Sûreté et sécurité : différences et complémentarités

Jean-René Ruault, Christophe Kolski, Frédéric Vanderhaegen, Dominique Luzeaux

Conférence C&ESAR 2015, Computer & Electronics Security Applications Rendez-vous, "Résilience des systèmes numériques" (23-25 Novembre), Rennes, France, pp. 23-37, 2015.

Sûreté et sécurité : différences et complémentarités

Jean-René Ruault*, Christophe Kolski*, Frédéric Vanderhaegen*,
Dominique Luzeaux**

* LAMIH-UMR CNRS 8201, Université de Valenciennes et du Hainaut-Cambrésis, Le Mont Houy, 59313 Valenciennes CEDEX 9
{prenom.com}@univ-valenciennes.fr
** rattaché à la Chaire Ingénierie des Systèmes Complexes de l'Ecole Polytechnique,
dominique.luzeaux@polytechnique.org

Abstract. Le monde actuel voit les technologies de l'information prendre une place croissante. La sécurité élargit les menaces affectant la sûreté des systèmes critiques mettant en œuvre ces technologies de l'information. Dans la perspective de la résilience des systèmes, qui est leur capacité à faire face à des événements imprévisibles, sans précédent, les enjeux de l'architecture système consistent à tisser les aspects relevant de la sûreté et ceux de la sécurité en construisant sur leur complémentarité. Nous proposons un modèle d'architecture orientée service intégrant la sécurité et la sûreté.

Keywords: Résilience, sécurité, sûreté, architecture système

1 Introduction

Les quinze dernières années ont vu le domaine de la sécurité des systèmes d'information évoluer radicalement. L'interconnexion puis la numérisation de la société et de l'ensemble des secteurs de l'économie, *via* notamment l'intégration des technologies de l'information potentiellement à l'ensemble des produits manufacturés, ont (re)placé l'information, davantage que le système d'information, au cœur de notre société. Même si le mouvement avait été amorcé au cours des années 90, la question centrale aujourd'hui est donc la sécurité de l'information comme le décrivent les normes ISO 27xxx (11, 12). La sensibilité à ces questions a été renforcée par la publication répétée d'attaques informatiques de toutes natures.

La résilience devient donc un enjeu tant économique qu'opérationnel, et les notions habituelles autour de la sécurité ne suffisent plus à la garantir. Dans cet article, nous nous intéresserons donc à la notion de sûreté, habituellement employée dans d'autres contextes, et nous décrirons l'apport mutuel de ces différentes notions, en les articulant au sein d'une architecture de contrôle de haut niveau par rapport aux architectures organique, fonctionnelle et physique du système.

Après avoir présenté la sécurité (protection des systèmes vis-à-vis d'attaques malveillantes) et la sûreté (protection des systèmes vis-à-vis du danger) (18), nous analysons leur complémentarité ainsi que leurs impacts sur l'architecture du système.

Nous proposons un modèle s'appuyant sur l'architecture orientée service et intégrant la sécurité et la sûreté.

La conclusion met en évidence des perspectives d'approfondissement, en particulier pour concevoir une architecture cohérente et qui soit évolutive.

2 Sécurité et sûreté : une nécessaire complémentarité

Sûreté et sécurité sont des termes employés dans de nombreuses disciplines, souvent avec des significations différentes, voire diamétralement opposées, d'une discipline à une autre (18). Dans ce contexte, nous reprenons à notre compte les définitions de sûreté et de sécurité (18), respectivement protection contre des accidents et protection contre des comportements malveillants.

2.1 La sécurité

Issue du chiffre[1], c'est-à-dire de l'échange d'information sécurisé dans le domaine militaire, la sécurité des systèmes d'information (SSI) est la démarche qui consiste à obtenir une confiance jugée suffisante dans la capacité d'un système d'information à respecter ses critères de sécurité face à des menaces intentionnelles.

Les critères formulés dans une expression de besoin de sécurité sont relatifs aux propriétés suivantes :

- Confidentialité : propriété d'un système d'information qui interdit l'accès à une information à quiconque n'est pas autorisé à en prendre connaissance.
- Intégrité : propriété d'un système d'information qui interdit qu'une information ou que le traitement d'une information soit indûment modifié.
- Disponibilité : propriété d'un système d'information qui permet qu'une information ou un traitement soit toujours accessible à quiconque est autorisé.

A ces critères de base sont parfois ajoutés d'autres critères comme par exemple ;

- Non répudiation : propriété d'un système d'information qui rend impossible à un utilisateur de nier avoir lu, modifié ou transmis une information.

La sécurité des systèmes d'information s'attache à faire respecter ces critères face à des attaques. La SSI n'est pas une performance obtenue au moment de l'acquisition du système et qui restera pérenne pendant toute son existence. C'est une démarche continue mise en œuvre tout au long du cycle de vie du système de l'expression de besoin au démantèlement. La sécurité d'un système d'information ne se prouve pas. Il s'agit d'acquérir un niveau de confiance jugé satisfaisant dans la capacité du système à résister aux attaques à faire respecter les critères de sécurité demandés. Ce niveau de confiance est atteint par le choix judicieux des intervenants, par une architecture accompagnée de certains produits correctement administrés, par une infrastructure et

[1] Service d'une armée ou d'une ambassade chargé de coder les messages secrets afin qu'ils ne puissent pas être dévoilés.

une organisation adaptée, par une couverture de test, une évaluation, un audit, une maintenance, …

Elargissant le périmètre de la SSI, perçue comme statique, la cybersécurité, perçue comme plus dynamique, peut être définie comme étant un ensemble des moyens organisationnels, techniques et humains assurant la confidentialité, l'intégrité et la disponibilité de l'information. La cybersécurité va au-delà du système d'information lui-même (11).

En conformité à ces normes, entre autres, des méthodes ont été élaborées et sont mises en œuvre pour assurer la sécurité des systèmes d'information. Ainsi, la méthode EBIOS, pour « expression des besoins et identification des objectifs de sécurité » comprend des éléments de gestion des risques (3) et des propositions d'outillage adaptées (2). La fiche d'expression rationnelle des objectifs de sécurité (FEROS), quant à elle, est une méthode d'évaluation des risques adaptée à la sécurité (23). Ces risques se déclinent en termes d'espionnage, de sabotage, d'écoute, d'accès illégitime, d'abus de droit et s'appuient sur des dispositifs matériels et logiciels que sont, entre autres, les portes dérobées, les chevaux de Troie, les vers, les logiciels espions. Lutter contre ces menaces consiste à détecter les intrusions et à générer des alertes (10). Ces enjeux, initialement prégnants dans le domaine militaire, concernent dorénavant tout autant le domaine civil, à la hauteur des enjeux économiques, sociaux, politiques, sociétaux, des échanges d'information qu'autorisent les technologies de l'information.

La résilience du système, au sens de la sécurité du système d'information – ce dernier étant considéré sous son acception système large, y compris sa composante qu'est la connexion –, se décline en des plans de continuité d'activité (PCA) et de reprise d'activité (PRA), ou leur déclinaison aux spécificités du système considéré (7, 8).

Parmi les impacts possibles d'une attaque – qu'elle soit de type déni de service ou piratage avec usurpation d'identité ou de droit –, les dysfonctionnements induits au niveau des infrastructures critiques peuvent générer des accidents catastrophiques. En effet, les systèmes actuels ayant de plus en plus une composante informatique, à la fois capteurs et actionneurs (télémaintenance), la sécurité voit son périmètre et son domaine d'application évoluer, débordant le domaine d'application d'origine pour s'approcher de ceux de la sûreté, c'est-à-dire la protection vis-à-vis du danger.

2.2 La sûreté

La sûreté est l'état d'être sauf, c'est-à-dire être protégé contre les conséquences de défaillances, d'erreurs, d'accidents, et de tout événement indésirable. Elle peut être aussi définie comme le contrôle de dangers identifiés pour maintenir un niveau de risque acceptable (16). Elle est alors vue comme un sous-objectif de la sûreté de fonctionnement, notion issue des activités humaines et industrielles à risque et formalisée par la cyndinique qui est la science du danger (9, 15). Elle s'appuie sur une démarche de type gestion des risques, qui consiste à identifier les événements redoutés et à évaluer tant la gravité de leurs conséquences que la probabilité d'occurrence de tels événements redoutés. La démarche consiste à éviter les accidents et, si des accidents surviennent, à en réduire les effets en mettant en œuvre des dispositifs de protection tels que des barrières.

Une telle démarche atteint ses limites dès lors que les dispositifs de sécurité sont désactivés, que les barrières sont franchies ou que les évolutions du contexte opérationnel engendrent de nouveaux événements redoutés qui ne peuvent pas être identifiés en phase amont des projets. Ces situations amènent à repenser la sécurité du point de vue de la résilience pour prendre en compte les situations réelles opérationnelles et donner aux opérateurs les moyens de piloter à vue.

Si, à l'origine, les événements redoutés de la sécurité relevaient de perturbations non prévues ou de défaillances, c'est-à-dire de comportement non volontaire, la généralisation des technologies de l'information et l'utilisation de ces technologies de l'information dans des dispositifs de commande et de contrôle d'infrastructures critiques, ainsi que dans les dispositifs de sécurité, ouvrent la voie à des comportements malveillants, c'est-à-dire des événements redoutés de nature intentionnelle. Ces comportements malveillants sont peu traités et pris en compte dans le domaine de la sûreté qui s'appuie principalement sur les modèles de défaillance des composants du système.

Par ailleurs, que ce soit dans le cadre de la sécurité ou dans celui de la sûreté, lorsqu'un incident se produit, qu'il soit intentionnel ou pas, il est nécessaire de le détecter et d'émettre une alerte pour traiter l'incident et sa cause. Le système d'alerte doit lui-même être sécurisé pour éviter qu'il ne soit leurré.

2.3 Complémentarité entre sûreté et sécurité

Notre article s'inscrit dans ce contexte de complémentarité entre sécurité et sûreté, et plus précisément, dans le cadre de la résilience des systèmes sociotechniques, c'est-à-dire : leur capacité à réagir et à récupérer après une perturbation, avec un minimum d'effet sur la stabilité de leur dynamique (17), en particulier pour faire face à des événements perturbateurs imprévisibles, sans précédent (14). La prise en compte de ces événements perturbateurs imprévisibles, sans précédent, ne peut être faite qu'en exploitation du système, en surveillant l'état du système et de son environnement afin d'alerter les opérateurs et leur permettre de naviguer à vue (22).

La sûreté et la sécurité ont pour point commun de préconiser de surveiller le système et d'alerter lorsqu'un événement redouté advient (10, 22). Elles ont aussi pour point commun que les barrières élaborées d'une part pour éviter qu'un événement redouté ne survienne, d'autre part pour réduire ses conséquences en cas de survenue, sont contournées. Les origines du contournement de ces barrières sont différentes dans les deux cas. Dans le domaine de la sûreté, il est principalement dû à l'accroissement des performances (19, 1) et aux évolutions de l'environnement opérationnel (21). Dans le domaine de la sécurité, il traduit un comportement intentionnel et malveillant, toute l'énergie étant consacrée à contourner ou détruire les barrières mises en place.

Dans tous les cas, il est nécessaire que les opérateurs sachent quel est l'état des barrières et qu'ils soient informés des attaques dont elles peuvent être la cible. Les opérateurs doivent aussi être informés du niveau de danger et de la présence, ainsi que de la contamination du système par un agent malveillant. Ils doivent alors avoir la capacité à naviguer à vue (i.e. assurer la viabilité du système sans disposer de modèle *a priori*

fiable de l'interaction de l'environnement avec le système), sur le plan de la sûreté, mais aussi à découpler ou arrêter des composants contaminés afin de limiter la contamination d'autres composants du système, et décontaminer ces composants avant de les remettre en fonctionnement, sur le plan de la sécurité.

Les analyses préliminaires de risques ainsi que la conception et la réalisation des dispositifs de sûreté, y compris les dispositifs de surveillance et d'alerte (22), doivent prendre en compte les exigences de la sécurité. En effet, dès lors que des composants d'un système échangent des informations, *a fortiori* lorsque des systèmes différents échangent des alertes, les informations échangées ne doivent pas être accessibles à ceux qui ont des comportements malveillants (confidentialité). Les informations échangées ne doivent pas être modifiées, corrompues, pour générer des fausses alarmes ou pour cacher des alarmes (intégrité). Et les dispositifs de sûreté ne doivent pas être détournés de leur usage à des fins de nuisance (non-répudiation). Enfin, les défauts de sécurité doivent être pris en compte comme étant des sources potentielles de danger. Ainsi l'analyse des menaces de la sécurité rejoint et complète l'analyse des modes de défaillance de la sûreté.

Le tableau 1 met en perspective les caractéristiques communes et les caractéristiques spécifiques de la sûreté et de la sécurité.

	Sûreté	**Sécurité**
Démarche d'analyse des risques	Identification des événements redoutés, de leur probabilité d'occurrence et de leurs conséquences	Identification des menaces, de leur vraisemblance, des vulnérabilités du système cible et de leurs conséquences
Caractéristique	Accident ou défaillance d'un composant du système (événement non intentionnel)	Attaque (événement intentionnel, malveillant)
Anticipation	Simulation pour mesurer la performance du système face à des événements redoutés prévisibles	Absence de mesure de performance du système
Méthode à mettre en œuvre	Méthodes de la sûreté de fonctionnement (AMDEC…)	EBIOS, FEROS
Dispositif de sécurité	Barrières, redondance, réduction des modes communs …	Pare-feu, accès par diode, système de détection d'intrus …

Tableau 1. Analyse comparée de la sûreté et de la sécurité.

3 Modèle d'architecture orientée service intégrant la sûreté et la sécurité

Nous proposons un modèle d'architecture orientée service intégrant la sûreté et la sécurité.

Ce modèle d'architecture vise à détecter les accidents, les dérives du point de la sûreté et les actes malveillants, les intrusions, du point de vue de la sécurité.

Nous présentons l'approche fonctionnelle de la complémentarité entre sûreté et sécurité puis nous regardons les impacts de la prise en compte de la sécurité et de la sûreté, avant de présenter le modèle d'architecture orientée service.

3.1 Approche fonctionnelle de la complémentarité entre sûreté et sécurité

Tant dans une démarche de sécurité (5, 6, 20), que dans une démarche de sûreté (22), il est recherché de surveiller l'état du système en fonctionnement et d'alerter lorsqu'une situation particulière (intrusion, proximité par rapport à une zone de danger) survient.

Le tableau 2 montre la comparaison des deux dimensions que sont sécurité et sûreté, vis-à-vis des trois fonctions que sont surveiller, évaluer les risques et alerter.

	Sûreté	**Sécurité**
Surveiller	Obtenir une représentation de l'environnement du système Obtenir une représentation de la dynamique de système	Surveillance de l'intégrité et gestion du changement Détection d'attaque Surveillance des équipements / automates Surveillance de la communication
Evaluer les risques	Évaluer des dérives Évaluer la proximité du danger	
Alerter	Alerter et conseiller les opérateurs	

Tableau 2. Analyse comparée de la sûreté et de la sécurité.

Il y a de fortes similarités quant à la surveillance des systèmes. Au regard des documents analysés (5, 6, 20), l'évaluation des risques et l'alerte semblent moins formalisées, relevant peut-être d'une intervention manuelle. Pour autant, l'évaluation de la menace ainsi que l'alerte sont des activités clef de la sécurité.

Nous proposons d'appliquer ces trois fonctions à la sûreté et la sécurité pour contrôler l'une et l'autre lorsque le système est mis en œuvre, au stade d'utilisation.

Par ailleurs, nous complétons cette approche en identifiant, sans prétendre faire une analyse fonctionnelle systématique de la sécurité, ce qui nécessiterait plus d'un article, les fonctions de sécurité suivantes relatives à la détection et au traitement approprié d'actes malveillants et d'intrusion.

- surveiller les systèmes opérants et détecter les actes malveillants et les intrusions qu'ils subissent ;

- tant que les systèmes sont exempts d'agent contaminant, émettre des patentes nettes[2] attestant de leur état de santé ;
- en cas d'actes malveillants, d'intrusion, lancer une alerte pour évaluer le périmètre de la zone compromise, l'identité de l'agent compromettant, les fonctions atteintes, leur criticité, et les fonctions alternatives non compromises susceptibles de limiter la dégradation du service ;
- réévaluer le niveau de sûreté, en fonction des actes malveillants détectés et de leurs conséquences, en tenant compte de la criticité du système, de son niveau de sûreté actuel et des conséquences des actes malveillants ;
- confiner les systèmes atteints, retirer les patentes nettes des systèmes contaminés, les blanchir, les mettre en quarantaine jusqu'à retour d'une situation saine, exempte d'agent compromettant ;
- déconfiner les systèmes qui ont recouvré un fonctionnement sécurisé et leur délivrer les patentes nettes leur permettant de fournir les services à leurs clients et à consommer ceux de leurs fournisseurs.

Les patentes nettes peuvent être complétées par des patentes brutes[3] pour les systèmes modérément infectés ou dont le fonctionnement est potentiellement dangereux, hors de sa zone de fonctionnement sûr. Cette patente brute permet de conserver opérationnels des systèmes dès lors que leur fonctionnement n'est pas dangereux pour les autres. Pour des raisons de sûreté, les systèmes critiques ne peuvent faire appel qu'à des services de systèmes présentant des patentes nettes. En particulier, des systèmes non critiques peuvent faire appel aux services de systèmes présentant des patentes brutes pour limiter les conséquences de délestage.

Après avoir présenté les fonctions de sécurité et de sûreté, nous poursuivons en appréhendant les impacts de la sûreté et de la sécurité sur l'architecture du système.

3.2 Architecture du système : impacts de la sûreté et de la sécurité

L'intégration de la sûreté et de la sécurité a des conséquences sur l'architecture du système. En effet, l'architecture fonctionnelle résultant des exigences de sûreté et ses dispositifs adaptés (22), ainsi que l'architecture résultant de la prise en compte de la sécurité, doivent être tissées avec l'architecture fonctionnelle « traditionnelle » du système – nous nous plaçons ici dans le paradigme habituel séparant les exigences fonctionnelles et non fonctionnelles, où les problématiques qui nous intéressent ici sont souvent qualifiées de « ities »[4] (13). Ces deux architectures de sécurité et de sûreté sont en fait transverses aux fonctions du système, et donc à l'architecture fonctionnelle basée sur la décomposition des fonctions du système et évidemment à

---

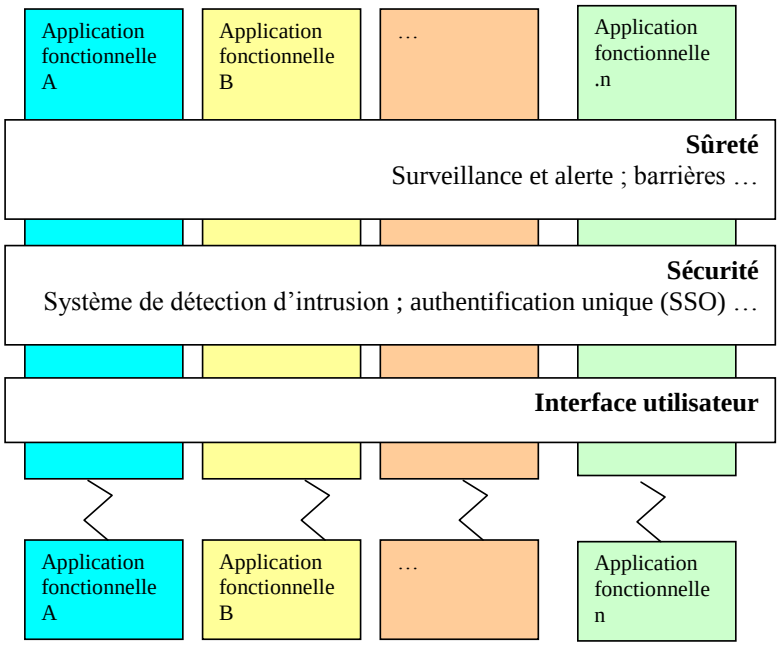
[2] Dans la marine marchande, une patente nette est une attestation légale qui constate qu'un navire est sorti d'un pays exempt de maladies contagieuses.

[3] Certificat de santé délivré dans les ports aux vaisseaux attestant qu'ils sont partis d'un pays infecté.

[4] Les « ities », suivant l'usage anglo-saxon, dénotent l'ensemble des propriétés non fonctionnelles d'un système et des disciplines afférentes : sécurité, utilisabilité, maintenabilité, portabilité, entre autres.

l'allocation de ces fonctions à des composants du système (cf. Figure 1). Ainsi, chaque fonction et chaque composant résultant dans l'allocation – sans présager d'une quelconque univocité entre les deux – sont affectés par ces deux dimensions (sûreté et sécurité). Pour que l'architecture fonctionnelle et l'architecture organique puissent évoluer facilement avec le minimum d'impacts sur ces deux dimensions, par exemple pour prendre en compte de nouveaux besoins, de nouvelles solutions technologiques, il est souhaitable que ces architectures soient découplées. Il en est de même pour pouvoir prendre en compte de nouvelles menaces de sécurité et de nouveaux événements redoutés de sûreté en minimisant les impacts sur l'architecture fonctionnelle et l'architecture physique du système. La conception orientée aspect (24) permet de séparer ce qui relève, d'une part des architectures fonctionnelle et organique du système, et d'autre part des dimensions de sécurité et de sûreté.

Figure 1. Architecture du système global, de la sûreté et de la cybersécurité



Si découpler les architectures fonctionnelle et organique du système des dimensions de la sécurité et de la sûreté est une première étape, il est aussi souhaitable de découpler, pour partie, ce qui relève de la sûreté et de la sécurité. En effet, ces deux dimensions évoluent à des rythmes différents. Si la stabilité est principalement recherchée pour la sûreté, avec souvent de fortes exigences de certification – comme dans le domaine aéronautique –, la prise en compte des menaces émergentes impose un rythme d'évolution plus élevé pour la sécurité afin de pouvoir déployer rapidement des solutions de sécurité adaptées à des menaces émergentes. Cela affecte directement les architectures des dispositifs de sûreté et de sécurité.

En contrepartie, découpler complètement la sûreté et la sécurité a pour conséquence de multiplier les capteurs et les dispositifs d'alerte, ce qui peut nuire à l'architecture globale du système et à ses performances, puisque chaque mesure, à un titre ou à un autre, perturbe le fonctionnement du système. De plus, certaines informations peuvent être pertinentes tant pour la sûreté que pour la sécurité. Il est donc nécessaire de s'assurer que des composants qui puissent être mutualisés (dispositifs de surveillance, dispositifs d'alerte) ne soient pas affectés par des rythmes d'évolution différents.

Dans ce contexte, les activités d'architecture du système globale, d'architecture de sûreté et d'architecture de sécurité doivent être menées de concert pour déterminer les dispositifs surveillés en fonction des risques identifiés (défaillance, attaque…), les capteurs nécessaires à la surveillance de ces dispositifs, les informations issues de ces capteurs et nécessaires pour alerter les opérateurs, les chaînes de ce traitement de ces informations, les alertes élaborées et les chaînes de transformation de ces alertes pour informer les opérateurs en fonction de leurs activités, des dispositifs d'interface utilisateur mis en œuvre et en fonction des contextes d'usage. L'analyse doit être menée au regard des contraintes pesant sur ces éléments (dispositifs surveillés, capteurs, informations recueillies, alertes…), en particulier leur niveau de pertinence tant pour la sûreté que pour la sécurité, ainsi que leurs rythmes d'évolution différents.

De plus, mener ces activités d'architecture de concert permet de prendre en compte les interactions entre la sécurité et la sûreté. Il faut évaluer les conséquences en rapport à la sûreté d'actes malveillants ou d'intrusion. En contrepartie, il faut aussi évaluer les conséquences en rapport à la sécurité d'un accident ou d'un fonctionnement du système en dehors de sa zone de mise en œuvre de façon sûre. Les actions menées suite à un acte malveillant doit prendre en compte, outre les conséquences de cet acte malveillant, les conséquences probables pour les systèmes critiques en interaction avec le système attaqué. Cela se traduit par une politique de confinement qui doit être mesurée. Suffisante pour confiner une intrusion malveillante, sans excès, sinon les systèmes confinés n'interagissent plus entre eux et globalement, ils ne sont plus disponibles. De plus, confiner un système suppose que cela ne mette pas en péril son fonctionnement sûr et donc sa sûreté.

La sécurité et la sûreté doivent être intégrées pour que ces interactions puissent être efficaces et assurer tat la sécurité que la sûreté des systèmes concernés.

Le modèle d'architecture orientée service que nous présentons maintenant intègre la sécurité et la sûreté.

3.3 Vers un modèle d'architecture orientée service

Après avoir les besoins d'intégration de la sécurité et de la sûreté, nous proposons une architecture multi-niveaux couvrant la sécurité et la sûreté et permettant aux systèmes d'interagir de façon sûre et sécurisée.

Cette architecture comprend trois niveaux.

- le niveau des systèmes opérants (22) consistant à :
  - fournir des services aux systèmes qui en sont clients, de façon sécurisée et sûre ;

  - utiliser de façon sécurisée et sûre les services fournis par les systèmes ;
  - émettre des alertes de sécurité en cas de détection d'agent compromettant, d'attaque, précisant le système ciblé et l'identité de l'attaquant ;
  - émettre des alertes de sûreté en cas d'accident ou de défaillance détectée, ou en cas de proximité d'une zone de danger
- le niveau du système de sûreté et sécurité :
  - détecter les alertes de sécurité et de sûreté et mettre en place la protection appropriée des systèmes, en particulier des systèmes critiques ;
  - gérer les annuaires des services, des clients, des abonnements, avec les niveaux d'habilitation et les niveaux de priorité associés et des menaces identifiées ;
  - après contrôle de l'absence d'agent compromettant, fournir aux systèmes les patentes nettes dont ils ont besoin ;
  - lancer les défis auprès des systèmes opérants et enregistrer leurs résultats ;
  - confiner, mettre en quarantaine, blanchir et, après contrôle de l'absence d'agent compromettant, lever la quarantaine ;
  - enregistrer les attaques,
  - évaluer les nouvelles menaces non encore répertoriées ;
- le niveau du système de surveillance du système de sûreté et de sécurité :
  - lancer les défis auprès du système de sécurité et de sûreté et enregistrer leurs résultats ;
  - s'assurer de l'absence de compromission du système de sécurité et de sûreté.

Pour chaque système, et pour chaque élément de ces systèmes, il est nécessaire d'identifier le niveau de criticité, tant au niveau de la sûreté que de la sécurité. L'objectif est de protéger les systèmes ayant un niveau élevé de criticité et les ressources dont ils ont besoin. Cette démarche permet d'élaborer une politique de confinement visant, pour la sûreté, à limiter les impacts sur l'environnement du système, et pour la sécurité, à limiter les entrées non autorisées. Cela consiste à réduire le couplage des systèmes critiques et d'augmenter leur autonomie. Cela peut se traduire par la redondance en utilisant des sources différentes et variées pour les ressources des systèmes critiques. Cela se traduit par la priorité attribuée aux systèmes critiques pour accéder à des ressources communes sujettes à la concurrence des autres systèmes.

Il est possible d'élaborer des règles pour accéder à un service donné :

- le système requérant ce service doit en avoir le droit, ce qui suppose une authentification de ce système client et la publication de son niveau d'habilitation l'autorisant à requérir ce service ;
- le système requérant ce service doit exprimer s'il est critique et prioritaire et, si oui, quel est son niveau de priorité ;
- le système fournissant ce service doit exprimer le niveau d'habilitation exigé pour accéder à ce service et les règles de priorité pour accéder au service ;
- le système requérant et le système fournissant ce service doivent présenter une patente nette délivrée par le système de sécurité et de sûreté justifiant qu'ils sont exempts d'agent compromettant.

Cette architecture multi-niveaux permet de différencier plusieurs types de flux. Ce sont, d'une part les flux des services entre systèmes opérants, et d'autre part, les flux relatifs à la sécurité et à la sûreté, entre le système de sécurité et de sûreté et les systèmes opérants, ainsi qu'entre le système de surveillance du système de sécurité et de sûreté et ce dernier.

Le diagramme N^2 ou matrice de couplage (cf. Figure 2) permet de montrer les flux entre systèmes opérants et les caractéristiques de sécurité et de sûreté de ces flux. Dans ce cas de figure, nous avons trois systèmes opérants différents, réciproquement A, B et C. Nous supposons que le système C est un système critique.

Le système A fournit le service A' aux systèmes B et C. Le système B fournit le service B' au système A et le service B'' au système C. Enfin, le système C fournit le service C' au système A. Outre les propriétés opérationnelles de ces services, ces derniers présentent des caractéristiques de sécurité et de sûreté, à savoir le niveau d'habilitation requis pour accéder au service (sécurité), le niveau de priorité du service (sûreté), ainsi que la patente nette attestant que le service fourni est exempt d'agent compromettant. Cette patente nette est particulièrement importante pour les services A' et B' puisqu'ils sont consommés par le système critique C. Le système critique C est prioritaire par rapport au système B pour consommer le service A'.

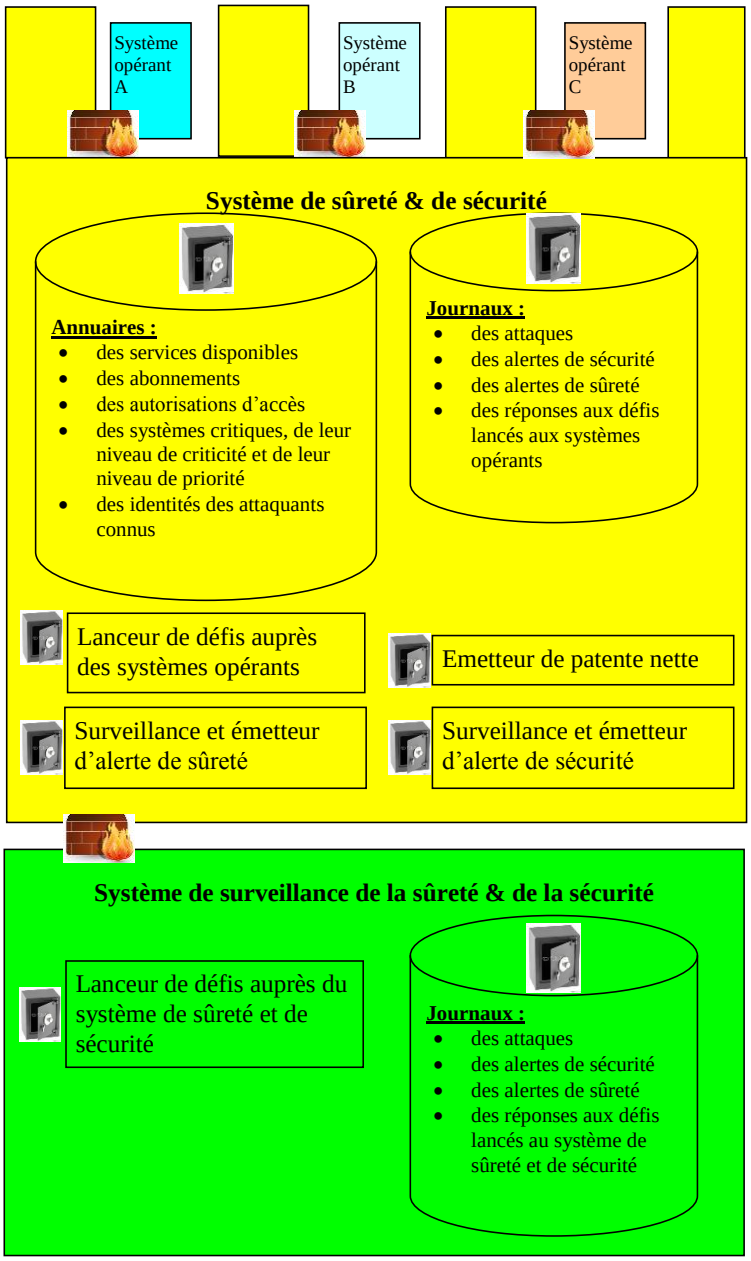
Figure 2 : Matrice N^2 décrivant les flux de services entre systèmes opérants.

Système opérant A	Service A' (niveau d'habilitation requis, niveau de priorité, patente nette)	Service A' (niveau d'habilitation requis, niveau de priorité, patente nette)
Service B'' (niveau d'habilitation requis, niveau de priorité, patente nette)	Système opérant B	Service B' (niveau d'habilitation requis, niveau de priorité, patente nette)
Service C' (niveau d'habilitation requis, niveau de priorité, patente nette)		Système opérant C (système critique)

L'architecture proposée en Figure 3 s'appuie sur une architecture orientée service et sépare les différents systèmes opérants (A, B et C) par le système de sécurité et sûreté. Cette architecture reprend et complète l'architecture sécurisée des cartes à microprocesseurs de type Java Card. Les systèmes opérants déclarent au système de sûreté et de sécurité les services qu'ils proposent, en précisant le niveau d'habilitation que ces services requièrent ainsi que leur niveau de priorité si ce sont des services critiques. Les systèmes opérants déclarent auprès du système de sûreté et de sécurité les services qu'ils fournissent, en précisant le niveau d'habilitation requis pour accé-

der à ces services et leur niveau de priorité des services requis si ce sont des services critiques.

Figure 3. Architecture proposée intégrant sûreté et sécurité



Le système de sécurité et de sûreté vérifie que le système opérant fournissant un service est exempt d'agent compromettant. Il inscrit le service opérant dans l'annuaire des services disponibles et délivre une patente nette d'une durée limitée au système opérant fournissant ces services.

Le système de sécurité et de sûreté maintient l'annuaire des services que proposent les différents systèmes opérants, ainsi que, pour chaque service, le niveau d'habilitation et le niveau de priorité nécessaires pour le requérir.

Les systèmes opérants s'abonnent auprès du système de sûreté et de sécurité aux services dont ils ont besoin, en précisant le niveau d'habilitation auquel ils ont accès ainsi que le niveau de priorité des services requis si ce sont des services critiques.

Le système de sécurité et de sûreté vérifie que le système opérant requérant un service est exempt d'agent compromettant. Il inscrit le service opérant dans l'annuaire des clients du service demandé et délivre une patente nette d'une durée limitée au système opérant requérant ce service. Le système de sécurité et de sûreté maintient l'annuaire les clients des services et de leur niveau d'habilitation propres leur permettant d'accéder aux services. Il maintient l'annuaire des systèmes critiques qui sont prioritaires en cas de situation dégradée ou de réduction des performances dues à des accidents ou à des actes de malveillance. Cet annuaire des systèmes critiques permet aussi de les alerter afin de remonter leur niveau de vigilance et de protection en cas d'attaque d'un système. Enfin, il maintient aussi l'annuaire des abonnements aux différents services en mentionnant le niveau de priorité attribué à chaque abonnement en fonction de la criticité du système client. Cet annuaire des abonnements aux différents services permet de cartographier les dépendances des systèmes, de façon dynamique, et d'effectuer dynamiquement les délestages en tenant compte de la criticité des systèmes clients en cas d'accident ou d'acte malveillant à l'encontre d'un système fournisseur. Cet annuaire permet aussi d'abonner les clients à d'autres systèmes fournisseurs, isofonctionnels, pour conserver les mêmes niveaux de performance, là encore, en cas d'accident ou d'acte malveillant à l'encontre d'un système fournisseur.

Outre les annuaires, le système de sécurité et de sûreté dispose aussi d'un émetteur de patente nette qui fournit ce type d'attestation après avoir vérifié que le système qui la demande est exempt d'agent compromettant. Enfin le système de sûreté et de sécurité dispose d'un lanceur de défis. Les défis sont lancés auprès des systèmes opérants de façon aléatoire et indépendamment de ces systèmes opérants. Le rôle des défis est de vérifier le bon fonctionnement des systèmes opérants du point de vue de la sécurité en particulier pour vérifier qu'ils ne sont pas contaminés ou n'ont pas subi d'actes malveillants, ainsi que pour vérifier que la vigilance ne s'émousse pas et que ne se développe pas des comportements laxistes. Les résultats du lanceur de défis contribuent à maintenir la patente nette des systèmes sains et de la retirer des systèmes qui s'avèreraient contaminés.

Une telle architecture implique que les annuaires, les journaux, l'émetteur de patente nette et le lanceur de défi soient protégés contre toute attaque, dans un coffre.

En cas d'attaque d'un système opérant critique ou d'un système fournissant des services à un système opérant critique opérant critique, ce dernier est confiné et mis en quarantaine. Ses services sont rendus indisponibles, le temps de la quarantaine, la patente nette est retirée du système opérant contaminé. De même, ses abonnements

aux services d'autres systèmes sont désactivés le temps de la quarantaine. Il est blanchi et sa remise en service est conditionnée, outre par le respect de la quarantaine, par la vérification de l'absence de résidus vestigiaux de l'agent compromettant. La remise en service s'accompagne de la délivrance d'une patente nette.

Enfin, la délivrance de patente brute permet de moduler le niveau de protection en fonction du niveau de contamination et du niveau de criticité et, in fine, limiter les impacts des délestages induits par la mise en quarantaine de systèmes contaminés.

Il s'agit là d'une proposition qui doit être précisée et validée expérimentalement.

4 Conclusion

La diffusion des technologies de l'information s'accompagne de la diffusion des risques liés à la sécurité des systèmes d'information. Cette dernière affecte la sûreté des systèmes, en particulier celles des systèmes critiques.

Après avoir analysé la complémentarité entre la sûreté et la sécurité, nous montrons en quoi ces deux dimensions affectent l'architecture d'un système. Pour concevoir une architecture cohérente et évolutive, il est nécessaire de trouver l'équilibre entre le découplage des aspects et leur tissage. Nous proposons un modèle d'architecture orientée service intégrant la sécurité et la sûreté. Ce modèle permet de délivrer des patentes nettes aux systèmes exempts d'agent contaminant et des patentes brutes à des systèmes non critiques faiblement contaminés. Cette architecture permet de moduler la protection en fonction de la sûreté et de la sécurité, en prenant en compte le niveau de criticité des systèmes et leur niveau de contamination.

Les axes de recherche consistent à préciser le contenu des patentes nettes et brutes, de définir le niveau acceptable de contamination pour délivrer des patentes brutes, ainsi que les conditions et modalités de délivrance des patentes nettes et brutes.

Cette proposition d'architecture doit être réalisée et validée expérimentalement.

5 Remerciements

Nous remercions Frédéric Pradeilles pour son aide et ses conseils.

6 Bibliographie

1. Amalberti R. (2009). Violations et migrations ordinaires dans les interactions avec les systèmes automatisés. Journal Européen des Systèmes Automatisés, vol 43, n° 6, pp. 647-660.
2. ANSSI (2004). Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) ; Section 5 ; outillage pour le traitement des risques SSI. Version du 5 février 2004.
3. ANSSI (2010). Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) ; Méthode de gestion des risques. Version du 25 janvier 2010.
4. ANSSI (2012). Cas pratique. La cybersécurité des systèmes industriels.
5. Brun, J-M., Platel L & Tea F. (2013). Cyber Sécurité des Systèmes de Contrôle Industriels : les spécificités des SCI, un challenge pour leur sécurité. Actes de Computer & Elec-

tronics Security Applications Rendez-vous, Sécurité des systèmes numériques industriels ; pp 6-16.
6. Brun, J-M., Platel L & Tea F. (2013). Sécurité informatique des systèmes de contrôle industriels ; détection et surveillance au niveau des équipements et du bus de terrain. Actes de Computer & Electronics Security Applications Rendez-vous, Sécurité des systèmes numériques industriels ; pp 62-75.
7. CLUSIF (2003). Plan de Continuité d'Activité – Stratégie et solution de secours du SI. Dossier technique.
8. CLUSIF (2014). Plan de Continuité d'Activité, Plan de Reprise d'Activité. Les Synthèses du CLUSIF.
9. EN 60300-3-15 (2010). Gestion de la sûreté de fonctionnement – Partie 3-15 : Guide d'application- Ingénierie de la sûreté de fonctionnement des systèmes.
10. Gad El Rab (2008). Evaluation des systèmes de détection d'intrusion. Université Paul Sabatier - Toulouse III, 2008.
11. ISO/IEC 27032 (2012). Information Technology – Security Techniques – Guidelines for security.
12. ISO/IEC 27001 (2013). Information Technology – Security Techniques – Information Security management systems – Requirements.
13. ISO/IEC/IEEE 15288 (2015). International Standard on Systems and software engineering – System life cycle processes.
14. Luzeaux D. (2011). Ingénierie des grands systèmes complexes. In Luzeaux D., Ruault J.-R. & Wippler J.-L. (Eds.), Maîtrise de l'ingénierie des systèmes complexes et des systèmes de systèmes : études de cas, Hermes-Lavoisier, Paris, pp. 21-106.
15. Ministère de l'écologie et du développement durable (2010). Guide pour l'estimation des dommages matériels potentiels aux biens des tiers en cas d'accidents majeurs.
16. MIL-STD-882E (2012). System Safety. Department of Defense Standard Practice.
17. Pariès J. (2006). Complexity, emergence, resilience. In Hollnagel E., Woods D. D. & Leveson N. (Eds.), Resilience Engineering. Concepts and precepts, Ashgate, Aldershot, pp. 43-53.
18. Piètre-Cambacèdés L. (2010). Des relations entre sûreté et sécurité. Thèse de doctorat Informatique et Réseaux, soutenue le 3 novembre 2010 (Paris).
19. Rasmussen J. (1997). Risk management in a dynamic society: a modelling problem. Safety Science, vol. 27, n° 2/3, pp. 183-213.
20. Reddy G.S., Rao V.N. & Kumar N. (2012). An intrusion tolerance approach for Internet security. International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, n°8, October 2012.
21. Ruault J.-R., Vanderhaegen F. & Kolski C. (2013). Sociotechnical systems resilience: a dissonance engineering point of view. 12th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine Systems, Las Vegas.
22. Ruault J-R. (2015). Proposition d'architecture et de processus pour la résilience des systèmes ; application aux systèmes critiques à longue durée de vie. Thèse de Doctorat d'Automatisme soutenue le 7 juillet 2015 (Valenciennes).
23. Secrétariat général de la défense nationale (1991). Fiche d'expression rationnelle des objectifs de sécurité.
24. Tarby J-C., Ezzedine H., & Kolski C. (2009). Trace-based Usability Evaluation Using Aspect-oriented Programming and Agent-based Software Architecture. In: Seffah A., Vanderdonckt J. and Desmarais M. (Eds.), Human-Centered Software Engineering: Architectures and Models-Driven Integration, Springer HCI Series, pp. 257-276.