spécificités des systèmes industriels, notamment par l'ajout de nouvelles sections.
- CEN-CENELEC-ETSI
  - "Smart Grid Reference Architecture" (2012-11)
  - "Smart Grid Information Security" (2014-12)
- Guides ENISA sur la sécurité des Smart Grids :
  - "Smart Grid Security" (2012-07)
  - "Appropriate security measures for Smart Grids" (12/2012)
  - "Proposal for a list of security measures for smart grids" (2013-11)
  - "Smart grid Threat Landscape and Good Practice Guide" (2013-11)
  - "Smart Grid Security Certification in Europe" (2014-12)
- ANSSI : Guide « Cybersécurité des systèmes industriels »
  - Maîtriser la SSI pour les systèmes industriels (2012)
  - Cas pratique (2012)
  - Méthode de classification et mesures principales (2014)
  - Mesures détaillées (2014)

• NIST
  - "NIST Interagency Report (NISTIR) 7628 Rev1 Guidelines for Smart Grid Cybersecurity" (2014-10)
  - "Guidelines for Smart Grid Cyber Security" (2010-8)

Par ailleurs des **documents informatifs**, résultant notamment de travaux européens, permettent de comprendre la problématique des REI et de se familiariser avec les normes qui leur sont applicables :

• ENISA, "Smart Grid Threat Landscape and Good Practice Guide" (2013-11)
• ENISA et Groupe de travail (EG2) de la Commission européenne, "Proposal for a list of security measures for smart grids" (2013-11)
• CEN-CENELEC-ETSI "SG-CG/M490/F Overview of SG-CG Methodologies" (2014-11)

Annexe 2 : Certification européenne de la cybersécurité des réseaux intelligents

La mise en place d'une certification européenne de la sécurité des réseaux intelligents a fait l'objet d'un rapport de l'ENISA publié en décembre 2014 : "*Smart grid security certification in Europe – Challenges and recommendations*".

Ce rapport souligne la nécessité de disposer de procédures de certification des REI pour donner aux utilisateurs l'assurance que les préoccupations de sécurité et de « privacité » ont été prises en compte et d'établir un niveau de confiance suffisant sur l'ensemble de la chaine des REI.

Le rapport constate qu'il existe ou que sont en cours de développement des procédures de certification dans certains pays et en relation avec certains référentiels normatifs. Ces approches sont fragmentées, non uniformisées et souvent coûteuses. Seuls quelques états (Allemagne, Grande-Bretagne (CPA) et Pays-Bas) ont développé des exigences spécifiques aux constituants des REI. Mais ces approches ne sont pas harmonisées.

En France, l'ANSSI a mis en place en 2008 une procédure de « *Certification de Sécurité de Premier Niveau* » qui constitue une alternative aux évaluations « *Critères Communs* », dont le coût et la durée peuvent être un obstacle, notamment lorsque le niveau de confiance visé est moins élevé. Cette certification n'est pas spécifique aux REI : elle s'appuie sur des critères, une méthodologie et un processus élaborés par l'ANSSI mais non reconnus au niveau international.

Les compteurs communicants sont régis par l'arrêté du 4 janvier 2012 relatif aux dispositifs de comptage sur les réseaux publics d'électricité. Cet arrêté précise à l'article 4 que « *les dispositifs de comptage mentionnés au présent article sont conformes à des référentiels de sécurité approuvés par le ministre chargé de l'énergie. Cette conformité est vérifiée par une évaluation et une certification conformément aux dispositions du décret du 18 avril 2002 susvisé* ».

Les questions relatives à la protection des données de caractère privé, c'est-à-dire relevant de la « privacité » font l'objet depuis juin 2014 d'un « *pack de conformité* » établi entre le CNIL et la FIEEC.

Au niveau international, la norme ISO/CEI 27001 « *Management de la sécurité de l'information* » donne lieu à certification. Celle-ci certifie que les organisations ont mis en place des politiques et des procédures pour développer, fabriquer ou mettre en œuvre des systèmes ou produits de traitement de l'information, notamment ceux rentrant dans les REI. Mais elle ne donne aucune assurance sur les produits proprement dits.

L'IASME (Information Assurance Standard for Small and Medium Sized Enterprises) est une version allégée de l'ISO/CEI 27001 développée en Grande-Bretagne.

Les normes ISO/CEI 15408 « *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité* » souvent appelées *« Critères communs »* définissent un cadre permettant à des industriels de développer des produits répondant à des exigences mutuellement reconnues et à des laboratoires de les tester en fonction de ces critères. Cette norme est appliquée avec succès aux "smart cards", elle pourrait être appliquée à certains éléments des REI, après définition de profils appropriés, mais n'est pas considérée, par le rapport de l'ENISA, comme susceptible d'être appliquée à l'ensemble de la chaîne des REI.

La norme ISO/CEI 19790 est un standard de certification applicable aux modules crytographiques.

La norme CEI 62443 (ex ISA99) "*Security for Industrial Automation and Control Systems*" est un ensemble de standards dont certains peuvent donner lieu à certification, soit de produits ou systèmes, soit d'organisation. Le standard CEI 62443-3-3 est le seul standard international pouvant donner lieu à la certification de systèmes sur la base de critères techniques classés selon sept exigences essentielles dénommées "*Foundational requirements*". Ce standard est complété par le standard CEI 62443-4-2 pour les composants des systèmes.

L'International Society of Automation (ISA) a mis en place avec les partenaires industriels intéressés un organisme de certification dénommé ISA Security Compliance Institute qui délivre un appel "*ISA Secure*" en utilisant des méthodes conforme à la norme ISO/CEI 17025 *« Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais »* (tableau 3) Ces labels sont reconnus au Japon mais ne sont pas distribués en Europe. Le tableau liste les

Référence	Objet de la certification	Méthodes ISA Secure
CEI 62443-2-4	Fournisseurs de service d'intégration et de maintenance	Standard d'origine WIB
CEI 62443-3-3	Systèmes de contrôle (en tant que « produits »)	SDLA et SSA
CEI 62443-4-1	Produits et systèmes (procédures de développement)	SDLA
CEI 62443-4-2	Composants	EDSA

Tableau 3 : Standards CEI 62443 certifiables et méthodes retenues par l'ISA Security Compliance Institute.

standards certifiables de la CEI 62443 avec les méthodes appliqués par l'ISA Secure.

Le rapport de l'ENISA propose de mettre en place une approche harmonisée au niveau européen qui définira les exigences essentielles auxquelles doivent satisfaire les procédures de certification en laissant libre les états de compléter par des « profils nationaux » prenant en compte les risques spécifiques identifiés après analyse de "national use cases".

Le rapport propose de développer l'approche harmonisée autour du modèle SGAM présenté à la section 1.4. et explique comment les approches normatives telles que celles de l'ISO/CEI 27001 ou ISO/CEI 62443 peuvent être mappées sur ce modèle.

Le rapport estime qu'il devrait être possible de partir de la méthodologie ("framework") par "*use cases*" proposée par le SG-IS dans son rapport SG-CG/SGIS "*Smart Grid Information Security*" (voir section 1.4.) pour développer un ensemble commun d'exigences reconnues tous les Etats membres ainsi que les profils spécifiques aux états. Le rapport note cependant que cette approche, si elle est considérée comme « une bonne approche », ne constitue pas à ce stade une méthode formellement reconnue au niveau européen.

Un "*steering committee*" européen veillerait à la conformité des schémas nationaux avec l'approche harmonisée de façon à assurer leur cohérence.

Annexe 3 : Les formations en cybersécurité

Les premières formations à la sécurité ont été créées en France au début des années 1990 sous la forme de masters spécialisés par l'ENSTA, Télécom ParisTech et le CERAM. Actuellement la formation à la sécurité des systèmes d'information et des réseaux est principalement enseignée dans les écoles publiques ou privées à orientation Informatique (INPG, ENSHEEIT, ENSEIRB, Télécom Nancy) ou Télécom (Télécom ParisTech, Bretagne, SudParis, Lille, Eurecom). Toutes ces écoles ont dans leur cursus une introduction à la sécurité dans les parties initiales (base scientifique de l'ingénieur) et une option de troisième année dédiée à la sécurité, voire en font un diplôme d'ingénieur sécurité spécifique (ENSICAEN (monétique), EPITA, ESAIP, ETNA (avec possibilité d'alternance), ESIGELEC, INSA Centre Val de Loire, TELECOM Lille, ENSIBS (formation ingénieur par alternance). Il convient d'ajouter aux formations ingénieurs, 25 masters universitaires orientés sur la sécurité et les mastères spécialisés (ESIEA, ESGI, INSA Lyon, Centrale Supélec/Télécom Bretagne, Télécom ParisTech, Télécom SudParis,..).

On peut estimer que chaque année environ 900 diplômés de niveau Bac+5 en sécurité sont formés par an.

Le site de l'ANSSI recense les formations en France sur la cybersécurité[33].

http://www.ssi.gouv.fr/administration/formations/formations-et-cybersecurite-en-france/

Ce recensement des formations montre que si les acteurs de la banque, de l'assurance, de l'informatique, de la défense, de l'aérospatial se sont mobilisés pour soutenir et orienter certaines des 47 formations évoquées ci-dessus sur leurs besoins spécifiques, ce n'est pas encore le cas du secteur économique de l'électricité.

En outre, dans le cadre du Pôle d'excellence Cyber mis en place dans le cadre du Pacte Défense Cyber par le ministre de la Défense[34], un catalogue des formations dispensées par ses partenaires a été élaboré et tenu à jour, en particulier suite aux évolutions étudiées avec ses partenaires industriels.

Annexe 4 : Les cryptosystèmes homomorphes

Bien que des cryptosystèmes homomorphes restrictifs (exclusivement additifs ou multiplicatifs) existent depuis des années, et possèdent de nombreuses applications (par exemple en traitement du signal), la théorie des cryptosystèmes pleinement homomorphes est encore récente et

[33] http://www.ssi.gouv.fr/administration/formations/formations-et-cybersecurite-en-france/

[34] http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber

pose encore plusieurs challenges, notamment en termes de performances. A ce titre, la fin de cette section fournit un état de l'art sur les techniques de cryptographie homomorphe et leur degré d'applicabilité.

À la fin des années soixante-dix, un article visionnaire de Rivest, Adleman et Dertouzos définit et analyse le potentiel applicatif d'une nouvelle notion qu'ils appellent les "privacy homomorphisms". Dans les faits, partant du constat que le cryptosystème RSA est homomorphe pour la multiplication, le produit de deux chiffrés est le chiffré du produit des deux clairs correspondants, ils finissent par conjecturer l'existence de cryptosystèmes à la fois sûrs et malléables, c'est-à-dire permettant de réaliser des calculs généraux directement sur des données chiffrées. Cette idée restera pendant longtemps une curiosité, les propriétés homomorphes toujours limitées à une opération de certains cryptosystèmes (ElGamal, Goldwasser-Micalli notamment) étant remarquées et tolérées car d'apparence bénigne en matière de sécurité.

Il faut attendre la fin des années 90 et en particulier le cryptosystème de Paillier pour que la recherche de cryptosystèmes homomorphes pour l'addition et la multiplication (on parle de systèmes pleinement homomorphes ou FHE) devienne la quête du Graal d'une partie de la communauté cryptographique. En effet, en sus d'offrir des performances tout à fait acceptables, le système de Pallier permet en outre de réaliser des additions entre deux chiffrés et également de multiplier un chiffré par un entier en clair. Il devient donc possible de réaliser n'importe quel opérateur linéaire (public) directement sur des données chiffrées et ce avec une efficacité raisonnable. Cette avancée suffit à donner naissance à un premier domaine de recherche appliqué pour la cryptographie homomorphe : le traitement du signal dans le domaine des chiffrés.

Il faut ensuite attendre 2009, pour que, contre toutes attentes, Craig Gentry alors à Standford propose, dans sa thèse de doctorat, une première construction crédible sur le plan de la sécurité et théoriquement efficace. Pour se fixer les idées, il convient néanmoins de préciser ce que les théoriciens entendent par efficacité. En effet, pour un niveau de sécurité l donné, un cryptosystème homomorphe est considéré comme efficace si le surcoût de performance lorsque l'on travaille dans le domaine des chiffrés est borné par un polynôme en l. Autant dire, et c'était malheureusement le cas pour cette première construction, que le degré du polynôme n'a pas besoin d'être très grand pour que ce surcoût de performance soit totalement prohibitif. De plus, la construction initiale de Gentry était d'une complexité redoutable. La conception d'un cryptosystème homomorphe n'est pas chose facile en raison d'un phénomène de bruitage dont l'amplitude augmente rapidement avec les calculs, surtout les multiplications, jusqu'à rendre le déchiffrement des résultats impossible. Pour résoudre ce problème, et c'est là sa contribution majeure, Gentry introduit une technique de débruitage aussi complexe que coûteuse, le bootstraping, qui revient à réaliser homomorphiquement une opération de rechiffrement (l'équivalent d'un déchiffrement suivi d'un chiffrement sans toutefois, magie de l'homomorphe, que les données ne soient jamais en clair).

Malheureusement, ce premier cryptosystème homomorphe, et plus généralement tous les systèmes à base de bootstraping connus à ce jour, s'avère beaucoup trop coûteux pour avoir une quelconque utilité pratique. La boîte de Pandore n'en est pas moins ouverte.

Les choses s'améliorent significativement courant 2012, Craig Gentry et deux coauteurs frappent à nouveau avec une approche radicalement différente : les cryptosystèmes (pseudo-) homomorphes à niveaux. Dans un système à niveaux, on ne travaille plus avec un seul cryptosystème mais avec une séquence de cryptosystèmes. En règle générale, les additions qui n'amplifient que très peu le bruit peuvent être réalisées au sein d'un même niveau mais, à contrario, les multiplications contraignent à changer de niveau. Toute la subtilité réside dans la combinaison d'un opérateur tensoriel qui étale le bruit et un opérateur de projection qui en réduit l'amplitude, au prix d'une incrémentation de niveau certes mais le bruit reste maitrisé sans avoir recours au bootstraping. À l'état de l'art début 2014, le système le plus performant connu est du à Zvika Brakerski (il a été publié pour la première fois en 2013 et a été ultérieurement optimisé dans d'autres publications). Il s'agit d'un système à niveaux dont les performances intrinsèques et le dimensionnement mémoire sont suffisamment maîtrisés pour envisager les premiers déploiements de techniques homomorphes dans des cadres d'utilisation réels suffisamment légers. Il est à noter que l'état de l'art de la cryptographie homomorphe avance à grands pas et qu'il semble se profiler une forme de loi de Moore, initialement proposée par le cryptographe français Carlos Aguilar Melchor : tous les 12 à 18 mois on gagne une racine carré en décroissance du surcoût de performance.

En parallèle de ces travaux pour l'essentiel menés par la communauté de la cryptographie, la communauté de la compilation et du parallélisme a commencé à s'intéresser finalement assez tôt (dès la fin 2010) aux techniques de cryptographie homomorphe en tant que nouvel environnement d'exécution aux propriétés singulières et au potentiel applicatif extrêmement riche. En particulier, il convient de souligner qu'un cryptosystème homomorphe fournit

des opérateurs qui travaillent au niveau bit (ou plus exactement au niveau de la représentation chiffrée d'un bit qui est — cryptosystèmes probabilistes obligent — une entité de relativement grande taille) c'est-à-dire à très bas niveau. Faire le lien, donc, entre un algorithme exprimé à l'aide d'un langage de haut niveau et un environnement d'exécution niveau binaire nécessite déjà une chaîne de transformations non triviales, un compilateur. Si, de plus, on souhaite que ce compilateur permette d'amoindrir au maximum le surcoût de performance par, notamment, recours au parallélisme alors il convient de se tourner vers le corpus technique de la compilation optimisante et de génération de code parallèle. A l'état de l'art de 2014, les résultats expérimentaux les plus convaincants ont été obtenus en combinant optimisations agressives des cœurs cryptosystèmes et génération de code parallèle optimisée. Dès lors, et ce sans diminuer le travail à venir pour traiter d'algorithmes plus complexes, il a été possible de démontrer l'exécution d'algorithmes bien réels (notamment des algorithmes de décision représentatifs pour le diagnostic médical) avec des performances acceptables (significativement inférieures à la seconde) et des niveaux de sécurité tout à fait respectables (128 bits). À noter également, une capacité d'interfaçage transparent des techniques homomorphes avec les primitives de cryptographie légères qui sont et seront déployées sur les objets communicants des REI.

A ce stade, l'enjeu est donc de capitaliser sur cette première génération d'outils afin de fournir une solution complète permettant d'exploiter la cryptographie homomorphe à coût raisonnable, tant en matière de génie logiciel qu'en matière de performance. Le tout en la validant dans le cadre de démonstrateurs sur des cas d'utilisation significatifs et en maintenant (encore du génie logiciel) une capacité à suivre et à bénéficier des avancées sur les cœurs de cryptosystèmes qui ne manqueront pas de se maintenir sur les prochaines années. Le domaine des REI et les développements technologiques autour de l'Internet des objets (IoT) fournissent un cadre idéal pour fournir une gradation de cas d'utilisation de complexité croissante pour la cryptographie homomorphe.

Annexe 5 : Principes d'identification et d'authentification

Pour les personnes

Les accès des personnes aux systèmes informatiques doivent répondre au triptyque « authentification, autorisation et audit ». Suivant les degrés de sécurisation retenus, les authentifications peuvent être simples ou fortes. Pour des organisations de taille conséquente, il est recommandé de s'appuyer sur des annuaires sécurisés. Ces annuaires embarquent les autorisations allouées.

Les accès aux systèmes informatiques des personnels doivent être tracés. Les actions engageantes vis-à-vis du procédé doivent être attribuables nommément à des personnes. Des processus doivent être mis en place pour accueillir de nouveaux intervenants, en cas de changement de leurs fonctions et en cas de départ de l'organisation.

Pour les systèmes critiques il est recommandé d'utiliser une authentification forte, généralement basée sur l'utilisation d'un composant matériel sécurisé (inviolable serait idéal mais impossible à réaliser) activable via une reconnaissance de l'utilisateur (PIN code, password, voire biométrie).

Pour les flux systèmes[35]

Les accès et communications des systèmes/applications doivent également répondre au triptyque authentification, autorisation et audit. Les échanges à l'intérieur du système et du système avec l'extérieur doivent être documentés dès les phases de conception et mis à jour pendant toute la durée de vie du système.

L'authentification des systèmes/applications pour des infrastructures sensibles doit aller au-delà des aspects purement logiciels et doit être intimement liée aux supports matériels, plus difficilement attaquables.

Les autorisations de communication doivent être vérifiées en entrée et en sortie de chaque système/application. Les flux doivent être surveillés et les dispositifs de contrôle des flux

La notion d'authentification, dans le cadre des échanges de données ou de l'authentification des composantes est généralement implantée via des techniques cryptographiques comme la signature électronique. Dans ce cas-là, la notion d'authentification est intimement liée à la notion de contrôle d'intégrité (le composant ou le message est bien un original non modifié). Il faut noter que ces schémas cryptographiques reposent sur l'utilisation d'algorithmes particuliers (généralement standardisés) utilisant un secret (clef cryptographique). La solidité (résistance aux attaques) est directement liée à la protection des données secrètes. Là encore, les dispositifs matériels dédiés, sont à privilégier pour les applications critiques et les hauts niveaux de sécurité.

Pour les composants du REI[36]

Une architecture de confiance doit être développée. Cette architecture implémente des contrôles d'intégrité généralisés du système destiné à vérifier que toutes ses

[35] Les flux systèmes : des réseaux et des personnes.

[36] Les composants : SCADA, centrale, data center, nœuds du réseau. NB : compte tenu de la diversité des REI de distribution, cette formulation est conservée.

composantes sont des originaux intègres (non modifiés de façon malveillante, incontrôlée ou non autorisée).

Cette architecture reprend les idées des architectures de confiance ("Trusted Computing") avec une « ancre » de sécurité, c'est-à-dire des composants matériels de haute sécurité stockant et manipulant les données sensibles (clefs cryptographiques, certificats, signatures). Par rapport aux architectures de type "Trusted Computing" avec un composant de type TPM ("Trusted Platform Module"), la vérification est généralisée à tous les composants du système (sous-systèmes, composantes matérielles, logicielles, etc.). L'ancre de confiance peut être assimilée à un TPM avec des fonctions complémentaires, comme la garantie d'authenticité présentée précédemment, mais également portant la garantie d'intégrité et d'authenticité des divers échanges (messages, communications) à l'intérieur du système.

Dans une version industrielle, ces ancres sont des composants intégrés sécurisés (anti-tampering, résistant aux attaques connues, certifiables aux niveaux EAL4+-5+ des Critères Communs) intégrés dans chacune des composantes du système (cartes mères, cartes de communication, compteurs, etc.).

Ces ancres implantent l'ensemble des primitives cryptographiques avancées et assurent une fonction de stockage sécurisé des informations critiques.

Une alternative existe et est généralement employée pour l'authentification des composantes d'un système reposant sur la signature électronique et la notion de certificat associé à chacune des composantes. Là encore, les notions d'intégrité et d'authenticité sont fortement imbriquées. Efficaces, ces schémas posent toutefois des problèmes dans certains cas d'utilisation :

- La sécurité de l'ensemble repose sur un tiers de confiance gérant les certificats. Une connexion permanente à ce tiers est souhaitable. L'existence d'une telle relation la confiance qui peut être accordée à ce tiers sur le long terme, et la relative complexité du schéma sont des freins à sa généralisation.
- La cryptographie évolue très vite. Des failles sont découvertes pratiquement journellement dans les standards, l'évolution des capacités de calcul rend caduques certaines fonctions de base ou taille de clef. Pour les systèmes industriels à durée de vie longue, des modifications à la fois des acteurs, des primitives et des caractéristiques des clefs est donc à prévoir, ce qui peut complexifier grandement le système.

Annexe 6 : Liste des contributeurs

Président du groupe de travail :
François Gerin – Président de la SEE.

ANSSI	Stéphane Meynet
Alstom Grid	Jean-Pierre Mennella
ATOS Worldgrid	Didier Joonekindt
ATOS Worldgrid	Hervé Barancourt
CEA	Nicole Mermilliod
CEA	Renaud Sirdey
CEA	Patrick Baldit
CEA	Florent Kichner
CEA	Laurent Olmédo
CEA – LETI	Alain Merle
EDF R&D,	Olivier Devaux
EDF R&D	Alia Fourati
ERDF	Alain Marty
ERDF	Marc Lagouardat
Gimelec	Nadi Assaf
ISA-France et SEE	Jean-Pierre Hauet
Orange	François Richard
RTE	Olivier Grabette
SEE	Gloria Kenter-Tuquerres
SEE/CST	Pierre Rolin
Siemens S.A.S	Jean-Christophe Mathieu
Siemens S.A.S et SEE	François Gerin
Siemens S.A.S.,	Annick Pellan-Baussan
Télécom-Bretagne	Frédéric Cuppens
Télécom-SudParis	Hervé Debar

Annexe 7 : Définitions

Ces définitions sont extraites des guides publiés par l'ANSSI. En dehors de leur document d'origine, certaines d'entre elles peuvent demander des compléments d'information.

A

Analyse d'un incident de sécurité : Procédé visant à collecter et analyser tout élément technique du système d'information permettant de comprendre le mode opératoire et l'étendue d'une compromission d'un système d'information.
Audit : Processus systématique, indépendant et documenté en vue d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits. Pour les besoins du Référentiel, un audit est constitué d'un sous-ensemble des activités d'audit de la sécurité d'un système d'information décrites au chapitre II et des recommandations assorties.
Auditeur : Personne réalisant un audit pour le compte d'un prestataire d'audit. Responsable d'équipe d'audit : personne responsable de l'audit et de la constitution de l'équipe d'audit, en particulier de la complémentarité de leur compétences.
Appréciation des risques (risk assessment) : Sous - processus de la gestion des risques visant à identifier, analyser et à évaluer les risques.
Authenticité : Propriété d'une information ou d'un traitement qui garantit son identité, son origine et éventuellement sa destination.
Autorité de cyberdéfense : Autorité nationale en charge de la défense des systèmes d'information, qui, dans le cadre des orientations fixées par le Premier ministre, décide des mesures que l'État met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale.
Attaque : Tentative d'atteinte à des systèmes d'information réalisée dans un but malveillant. Elle peut avoir pour objectif de voler des données (secrets militaires, diplomatiques ou industriels, données personnelles bancaires, etc.), de détruire, endommager ou altérer le fonctionnement normal de systèmes d'information (dont les systèmes industriels).

B

Bien : Tout élément représentant de la valeur pour le prestataire.
Bien : Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs. On distingue notamment les biens essentiels et les biens supports.
Bien essentiel : Information ou processus jugé comme important pour l'organisme. On appréciera ses besoins de sécurité mais pas ses vulnérabilités.
Bien support : Bien sur lequel reposent des biens essentiels. On distingue notamment les systèmes informatiques, les organisations et les locaux. On appréciera ses vulnérabilités mais pas ses besoins de sécurité.
Besoin de sécurité : Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné (disponibilité, confidentialité, intégrité,...).
Exemples : doit être disponible dans la journée, doit être connu du groupe projet.

C

Critères d'audit : Ensemble des référentiels, guides, procédures ou exigences applicables à la sécurité du système d'information audité.
Critère de sécurité : Caractéristique d'un bien essentiel permettant d'apprécier ses différents besoins de sécurité.
Exemples : disponibilité, intégrité, confidentialité, traçabilité.
Constats d'audit : Résultats de l'évaluation des preuves d'audit recueillies par rapport aux critères d'audit.
Compromission : Prise de connaissance, certaine ou probable, d'une information ou d'un support protégé par une ou plusieurs personnes non-autorisées. Voir également Intrusion.
Cloud computing (informatique en nuage) : Modèle permettant un accès aisé, à la demande et au travers d'un réseau, à un ensemble partagé de ressources informatiques.
Confidentialité : Propriété permettant de s'assurer que l'information ne soit accessible qu'aux personnes autorisées à y accéder (droit d'en connaître).
Cybersécurité : État recherché pour un système d'information lui permettant de résister à des événements d'origine malveillante susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services rendus par ce système.
Cyberdéfense : Ensemble des mesures techniques et non techniques permettant à un État de défendre les systèmes d'information jugés essentiels.

D

Disponibilité : Aptitude d'une fonction à rendre le service attendu en temps voulu et dans les conditions d'usage prévu.
Développement sécurisé (secure coding) : développement réalisé à l'aide de méthodes, règles, outillages et compétences humaines spécifiques dans le but de fournir un programme sécurisé.

E

Efficacité : Niveau de réalisation des activités planifiées et d'obtention des résultats escomptés.

État de l'art : Ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles à un instant donné, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine réglementaire.

Évènement lié à la sécurité de l'information : Occurrence identifiée de l'état d›un système, d›un service ou d›un réseau indiquant une faille possible dans la politique de sécurité de l'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité de l'information.

Externalisation (en anglais "outsourcing") : Démarche consistant à confier à un tiers tout ou partie d'une activité qui jusqu'alors était réalisée en interne.

Entité responsable : Personne morale ou physique qui a la responsabilité légale de la mise en place des mesures appropriées de cybersécurité pour le système concerné.

Événement redouté : Scénario générique représentant une situation crainte par l'organisme. Il s'exprime par la combinaison des sources de menaces susceptibles d'en être à l'origine, d'un bien essentiel, d'un critère de sécurité, du besoin de sécurité concerné et des impacts potentiels.

Exemple : une personne mal intentionnée (journaliste, hacker, concurrent) parvient à obtenir le budget prévisionnel de l'organisme, jugé confidentiel et publie l'information dans les médias.

F

Faille : Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

G

Gravité d'un incident de sécurité : Niveau d'impact de l'incident de sécurité sur le système d'information du commanditaire ou Quantification des conséquences d'un événement redouté ou d'un risque.

Gestion des risques (risk management) : Processus itératif de pilotage, visant à maintenir les risques à un niveau acceptable pour l'organisme. La gestion des risques inclut typiquement l'appréciation, le traitement, la validation du traitement et la communication relative aux risques.

[D'après ISO Guide 73 : Processus de management du risque : application systématique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de surveillance et de revue des risques].

H

Homologation de sécurité : Déclaration par l'autorité d'homo-logation, au vu du dossier d'homologation, que le système d'information considéré est apte à remplir sa mission conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels sont acceptés et maîtrisés. L'homologation de sécurité reste valide tant que le système d'information opère dans les conditions approuvées par l'autorité d'homologation et ceci pour une durée donnée.

[D'après IGI 1300 : Déclaration par l'autorité d'homologation, au vu du dossier d'homologation, que le système d'information considéré est apte à traiter des informations d'un niveau de classification donné conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels induits sont acceptés et maîtrisés. L'homologation de sécurité reste valide tant que le SI opère dans les conditions approuvées par l'autorité d'homologation].

I

Infogérance : Terme consacré à l'externalisation appliquée au domaine des systèmes d'information. Selon la définition de l'Agence française de normalisation (AFNOR), « l'infogérance est un service défini comme le résultat d'une intégration d'un ensemble de services élémentaires, visant à confier à un prestataire informatique tout ou partie du système d›information d'un client, dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de services et une durée définis ».

Incident de sécurité : Un incident de sécurité est indiqué par un ou plusieurs évènement(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité de compromettre les opérations liées à l'activité de l'organisme et/ou de menacer la sécurité de l'information.

Indicateur de compromission : Combinaison d'informations techniques représentatives d'une manifestation de compromission, qui peuvent être identifiées à partir de l'analyse d'un système, d'un code malveillant ou de traces réseau.

Intégrité : Propriété permettant de garantir l'exactitude, la fiabilité et l'exhaustivité des informations et des méthodes de traitement.

Investigation : Procédé visant à collecter et analyser tout élément technique du système d'information permettant de comprendre le mode opératoire et l'étendue d'un incident de sécurité sur un système d'information.

Impact : Conséquence directe ou indirecte de la non-réalisation des besoins de sécurité sur l'organisme et/ou sur son environnement.

Exemples : Sur la mission, sur la sécurité des personnes, financiers, juridiques, sur l'image, sur l'environnement.

Imputabilité : Capacité d'attribuer la responsabilité juridique d'une action à une personne physique ou morale.

Intrusion : Prise de contrôle, certaine ou probable, d'un système d'information ou de l'un de ses constituants par une ou plusieurs personnes non-autorisées.

Test d'intrusion : Test de la sécurité d'un système d'information consistant généralement à simuler le comportement d'un utilisateur ou d'un logiciel malveillant.

Information : [IGI 1300] tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.

Information ou support protégé : [IGI 1300] renseignement, procédé, objet, document, donnée informatisée ou fichier présentant un caractère de secret de la défense nationale (cf. art.1er du décret du 17 juillet 1998).

Information sensible non classifiée de défense : Information dont la confidentialité, la disponibilité et l'intégrité ne procèdent pas du secret de la défense nationale tel que défini par les articles 413:9 à 413:12 du code pénal et le décret 98:608, mais des dispositions spécifiques prévues dans la loi, notamment l'atteinte au secret professionnel (CP 226:13 et 226:14), les atteintes aux droits de la personne résultant des fichiers et des traitements informatiques (CP 226:16 à 226:24), et d'autres obligations légales ou contractuelles.

Intervenant : Employé ou sous-traitant d'un prestataire réalisant une mission pour celui-ci.

M

Mesure : Moyen de gérer un risque, comprenant la politique, les procédures, les lignes directrices, et les pratiques ou structure organisationnelles, et pouvant être de nature administrative, technique, gestionnaire ou juridique.

Mesure de sécurité : Moyen de traiter un risque de sécurité de l'information. La nature et le niveau de détail de la description d'une mesure de sécurité peuvent être très variables.

Menace : Cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme.

Maintenance : Ensemble des activités de type curative, préventive, corrective et évolutive permettant le maintien en condition opérationnelle (MCO) et maintien en condition de sécurité (MCS) d'un système.

O

Organisme : Ensemble d'installations et de personnes avec des responsabilités, pouvoirs et relations.

P

Partie prenante (stakeholder) : Personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité.

Politique (SSI) : Intentions et dispositions générales formellement exprimées par la direction d'une entité.

Prestataire d'audit : Organisme réalisant des prestations d'audit de la sécurité des systèmes d'information.

Preuves d'audit : Enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères d'audit et sont vérifiables.

Périmètre : Environnement physique, logique et organisationnel dans lequel se trouve le système d'information ou la portion du système d'information, sur lequel la prestation est effectuée.

Périmètre d'audit : Environnement physique, logique et organisationnel dans lequel se trouve le système d'information ou la portion du système d'information, sur lequel l'audit est effectué.

Prestataire : Organisme proposant une offre de service de détection des incidents de sécurité conforme au référentiel.

Prestataire de services de confiance : Organisme ou entité offrant des services consistant en la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique.

Q

Qualification d'un incident de sécurité : Détermination de la nature et de la gravité d'un incident de sécurité.

Qualification d'un prestataire de services de confiance : Acte par lequel l'Agence nationale de sécurité atteste de la conformité de tout ou partie de l'offre d'un prestataire de services de confiance à un référentiel d'exigences.

R

Rapport d'audit : Document de synthèse élaboré par l'équipe d'audit et remis au commanditaire de l'audit à l'issue de l'audit. Il présente les résultats de l'audit et en particulier les vulnérabilités découvertes ainsi que les mesures correctives proposées.

Recette : Ensemble de tests permettant de vérifier la conformité d'un équipement ou d'un système et de sa configuration par rapport à l'usage qui en est attendu. Ces tests sont généralement effectués sur le lieu d'installation par l'intégrateur ou l'utilisateur final. (Traduction anglaise : Site Acceptance Test.).

Recette Usine : Ensemble de tests permettant de vérifier la conformité d'un équipement ou un système à ses spécifications. Ces tests sont généralement effectués en usine par le constructeur. Traduction anglaise : Factory Acceptance Test.

Référentiel d'exigences : Document définissant les exigences applicables à un système, un produit ou à une famille de prestataires de services de confiance.
Risque : Combinaison de la probabilité d'un événement de sécurité et de ses conséquences ou Scénario, avec un niveau donné, combinant un événement redouté et un ou plusieurs scénarios de menaces. Son niveau correspond à l'estimation de sa gravité et de sa vraisemblance.

S

Sécurité d'un système d'information : Ensemble des moyens techniques et non-techniques de protection, permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles.
Sous-traitance : opération par laquelle le prestataire confie sous sa responsabilité à une entité tout ou partie de l'exécution d'un contrat conclu avec le commanditaire.
Spécification : Ensemble explicite d'exigences à satisfaire pour un produit ou un service.
Sûreté de fonctionnement : Étude des défaillances et des pannes d'un système visant à s'assurer de l'aptitude de celui-ci à accomplir des fonctions, dans des conditions définies et durant un intervalle de temps donnés. La sûreté de fonctionnement traite en particulier les propriétés de fiabilité, maintenabilité, disponibilité et sécurité (FMDS). La sécurité est entendue ici au sens des biens et des personnes. L'Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticités (AMDEC) est une méthode fréquemment employée en sûreté de fonctionnement.
Système d'information : Ensemble organisé de ressources (matériel, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information.
Systèmes d'information sensibles : Système qui traite d'informations dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre.
Systèmes d'information Diffusion Restreinte : Système d'informations sensibles qui traitent d'informations portant la mention Diffusion Restreinte ou ses équivalentes européennes ou internationales.
Scénario de menace : Scénario, avec un niveau donné, décrivant des modes opératoires. Il combine les sources de menaces susceptibles d'en être à l'origine, un bien support, un critère de sécurité, des menaces et les vulnérabilités exploitables pour qu'elles se réalisent. Son niveau correspond à l'estimation de sa vraisemblance.
Exemples : vol de supports ou de documents du fait de la facilité de pénétrer dans les bureaux ; piégeage du logiciel du fait de la naïveté des utilisateurs.
Surface d'attaque : Ensemble des ressources vulnérables d'un système donné, exposées à des attaques par des sources de menace extérieures via les différentes interfaces entre ce système et son environnement.
Source de menace (threat source) : Chose ou personne à l'origine de menaces. Elle peut être caractérisée par son type (humain ou environnemental), par sa cause (accidentelle ou délibérée) et selon le cas par ses ressources disponibles, son expertise, sa motivation...

T

Tiers : Personne ou organisme reconnu comme indépendant du prestataire et du commanditaire.
Traçabilité : propriété permettant de fournir les moyens de preuve et de contrôle sur les informations et les méthodes de traitement
Télémaintenance : action d'effectuer à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsable, des tâches de maintenance sur des installations techniques. Ceci implique notamment de pouvoir faire des modifications de paramétrages ou de programmes.
Sont aussi parfois regroupées sous ce terme les activités de télégestion et télédiagnostic.
Télédiagnostic : Action d'effectuer à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsable, un diagnostic d'installation technique. Ceci n'inclut pas de modification de paramétrage (lecture seule).
Télégestion : Action de prendre le contrôle à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsables, d'installations techniques géographiquement réparties (lecture/écriture).
Test unitaire : procédure permettant de vérifier le bon fonctionnement d'une partie précise d'un système (un de ses composants ou sous-ensemble). Les résultats des tests sont consignés dans un dossier de tests.

V

Vulnérabilité : Faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace.
Victime : Organisme dont tout ou partie de son système d'information fait l'objet d'un incident de sécurité d'origine malveillante.
Vraisemblance : Estimation de la possibilité qu'un scénario de menace ou un risque se produise. Elle représente sa force d'occurrence.

Annexe 8 : Acronymes utilisés dans le Livre blanc

ADEME : Agence de l'environnement et de la maîtrise de l'énergie
AES : Advanced Encryption Standard
AH : Authentification Header
AMDEC : Analyse des modes de défaillance, de leurs effets et de leur criticité
AMI : Appel à manifestation d'intérêt
ANSSI : Agence nationale de la sécurité des ystèmes informatiques
APT : Advanced Persistent Threats
CEI : Commission électrotechnique internationale
CEN : Comité européen de normalisation
CENELEC : Comité européen de normalisation en électronique et en électrotechnique
CIM : Computer Integrated Manufacturing
CIP : Critical Infrastructure Protection
CNIL : Commission nationale de l'informatique et des libertés
COFRAC : Comité français d'accréditation
COSEM : Companion Specification for Energy Metering
CPL : Courants porteurs en ligne
CRE : Commission de régulation de l'énergie
DCP : Données à caractère personnel
DES : Data Encryption Standard
DLMS : Device Language Message Specification
DMS : Distribution Management System
DNS : Directive nationale de sécurité
EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité
ECC : Elliptic Curve Cryptography
EDSA : Embedded Device Security Assurance
EG2 : Expert Group 2
ELD : Entreprise locale de distribution
EMS : Energy Manafement System
ENISA : European Network and Information Security Agency
ERDF : Électricité Réseau Distribution France
ERO : Energy Regulatory Office
ESP : Encapsulating Security Payload
ETI : Entreprises de taille intermédiaire
ETSI : European Telecommunications Standards Institute
FAI : Fournisseurs d'accès à Internet
FERC : Federal Energy Regulatory Commission
FIEEC : Fédération des industries électriques, électroniques et de communication
GDPR : General Data Protection Regulation
GOOSE : Generic Object Oriented Substation Events
GSM : Global System for Mobile Communications
H2M : Human to Machine
HINT : Holistic Approaches for Integrity of ICT-Systems
HTTP : HyperText Transfer Protocol
HTTPS : HyperText Transfer Protocol Secure
IACS : Industrial Automation & Control Systems (Systèmes d'automatisme et de contrôle industriel)
IASME : Information Assurance Standard for Small and Medium Sized Enterprises
ICMP : Internet Control Message Protocol)
ICS : Information commercialement sensible
IDS : Intrusion Detection System
IED : Intelligent Electronic Device
IETF : Internet Engineering Task Force
IF-MAP : Interface for Metadata Access Points
IIoT : Industrial Internet of Things
IoT : Internet of Things
IP : Internet Protocol
IPS : Intrusion Prevention System
Ipsec : Internet Protocol Security
ISA : International Society of Automation
ISAKMP : Internet Security Association and Key Management Protocol
ISO : International Organization for Standardization
ISTP : Institut supérieur des techniques de la performance
IT : Information technology
LoRa : Long Range
LPM : Loi de programmation miltaire
M2M : Machine to Machine
MOOC : Massive Online Open Course
NERC : North American Electric Reliability Corporation
NIST : National Institute of Standards and Technology
NSA : National Security Agency
NTP : Network Time Protocole
OIV : Opérateurs d'importance vitale
OLE : Object Linking and Embedding
OPC-UA : OLE for Process Control - Unified Architecture
OSI : Open Systems Interconnection
OTP : One Time Password
PERA : Purdue Enterprise Reference Architecture
PIA : Programme investissements d'avenir
PIN : Personal Identification Number
PLC : Programmable Logic Controller
PME : Petites et moyennes entreprises
PUF : Physical Unclonable Function
REI : Réseau électrique intelligent
RGS : Référentiel général de sécurité
RSA : Rivest, Shamir, Adleman

RTE :	Réseau de transport d'électricité
RTU :	Remote Terminal Unit
SA :	Security Association
SCADA :	Supervisory Control And Data Acquisition
SDLA :	Security Development Lifecycle Assurance
SEE :	Société de l'électricité, de l'électronique et des technologies de l'information et de la communication
SGAM :	Smart Grid Architecture Model
SG-CG :	Smart Grids Coordination Group
SGIS :	Smart Grid Information Security
SGIS-SL :	Smart Grid Information Security - Security Levels
SIEM :	Security Information and Event Management
SMSI :	Système de management de la sécurité de l'information
SOC :	Security Operating Center
SOG-IS :	Senior Officers Group for Information Systems
SSA :	System Security Assurance
TCG :	Trusted Computing Group
TCP :	Transport Control Protocol
TIC :	Technologies de l'information et de la communication
TLS :	Transport Layer Security
TPM :	Trusted Platform Module
UDP :	User Datagram Protocol
VPN :	Virtual Private Network
WAN :	Wide Area Network
WIB :	Wor+A1:C107king-party on Instrument Behaviour
WPA :	Wi-Fi Protected Access
ZSE :	Zones de sécurité

Ce Livre blanc est issu des travaux du groupe de travail « REI-cyber » constitué au sein du cercle des entreprises de la SEE. ***juin 2015***