Résilience intégrée de la sécurité et de la sûreté des systèmes, Surveiller le système et alerter les opérateurs pour naviguer à vue

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

Published in: *Génie Logiciel*, volume 117, pp. 2-12, 2016.

Résilience intégrée de la sécurité et de la sûreté des systèmes, Surveiller le système et alerter les opérateurs pour naviguer à vue

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

** LAMIH-UMR CNRS 8201, Université de Valenciennes et du Hainaut-Cambrésis,*
Le Mont Houy, F59313 Valenciennes CEDEX 9, France
{surname.name}@univ-valenciennes.fr
*** rattaché à la Chaire Ingénierie des Systèmes Complexes de l'Ecole Polytechnique, Palaiseau*
dominique.luzeaux@polytechnique.org
**** Research and Innovation Department, ABE - Advanced Business Engineering, 77400 Lagny, France*
wilson.goudalo@abe-engineering.net

Résumé : Tandis que des travaux sont menés pour traiter les risques de nature accidentelle (sûreté), en sûreté de fonctionnement et en ingénierie de la résilience, d'autres travaux sont menés en sécurité des systèmes d'information pour traiter des risques de nature malveillante (sécurité). L'article propose une approche de résilience intégrée de la sécurité et de la sûreté pour surveiller l'état et la dynamique d'un système afin de détecter la proximité d'un danger, la sortie du domaine de définition du système, l'attaque d'acteurs malveillants, d'en alerter les opérateurs pour qu'ils puissent construire et maintenir une conscience de la situation et naviguer à vue quand ils font face à des situations imprévisibles, sans précédent. En particulier, l'article présente les informations clefs de la sécurité, de la sûreté et des interactions entre elles pour aider les opérateurs à comprendre la situation et à intervenir de façon appropriée.

Mots clés : système, architecture, résilience, sécurité, sûreté, surveillance, alerte, conscience de la situation

1. INTRODUCTION

Ces dix dernières années, la plupart des travaux menés par la communauté « ingénierie de la résilience » concernent des systèmes critiques pour lesquels les événements redoutés présentent des conséquences plus ou moins graves, voire catastrophiques, du point de vue de la sécurité des personnes et des biens. Par ailleurs, ces travaux s'inscrivent principalement en ingénierie, c'est-à-dire dans les stades amont des projets. Peu de travaux concernent la résilience en exploitation des systèmes, sur le vif, pour prendre en compte des événements imprévisibles, sans précédent [22]. Enfin, ces travaux prennent rarement en compte la sécurité vis-à-vis d'actes malveillants.

D'un autre côté, de plus en plus de travaux sont menés articulant la sécurité eu égard aux accidents et la sécurité eu égard aux actes malveillants. Ludovic Pietre-Cambacédès [19] a réalisé une très large recension de ces travaux. Il a défini de façon claire les notions de sûreté pour rendre compte des risques de nature accidentelle, sans malveillance, et de sécurité pour rendre compte des risques de nature malveillante. Il a présenté leur champ respectif et proposé une méthode d'analyse intégrant dans un même modèle formel les perspectives respectives de la sûreté et de la sécurité.

Après avoir présenté les concepts clefs de l'ingénierie et de l'architecture des systèmes, de la sûreté, de la sécurité et de la résilience, l'article proposera les bases d'une résilience intégrée de la sécurité et de la sûreté, en s'appuyant sur les travaux de Ludovic Pietre-Cambacédès – utilisant les notions telles que définies ci-dessus – et en complétant le patron de conception « surveillance et alerte » présenté et illustré dans [22].

2. ÉTAT DE L'ART

La protection du personnel, du voisinage, de l'environnement vis-à-vis des risques de nature accidentelle est l'enjeu majeur de la sûreté de fonctionnement et vise à la sécurité des personnes et des biens. Depuis le début du siècle, au-delà des travaux traditionnels en sûreté de fonctionnement, cette démarche a évolué pour prendre en compte la capacité d'un système à recouvrer un état stable, sûr, voire de poursuivre une partie de sa mission en mode dégradé, après un accident, capacité que l'on dénomme résilience des systèmes [14], [20]. Lors de l'exploitation du système, cela consiste à surveiller l'état du système, à alerter les opérateurs lorsque le système sort de son domaine d'emploi et est en proximité du danger afin que ces opérateurs puissent construire et maintenir une conscience de la situation et, *in fine*, naviguer à vue face à des situations imprévisibles, sans précédent.

Par ailleurs, la numérisation des systèmes de contrôle-commande, le développement des architectures ouvertes basées sur des composants disponibles sur étagères, la connexion entre différents systèmes, entre autres, ouvrent la porte à des nouveaux risques, non pas de nature accidentelle, mais de nature malveillante, risques couverts par la sécurité des systèmes d'information.

Ces risques, de nature accidentelle d'un côté, de nature malveillante d'un autre côté, ne sont pas indépendants les uns des autres [19]. Ainsi, une position *fail safe* et une position *fail secure* peuvent être antagonistes. Ludovic Pièvre-Cambacédès [19] montre ainsi que dans le cas d'un bâtiment, dans le cas d'un accident, la position *fail safe* prescrit que les portes doivent rester ouvertes pour permettre l'évacuation des personnes qui sont dans le bâtiment. En revanche, la position *fail secure* prescrit que les portes doivent rester fermées pour empêcher des acteurs malveillants de pénétrer dans le bâtiment. Un tel antagonisme doit être traité en ingénierie afin de trouver une solution de conception qui satisfasse les deux contraintes *fail safe* et *fail secure*. Il est nécessaire de prendre en compte ces interactions au plus tôt durant les stades d'ingénierie, ainsi que durant l'exploitation d'un système, afin que les opérateurs sachent quelles sont ces interactions et les prennent en compte dans leur compréhension de l'état et de la dynamique du système, ainsi que dans les décisions qu'ils prennent et les actions qu'ils engagent.

Ludovic Pièvre-Cambacédès [19] a défini de façon claire les notions de sûreté pour rendre compte des risques de nature accidentelle, sans malveillance, et de sécurité pour rendre compte des risques de nature malveillante. Ce sont ces définitions qui sont utilisées dans ce présent article.

L'état de l'art présente les notions d'ingénierie et d'architecture des systèmes, discipline fédératrice à laquelle sont en lien les autres disciplines, de sûreté et de résilience des systèmes, de surveillance de l'usage du système, de la conscience de la situation des opérateurs et de sécurité des systèmes afin de les articuler dans la proposition de résilience intégrée de la sûreté et de la sécurité des systèmes.

2.1 Architecture et ingénierie des systèmes

L'architecture système décrit la structure du système, des services qu'il fournit et ses liens avec les autres systèmes qui forment son environnement. Plusieurs types d'architecture sont modélisés, dont l'architecture fonctionnelle et l'architecture physique [15].

Une approche de type boîte noire permet d'identifier ses interactions avec son environnement, et en particulier les services qu'il fournit à cet environnement. Ces services déterminent les fonctions qu'il doit réaliser. Ensuite, l'architecture fonctionnelle décrit l'organisation et les interactions de ces fonctions. Ces dernières décrivent ce que fait le système pour réaliser un but indépendamment de la façon de faire. Elles sont décomposées hiérarchiquement pour permettre d'identifier les fonctions terminales. Une fonction transforme des entrées qui lui sont fournies pour produire des résultats sous forme de sorties en s'appuyant sur des ressources et respectant un ensemble de règles. Chaque fonction est réalisée par un ou plusieurs composants. Il s'agit de l'allocation des fonctions aux composants.

L'architecture physique décrit la structure de ces composants. Parmi plusieurs architectures physiques candidates, l'architecture physique retenue est celle qui satisfait au mieux aux objectifs de coût, de délai de production, de capacité à évoluer et répondre aux besoins fonctionnels et non fonctionnels. Des composants peuvent réaliser des fonctions différentes. Il n'y a pas de relation de bijection entre l'architecture fonctionnelle et l'architecture physique.

Les exigences de sûreté et celles de sécurité relèvent des besoins non fonctionnels, au même titre que les exigences d'utilisabilité [18], [6], [7]. Dans de nombreuses situations, ces exigences sont transverses aux fonctions, ce qui a des impacts non négligeables sur les architectures fonctionnelles et physique du système.

L'article se poursuit en approfondissant ce qui relève de la sûreté des systèmes.

2.2 Sûreté des systèmes

La sûreté des systèmes est la protection contre les conséquences de défaillances, d'erreurs, d'accidents, et de tout événement indésirable. Elle est aussi définie comme le contrôle de dangers identifiés pour maintenir un niveau de risque acceptable [17]. Elle s'appuie sur la gestion des risques et consiste à identifier les événements redoutés, à évaluer leur probabilité d'occurrence (fréquent, probable, occasionnel, isolé, improbable) ainsi que le niveau de sévérité de leurs conséquences (catastrophique, critique, marginal, négligeable). Le croisement de la probabilité d'occurrence et du niveau de sévérité des conséquences permet de déterminer le niveau de criticité du risque, élevé, sérieux, moyen, faible. La Figure 1 illustre la matrice des risques selon la norme MIL-STD 882E [17].

Sévérité / Probabilité	Catastrophique (1)	Critique (2)	Marginal (3)	Négligeable (4)
Fréquent (A)	Élevé	Élevé	Sérieux	Moyen
Probable (B)	Élevé	Élevé	Sérieux	Moyen
Occasionnel (C)	Élevé	Sérieux	Moyen	Faible
Isolé (D)	Sérieux	Moyen	Moyen	Faible
Improbable (E)	Moyen	Moyen	Moyen	Faible
Éliminé (F)	Éliminé			

Figure 1 : Matrice d'évaluation des risques d'après [17]

La démarche de la sûreté vise à éviter les accidents. Pour autant que des accidents surviennent, l'objectif est d'en réduire les effets en mettant en œuvre des dispositifs de protection tels que des barrières [24], [25].

Cette démarche atteint ses limites lorsque les dispositifs de sécurité sont désactivés, les barrières franchies, ou que le contexte opérationnel évolue, générant de nouveaux événements redoutés lesquels ne peuvent pas être identifiés en phase amont des projets.

La sûreté achoppe à prendre en compte les situations imprévues, sans précédent, que peut rencontrer le système, en particulier lorsqu'il est amené à fonctionner hors de son domaine d'emploi.

Cela amène à repenser la sûreté du point de vue de la résilience pour prendre en compte les situations réelles opérationnelles sur le vif et donner aux opérateurs les moyens de piloter à vue, objet de la prochaine section de l'article.

2.3 Résilience des systèmes

Malgré tous les efforts possibles, toutes les situations que connaîtra le système ne peuvent pas être envisagées lors des stades de conception et de réalisation. Dans ce contexte, lorsque le système est mis en œuvre, les opérateurs humains peuvent être face à des situations sans précédent, imprévisibles, qui n'auront pas été envisagées en conception. Les dispositifs de sécurité sont alors inopérants face à ces situations. Les opérateurs doivent pouvoir naviguer à vue et disposer des moyens pour faire face à l'adversité. La résilience concerne ce qui ne peut pas être anticipé et est la capacité d'un système à s'ajuster face à des perturbations en dehors du périmètre spécifié des mécanismes d'adaptation du système, à s'y adapter ainsi qu'à apprendre les règles d'adaptation adéquates [14].

La résilience est le processus dynamique de pilotage à vue permettant aux opérateurs de faire face à l'incertitude, de comprendre la situation à laquelle ils font face, d'apprendre et de s'y adapter aussi bien que possible. Pour cela, le système doit pouvoir évaluer sa position par rapport au danger, surveiller sa dynamique, reconnaître les situations où il est susceptible de sortir de son domaine d'emploi et d'alerter les opérateurs [14].

Les informations de l'alerte peuvent comprendre six blocs, respectivement [22] :

- le niveau de risque : la sévérité, la probabilité, la criticité ;
- la description du système : l'identifiant du composant du système concerné ;
- l'état évalué : les données historiées de l'état du système, le problème diagnostiqué, les dérives constatées, l'état courant, l'état de référence, l'écart entre l'état courant et l'état de référence, la proximité d'une zone de danger, le type de danger identifié, les marges de réserves disponibles ;
- les conseils : les actions recommandées, pouvant comporter des alternatives ;
- le contexte de l'alerte : l'horodatage et la localisation du composant concerné ;
- le niveau de confiance de l'alerte.

La section suivante présente une solution permettant de surveiller le système et d'alerter les opérateurs pour qu'ils puissent conduire à vue.

2.4 Surveillance de l'usage du système et signature

La navigation à vue s'appuie sur la capacité des opérateurs à connaître l'état du système, à savoir dans quel environnement ils opèrent. Un système de surveillance de l'usage et de l'état d'un système permet aux opérateurs de connaître l'état du système dont ils ont la charge afin d'éviter un accident. Ainsi que l'illustre le diagramme d'activité SysML (Figure 2), un tel système recueille des informations provenant du système et de son environnement, évalue la situation courante et en alerte les opérateurs en les conseillant sur la conduite à tenir [22].

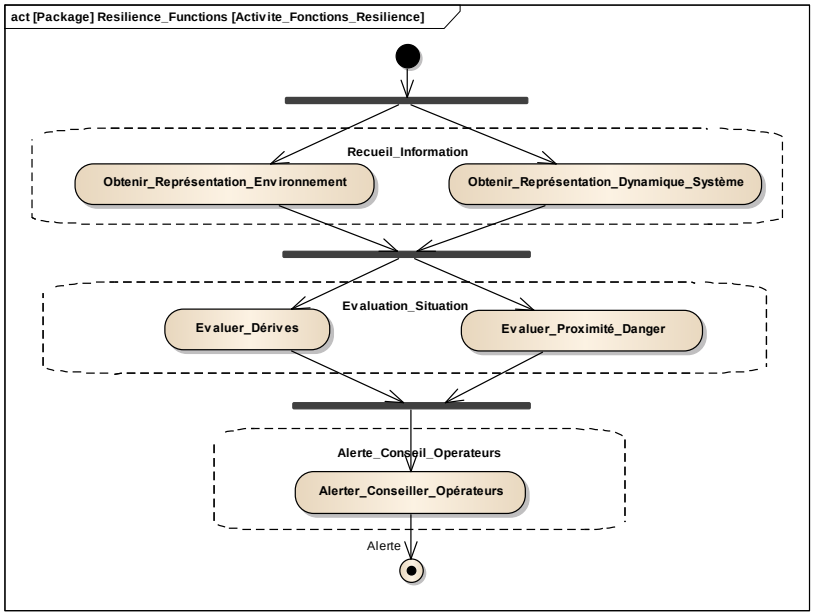

Figure 2 : Diagramme d'activité de la fonction « éviter » [22]

La surveillance d'un système permet de détecter des dérives de l'état d'un système, l'apparition d'un comportement anormal, et d'en alerter l'opérateur, ainsi que l'illustre le diagramme de bloc interne SysML (Figure 3). Ce dernier est rapidement alerté lorsque le système surveillé dévie et sort de son domaine d'emploi. Cette surveillance nécessite de disposer en permanence d'informations reflétant l'état réel du système [22].

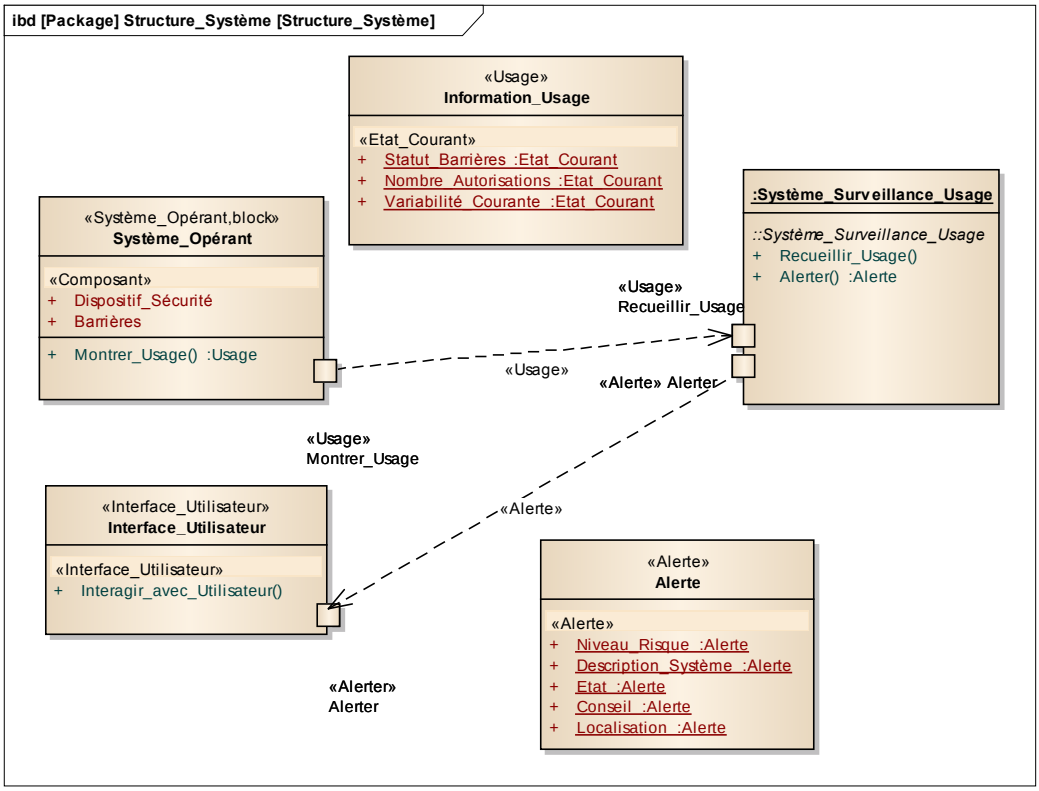

Figure 3 : Interfaces et flux entre systèmes opérant, surveillance d'usage et interactif [22]

Dans ce contexte, les recommandations générales pour l'architecture des BIT (*built-in test*) dans un système intégré définit « la fonction alarme qui a pour but d'informer l'utilisateur du système des événements perturbant le fonctionnement du système et leurs circonstances d'apparition » [3]. La fonction alarme regroupe les informations relatives à l'état du système, dont les défaillances des constituants, et celles relatives aux conditions d'emploi. Une défaillance se manifeste physiquement par un « symptôme ». La combinaison exhaustive des symptômes découlant de la défaillance d'un service est la « signature » de cette défaillance. Il est clair que la relation entre défaillance et signature n'est pas bijective : en effet, une signature peut être commune à plusieurs défaillances. De plus, une défaillance initiale peut générer de nombreuses autres défaillances en cascade. Pour comprendre quelle est la défaillance initiale et la cascade induite, il est nécessaire de démêler l'écheveau des signatures.

Dans la norme [3], la surveillance des machines représente l'ensemble des données (niveau de vibration, température, pression…) reflétant les conditions d'exploitation de la machine. Les niveaux sont enregistrés et comparés aux données de référence précédemment relevées, aux alarmes préréglées ou au seuil de déclenchement. Toute modification de ces niveaux est soigneusement examinée, car elle indique généralement le développement d'une anomalie néfaste pour l'état de la machine.

Une table des fonctions défaillantes les trace afin de constituer des arbres de défaillances [3]. Elle comprend notamment les informations suivantes :

- référence de la fonction défaillante, suivant un format normalisé, pour l'identifier et la caractériser ;
- dénomination de la fonction défaillante.

Cette norme [3] propose de formuler les signatures dans une table qui leur soit adaptée ; elle comprend les informations suivantes :

- référence de la signature, suivant un format normalisé, pour gérer les signatures ;
- signature simple issue d'un test ou synthétisant d'autres signatures ;
- fonctions défaillantes, faisant référence à la table des fonctions défaillantes ;
- temps de latence minimum, plus petit retard entre l'apparition de la défaillance et celle de la signature ;
- temps de latence maximale, plus grand retard entre l'apparition de la défaillance et celle de la signature ;
- conditions de validité de la signature, conditions externes et internes pour lesquelles une signature est exploitable ;
- durée minimum de la condition de validité de la signature, durée minimum de présence de la condition de validité pour que la signature soit valide ;
- règles de maintien de la signature appliquée aux signatures simples pour éviter de prendre en compte des fausses alarmes.

En complément à cette table de signatures, pour permettre de comprendre la dynamique des chaînes d'événements, la norme [3] propose une table de dépendances qui trace la diffusion d'un événement d'une fonction à une autre, d'un composant à un autre. Cette table de dépendances comprend la liste des dépendances directes et les conditions nécessaires de propagation d'un événement.

Les informations de l'alerte permettent aux opérateurs de construire et de maintenir une représentation dynamique et actualisée de l'état du système, représentation aussi appelée « conscience de la situation », objet de la section suivante.

2.5 Conscience de la situation

Dans la précédente section, nous avons pu constater que, face à des situations imprévues, les opérateurs doivent pouvoir conduire à vue et, pour cela, comprendre la dynamique du système pour éviter un accident. La conscience de la situation, *situation awareness* en anglais, est la clef de la compréhension de la dynamique du système. Elle peut être définie comme étant la représentation, la connaissance, qu'un opérateur a de l'état d'un système et de l'état de l'environnement [4]. Par extension, la conscience partagée de la situation, *shared situation awareness* en anglais, peut être définie comme étant la représentation collective, une compréhension partagée, qu'ont plusieurs opérateurs de l'état du système et de son environnement.

Dans ce qu'il caractérise comme l'approche centrée sur la régulation, Chalandon [4] définit la conscience de la situation comme étant une représentation fonctionnelle continuellement mise à jour, tendue entre l'adaptation immédiate et la définition de la tâche. Elle s'appuie sur un ajustement permanent d'une représentation en fonction de l'historique de la situation et des buts à atteindre. L'approche centrée sur la régulation se caractérise par l'acceptation par l'opérateur de « ne pas comprendre la situation », au sens de compréhension maximale, exhaustive de la situation, car les ressources nécessaires à cette activité sont incompatibles avec la dynamique de la tâche. Par souci d'économie et d'opérativité, la régulation se traduit ici par le compromis cognitif que l'opérateur met en œuvre et contrôle par une activité métacognitive prenant en compte les exigences de la tâche, ses savoirs et savoir-faire et le niveau de risque accepté. Ce compromis cognitif est le niveau de compréhension minimal pour une efficacité maximale en termes d'objectifs d'action [4]. Dans le contexte des environnements dynamiques des systèmes critiques comprenant une large variété de dispositifs dont les interactions peuvent être imprévisibles, la conscience de la situation doit prendre en compte les déviations mineures ou les défaillances, non critiques par elles-mêmes, mais pouvant évoluer ou interagir au cours du temps pour mener à un accident. Une rétroaction adéquate de l'état et du comportement du système est essentielle pour la conscience de la situation des opérateurs [23].

En complément des risques de nature accidentelle traités jusqu'à maintenant, la sécurité des systèmes, objet de la prochaine section, concerne les risques de nature malveillante.

2.6 Sécurité des systèmes

Si la sûreté traite des risques de nature accidentelle, sans intention de nuire, la sécurité, quant à elle, concerne les risques de nature malveillante. À l'origine, la sécurité est issue des besoins d'échange d'information sécurisé dans le domaine militaire et est mise en œuvre dans la sécurité des systèmes d'information (SSI). La sécurité est la démarche consistant 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 ;

L'objectif de la sécurité est de faire respecter ces critères malgré des attaques malveillantes. La sécurité est une démarche continue mise en œuvre tout au long du cycle de vie du système de l'expression de besoin au démantèlement. De par l'incapacité de connaître *a priori* tous les événements de sécurité, toutes les stratégies d'attaque, la sécurité ne se prouve pas. En revanche, il s'agit d'acquérir un niveau de confiance jugé satisfaisant dans la capacité du système à résister aux attaques et à faire respecter les critères de sécurité demandés.

En conformité aux normes consacrées à la sécurité des systèmes d'information [8], [9], [10], [12], [13], 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 [2] et des propositions d'outillage adapté [1]. La fiche d'expression rationnelle des objectifs de sécurité (FEROS), quant à elle, est une méthode d'évaluation des risques adaptée à la sécurité [12]. Ces risques sont ceux d'espionnage, de sabotage, d'écoute, d'accès illégitime, d'abus de droit. Les dispositifs matériels et logiciels d'attaque sont, sans prétendre être exhaustif, l'usage de portes dérobées, les chevaux de Troie, les vers, les logiciels espions. La lutte consiste à détecter les intrusions, les événements liés à la sécurité de l'information [13] et à générer des alertes [5].

À l'instar des bonnes pratiques dans le domaine de la sûreté, les normes relatives à la sécurité de l'information [8], [11], [12] préconisent de gérer les risques, de surveiller le système et d'alerter sur la situation sécuritaire du système. Cet article se centre sur les fonctions de surveillance et d'alerte.

La norme [11] préconise de surveiller le système et de journaliser les informations relatives à la sécurité. Cette journalisation consiste à enregistrer et conserver à titre probatoire ces informations, entre autres :

- les identifiants utilisateurs ;
- les activités du système ;
- l'identifiant et la localisation géographique du système ;
- l'horodatage des événements significatifs ;
- les tentatives, réussies ou échouées, d'accès aux données ou ressources du système ;
- les modifications apportées à la configuration du système ;
- l'utilisation des privilèges ;
- les fichiers qui ont fait l'objet d'un accès et la nature de cet accès ;
- les alarmes déclenchées par le système de contrôle d'accès ;
- l'activation ou la désactivation des systèmes de protection.

À l'instar du document [3], les données brutes issues d'activités de mesure des événements indésirables sont traitées et consolidées afin d'élaborer des indicateurs synthétiques présentant la sécurité du système, par exemple la protection contre les codes malveillants, de façon appropriée aux opérateurs [8].

2.7 Conclusion

L'état de l'art a dressé une synthèse des éléments clefs qui contribuent à la résilience intégrée de la sûreté et de la sécurité d'un système. Ces éléments reposent sur la sûreté qui traite des risques de nature accidentelle, sans intention de nuire, et sur la sécurité qui, en revanche, traite des risques de nature malveillante. La surveillance de l'état et de la dynamique du système permet de recueillir les informations brutes relevant des événements indésirables, dans le domaine de la sécurité, et des événements redoutés, dans le domaine de la sûreté. Ces informations brutes sont traitées et consolidées en indicateurs qui sont présentés aux opérateurs. Ces indicateurs contribuent à la construction et au maintien de la conscience de la situation des opérateurs.

La proposition consiste à articuler les informations relevant de la sécurité et celles relevant de la sûreté, afin que les opérateurs puissent élaborer une compréhension de l'état et de la dynamique du système sur ces deux dimensions et statuer des actions à mener en prenant en compte les interactions entre sécurité et sûreté.

3. PROPOSITION : RÉSILIENCE INTÉGRÉE DE LA SÛRETE ET DE LA SÉCURITÉ DES SYSTÈMES

À l'origine, dans les systèmes critiques, les événements redoutés relevaient de la sûreté, de perturbations non prévues ou de défaillances, sans qu'il y ait malveillance. La généralisation des technologies de l'information et leur utilisation dans des dispositifs de commande et de contrôle de systèmes critiques, ainsi que dans les dispositifs de sûreté, ouvrent la voie à des événements redoutés de nature malveillante relevant de la sécurité. Les 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.

En phase opérationnelle, pour mener leur mission au mieux et faire face à l'adversité, les opérateurs doivent disposer d'informations pour développer et maintenir une représentation partagée de l'état et de la dynamique du système. Pour ce qui relève de la sûreté, ces informations sont des alertes de pannes, de sortie du domaine de vol, de la proximité d'un danger. Mais ces informations sont aussi des alertes de sécurité, telle l'information relatant la compromission du système par un agent malveillant.

Ces informations sont des signatures, des ensembles de symptômes induits par l'état et par la dynamique du système du point de vue de la sécurité et de la sûreté du système. À partir de ces signatures, les opérateurs diagnostiquent l'état du système et prennent des initiatives, en fonction du diagnostic effectué, pour maintenir le système sécurisé et sûr. Le diagnostic serait simple s'il y avait une relation bijective entre les états et les symptômes. Ce n'est déjà pas le cas lorsque la sécurité et la sûreté sont prises indépendamment l'une de l'autre. Par construction, ce n'est pas le cas dans le domaine de la sécurité puisque l'acteur malveillant cherche à se cacher, *a fortiori* lorsqu'il y a des interactions entre sûreté et sécurité.

Dans ce contexte, le dispositif de surveillance et d'alerte de l'état du système doit aider les opérateurs à lever les ambiguïtés, identifier les événements initiaux, les chaînes d'événements induites par ces événements initiaux, ainsi que les interactions.

Ces signatures sont construites par chaque discipline en prenant en compte ces interactions entre sécurité et sûreté dans le vif, pour des situations qui n'auraient pas été envisagées en ingénierie. Au même titre que le dispositif de surveillance et d'alerte doit informer les opérateurs de la situation courante, de la dynamique du système du point de vue de la sûreté [22], il doit aussi informer les opérateurs des événements de sécurité et des interactions entre ces événements de sécurité et les événements de sûreté.

Dans le domaine de la sûreté, les signatures relatives aux défaillances permettent de couvrir une partie du besoin, lorsque l'état du système est induit par une défaillance de composants. Les informations de l'alerte [22] les complètent lorsque l'état du système est induit par celui de l'environnement et de son emploi (exemple, sortie du domaine d'emploi) et non par une défaillance de composants.

Dans le domaine de la sécurité, les valeurs de mesures, en quelque sorte équivalentes aux signatures du domaine de la sûreté, décrivent les événements de sécurité, par exemple une compromission par un acteur malveillant.

Ainsi que le souligne Piètre-Cambacédès [19], sécurité et sûreté ne sont pas indépendantes et interagissent entre elles. Un acteur malveillant peut profiter d'une défaillance du système pour le compromettre. Dans ce contexte, il est nécessaire de rendre compte de cette interaction aux opérateurs afin qu'ils puissent prendre les initiatives adéquates, et agir sur les deux dimensions de la sécurité et de la sûreté.

Il s'agit, dans un premier temps, de surveiller le système et de détecter un événement initial relevant de la sécurité ou de la sûreté, puis de tracer, via des arbres de dépendances, les événements secondaires, directs ou indirects, induits par cet événement initial, en prenant en compte les interactions entre sûreté et sécurité.

Dans un second temps, il est nécessaire de caractériser ces événements et d'identifier leurs origines, qui peuvent être, sans prétendre à l'exhaustivité, des défaillances de composants, des contournements de barrières, des actions malveillantes. Cette caractérisation et cette identification s'appuient sur les symptômes engendrés par ces événements, sur les arbres de dépendances permettant de remonter à l'événement initial. Elles servent à évaluer la situation à laquelle fait face le système. Cette évaluation doit prendre en compte l'ambiguïté des symptômes ne permettant pas de statuer de façon claire et précise sur un événement précurseur. Elle doit aussi prendre en compte les effets des actions malveillantes, par exemple qui camouflent une compromission, ou qui leurrent le système et l'empêchent de détecter un événement de sûreté ayant des conséquences critiques, voire catastrophiques. Enfin, l'évaluation doit déterminer quelles sont les fonctions et les composants compromis afin de pouvoir les circonscrire et de permettre aux opérateurs de déterminer les impacts du confinement des fonctions et composants compromis. Pour cela, il est nécessaire que le dispositif de surveillance comprenne un répertoire à jour des menaces, des acteurs malveillants et de leurs stratégies d'attaque ainsi que d'une cartographie des fonctions et des composants, copie en temps réel des architectures fonctionnelle et organique du système.

Dans un troisième temps, il s'agit d'alerter les opérateurs pour leur rendre compte de la situation tant du point de vue de la sécurité que de la sûreté, et de leurs interactions en leur présentant les signatures générées par les événements. Au-delà d'une présentation statique des signatures, le dispositif doit aider les opérateurs à approfondir le diagnostic en leur permettant de formuler des hypothèses sur les origines des événements, d'effectuer des sondages pour confirmer ou infirmer leurs hypothèses, afin de pouvoir identifier quelles seraient les actions les plus appropriées à mener.

Enfin, au-delà de la surveillance du système et de l'alerte des opérateurs quand des événements interviennent, le dispositif pourrait aider les opérateurs en leur permettant de développer une méthode essai-erreur, d'une part en expérimentant des solutions dans une simulation qui soit un miroir du système réel et de son environnement tout aussi réel, d'autre part en agissant en boucle courte sur le système réel et son environnement. L'intérêt de la simulation est de

permettre aux opérateurs de tester des solutions sans crainte d'endommager le système et d'accroître la gravité des conséquences des événements détectés. Mais pour que ces tests soient valides et pertinents pour les opérateurs, il est nécessaire que la simulation soit fidèle à l'état et à la dynamique du système et de son environnement. Dans l'hypothèse où, quelle qu'en soit la raison, la simulation ne serait pas fidèle, les expérimentations que feraient les opérateurs seraient fausses par rapport au système réel et à son environnement. Les opérateurs prendraient alors des décisions inadaptées et leurs actions ne permettraient pas de restaurer le système, voire aggraveraient son état et laisseraient l'acteur malveillant compromettre le système. Dans ce contexte, la simulation doit être désactivée automatiquement s'il s'avère qu'elle ne représente pas fidèlement le système et son environnement.

L'alerte auprès des opérateurs intégrant des signatures de la sûreté et de la sécurité doit être sécurisée. En effet, une telle information est critique et ne doit pas être accessible à des acteurs malveillants. Pour autant, elle doit être accessible à tous ceux qui en ont besoin, c'est-à-dire à tous ceux qui peuvent être affectés par un accident du système et tous les systèmes de l'environnement qui peuvent avoir un accident avec le système concerné. Cela implique que les alertes soient diffusées de façon sécurisée aux seuls systèmes qui sont affectés ou susceptible d'être affectés par les conséquences des problèmes de sécurité et de sûreté que rencontre le système concerné. Il s'agit, par exemple, d'une dépendance fonctionnelle, d'une proximité géographique, de l'usage de mêmes ressources, de trajectoires qui se croisent, etc. Cette diffusion sécurisée d'alerte de sécurité et de sûreté génère des contraintes spécifiques sur la sécurité du système et ouvre des perspectives de recherche qui sont détaillées dans la section « Conclusion et perspectives ».

Le patron de conception « surveiller et alerter » [22] est ainsi complété (Figure 4) pour prendre en compte les informations relevant de la sécurité en sus de celles concernant la sûreté, et formuler une alerte intégrant sûreté et sécurité.

En intégrant les informations relevant de la sécurité et celles relevant de la sûreté, les informations communes tels que l'identifiant, l'horodatage et la localisation du système contributeur, les interactions entre sécurité et sûreté peuvent être explicitées et devenir plus faciles à comprendre par les opérateurs.

Ces informations d'alerte chiffrée intégrant sécurité et sûreté sont organisées de la façon suivante :

- indicateur synthétique du niveau de risque et de la nature de risque (sécurité ou sûreté), explicitant les risques affectant les personnes (décès, blessure, maladie professionnelle) et l'environnement ;
- description du système concerné, dont identifiant, type de système (opérateur d'importance vitale), voire son classement (système classé Seveso) ;
- l'état courant et la dynamique du système et de son environnement ;
  - ○ événements redoutés (sûreté) et événements indésirables (sécurité) initiateurs de l'état du système ;
  - ○ horodatage et localisation des événements initiateurs ;
  - ○ fonctions et composants affectés (sûreté) et/ou compromis (sécurité) ;
  - ○ données historiées présentant l'évolution temporelle des conséquences induites par les événements initiateurs de l'état du système, en particulier des compromissions (par exemple, les tentatives réussies ou échouées d'accès au système, les modifications apportées à la configuration du système) ;
  - ○ dérives constatées (par exemple, le contournement de barrières de sécurité ou la désactivation des dispositifs de protection) ;
  - ○ écart entre l'état courant et l'état de référence ;
  - ○ proximité d'une zone de danger (sûreté) ou de menace (sécurité) ;
  - ○ type de danger (sûreté) ou de menace (sécurité) identifié ;
  - ○ temps de latence minimum et maximale entre l'apparition des événements initiateurs et celle de l'alerte ;
  - ○ durée minimum de la condition de validité de l'alerte ;
  - ○règles de maintien de l'alerte ;
  - ○ interactions entre sûreté et sécurité identifiées ou potentielles, par exemple une position *fail safe* qui ouvre une porte dans le dispositif de sécurité ;
  - ○ marges de réserves disponibles, en particulier qui permet de confiner des composants compromis tout en préservant la capacité de sûreté du système ;
- les conseils aux opérateurs, pouvant présenter des hypothèses à investiguer ou différentes solutions potentielles ;
- le niveau de confiance de l'alerte, dont les conditions de validité de l'alerte.

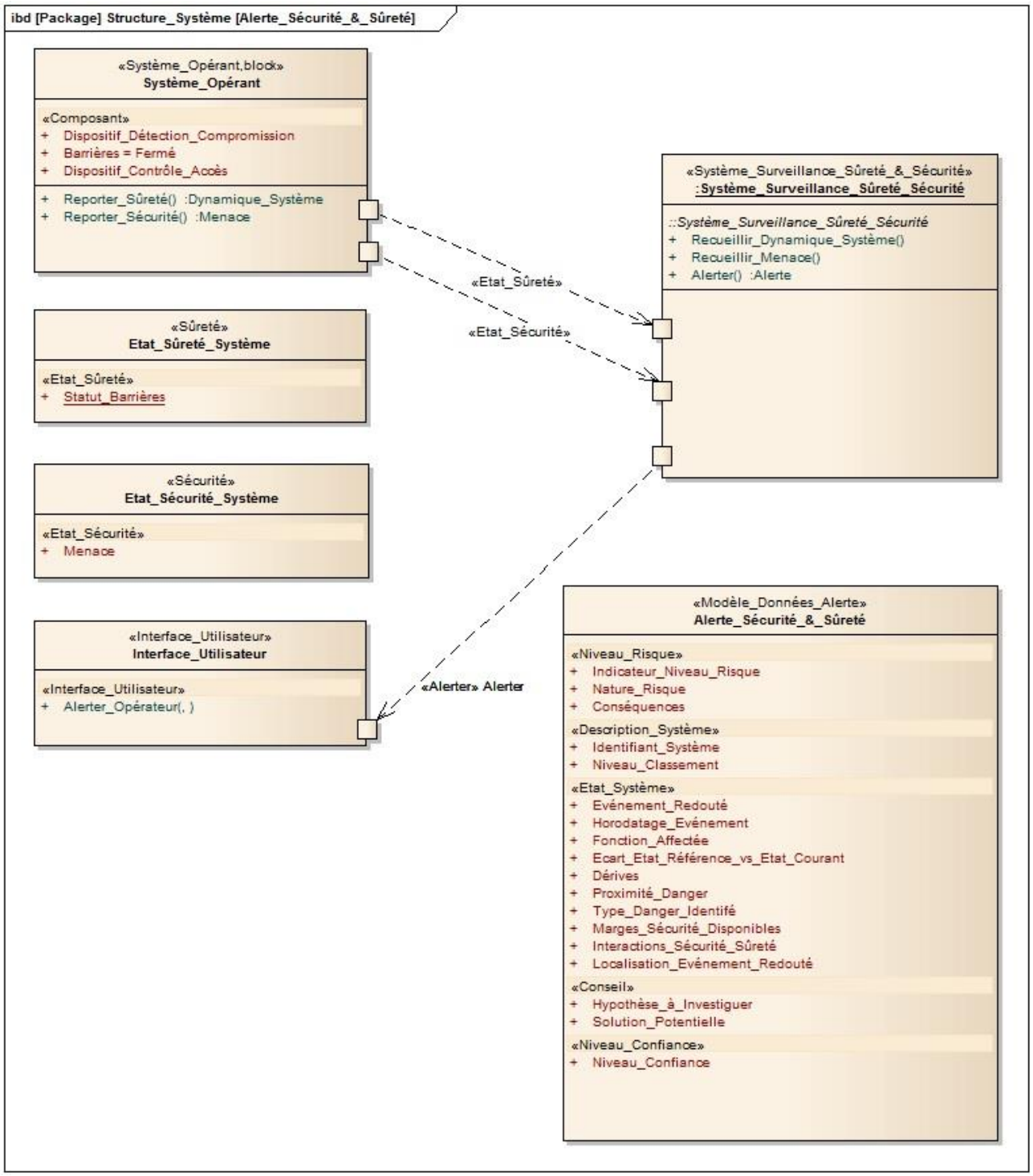

Figure 4 : Adaptation du dispositif de surveillance et d'alerte intégrant sécurité et sûreté

Cette proposition présentant une alerte intégrant les informations relatives à la sûreté et à la sécurité, ainsi que celles relatives à leurs interactions, est une première étape.

Elle ne traite pas cependant de la dynamique d'élaboration de l'alerte qui tiendrait compte des temporalités différentes de ses deux dimensions constitutives. Elle ne traite pas, non plus, des contraintes que l'intégration de la sûreté et de la sécurité engendrent sur l'architecture du système dans sa globalité et sur celle du dispositif de surveillance de l'état du système. En particulier, certaines informations doivent nécessairement être mises en commun, à l'instar des fonctions et composants affectés, et de l'horodatage et de la localisation des événements initiateurs ; en revanche, il est possible que certaines informations ne puissent pas être partagées et doivent être protégées, tel le répertoire des menaces. Enfin, elle n'aborde pas les traitements des données brutes (défaillances, mesures des événements indésirables…) pour élaborer une alerte claire et précise, pour donner aux opérateurs les moyens d'investigation, de test d'hypothèses et d'analyse par raffinements successifs de la situation du système des points de vue de la sécurité, de la sûreté et de leurs interactions. Tous ces points sont des perspectives de recherche.

Ces informations de l'alerte doivent être adaptées au système concerné et évaluées avec les opérateurs afin d'élaborer un ensemble d'informations cohérent et pertinent pour que les opérateurs puissent construire et maintenir une compréhension partagée de l'état et de la dynamique du système, en particulier quand ils doivent piloter à vue et font face à des situations sans précédent qui n'ont pas été envisagées lors de la conception du système.

5. CONCLUSION ET PERSPECTIVES

Dans le contexte de la résilience des systèmes critiques, alerter les opérateurs des informations relevant de la sûreté et de la sécurité est crucial pour qu'ils puissent construire et maintenir une conscience de la situation et naviguer face à des événements sans précédent, imprévisibles.

S'appuyant sur l'état de l'art qui présente succinctement les notions d'ingénierie et d'architecture des systèmes, de sûreté et de résilience des systèmes, de surveillance de l'état des systèmes afin de contribuer à la conscience de la situation par les opérateurs, et la sécurité des systèmes, cet article propose d'articuler sûreté et sécurité afin d'élaborer une alerte intégrant ces deux dimensions et leurs interactions. Cette alerte a pour objectif de contribuer à la construction et au maintien d'une compréhension de l'état et de la dynamique du système, en particulier face à l'adversité, à des événements imprévisibles et sans précédent, afin que les opérateurs puissent piloter à vue.

Des sujets non traités dans cette proposition constituent des perspectives de recherche. Il s'agit en particulier de la dynamique de l'élaboration de l'alerte en tenant compte des temporalités différentes de la sécurité et de la sûreté, des contraintes que l'intégration de ces dimensions génèrent sur l'architecture du système, enfin des traitements pour constituer une alerte claire et précise à partir des données brutes. Des architectures traitant explicitement sûreté et sécurité sont aussi à proposer.

En ce qui concerne la gestion des accès [11], il n'est pas possible de définir *a priori* l'ensemble des acteurs et systèmes auxquels devront être communiquées les alertes de sûreté. En effet, ces acteurs et ces systèmes sont ceux qui sont affectés par l'état et la dynamique d'un système. Il faut donc envisager un contrôle d'accès dynamique et contextuel. Par exemple, l'alerte concernant un car scolaire bloqué à un passage à niveau doit être diffusée aux trains circulant à proximité du passage à niveau afin qu'ils puissent freiner au plus tôt et éviter un accident. En revanche, cette alerte n'a pas à être diffusée aux systèmes qui ne sont pas affectés par la présence du car scolaire au milieu du passage à niveau, tels que des trains à l'arrêt sur un site de maintenance.

D'autres travaux sont à mener pour articuler les modèles de la sécurité et ceux de la sûreté, en particulier pour définir et clarifier les notions relatives aux risques, aux menaces, à l'aune des enjeux de la résilience.

6. RÉFÉRENCES

[1] ANSSI : Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) ; Section 5 ; outillage pour le traitement des risques SSI. février 2004.

[2] ANSSI : Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) ; Méthode de gestion des risques. janvier 2010.

[3] BNAE : RG.Aéro 000 721 ; Recommandations Générales pour l'architecture des BIT dans un système intégré, 2015.

[4] Xavier Chalandon : Conscience de la situation : invariants internes et invariants externes. Thèse de Doctorat d'Ergonomie soutenue le 2 mai 2007 (CNAM), 2013.

[5] Mohammed Gad El Rab : Évaluation des systèmes de détection d'intrusion. Thèse de Doctorat, Université Paul Sabatier - Toulouse III, 2008.

[6] ISO 9241-11 : Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) -- Partie 11: Lignes directrices relatives à l'utilisabilité, 1998.

[7] ISO 9241-110 : Ergonomie de l'interaction homme-système -- Partie 110: Principes de dialogue, 2006.

[8] ISO/IEC 27004: Information security management — Measurement, 2009.

[9] ISO/IEC 27032 : Information Technology – Security Techniques – Guidelines for security,(2012.

[10] ISO/IEC 27001 : Information Technology – Security Techniques – Information Security management systems – Requirements, 2013.

[11] ISO/IEC 27002 : Code de bonne pratique pour le management de la sécurité de l'information, 2013.

[12] NF ISO/CEI 27005 : Gestion des risques liés à la sécurité de l'information, 2013.

[13] NF ISO/CEI 27000 : Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire, 2015.

[14] Dominique Luzeaux : Ingénierie des grands systèmes complexes. In Dominique Luzeaux, Jean-René Ruault & Jean-Luc Wippler (Eds.), Maîtrise de l'ingénierie des systèmes complexes et des systèmes de systèmes : études de cas, Hermes-Lavoisier, Paris, pp. 21-106, 2011.

[15] Dominique Luzeaux et Jean-René Ruault : L'ingénierie système. Collection 100 questions pour comprendre et agir, AFNOR éditions, Paris, 2013.

[16] Ministère de l'écologie et du développement durable : Guide pour l'estimation des dommages matériels potentiels aux biens des tiers en cas d'accidents majeurs, 2010.

[17] MIL-STD-882E : System Safety. Department of Defense Standard Practice, 2012.

[18] National Institute of Standards and Technology: Common Industry Specification for Usability – Requirements ; NISTIR 7432, 2007.

[19] Ludovic Piètre-Cambacèdés : Des relations entre sûreté et sécurité. Thèse de doctorat Informatique et Réseaux, soutenue le 3 novembre 2010 (Paris),

[20] Jean-René Ruault, Frédéric Vanderhaegen & Dominique Luzeaux : Sociotechnical systems resilience. 22nd Annual INCOSE International Symposium, Rome, 2012.

[21] Jean-René Ruault, Frédéric Vanderhaegen et Christophe Kolski : 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, 2013.

[22] Jean-René Ruault : Proposition d'architecture et de processus pour la résilience des systèmes ; application aux systèmes critiques à longue durée de vie. Thèse de Doctorat en Automatique soutenue le 7 juillet 2015 (Valenciennes), 2015.

[23] N. B. Sarter et D. D. Woods : Situation awareness: A critical but ill-defined phenomenon. International Journal of Aviation Psychology, vol. 1, n°1, pp. 45–57, 1991

[24] Frédéric Vanderhaegen : Analyse et contrôle de l'erreur humaine. Hermès-Lavoisier, Paris, 2003.

[25] Frédéric Vanderhaegen: Human-error-based design of barriers and analysis of their uses. Cognition, Technology and Work, 12(2), pp. 133-142, 2013.

BIOGRAPHIES

Jean-René Ruault, expert technique navigabilité, DGA ; enseignant-chercheur rattaché au LAMIH, université de Valenciennes

Diplômé de l'EHESS, il obtient un doctorat en automatique à l'université de Valenciennes en juillet 2015. Il est qualifié aux fonctions de maître de conférences dans cette discipline. Il rejoint la DGA en 2004 après avoir travaillé plus de dix ans dans des sociétés de service. Il est actuellement expert technique navigabilité dans le domaine aéronautique. Il a été qualifié au niveau expert en 2008 pour ses activités d'ingénierie de systèmes au sein du pôle système de systèmes de la DGA. Il est membre de l'AFIS depuis 2001, association à laquelle il contribue activement. Il a publié une trentaine d'articles dans le domaine de l'ingénierie de systèmes et des interactions homme-machine. Dominique Luzeaux, Jean-Luc Wippler et lui ont co-rédigé des ouvrages consacrés à l'ingénierie système et à l'ingénierie de systèmes de systèmes, parus chez ISTE et chez AFNOR éditions. Il enseigne l'ingénierie système et les IHM. Il a été coprésident de la conférence Ergo'IA 2006.

Christophe Kolski, professeur en informatique

Il a obtenu le doctorat en 1989 et l'Habilitation à Diriger des Recherches en 1995. Il est spécialisé en Interaction Homme-Machine (IHM), plus particulièrement en méthodes et modèles pour la conception et l'évaluation de systèmes interactifs, et en interaction aussi bien intelligente que tangible. Il enseigne le génie logiciel et l'IHM à l'Université de Valenciennes et du Hainaut-Cambrésis. Il est actuellement directeur-adjoint du Département Informatique au LAMIH-UMR CNRS 8201. Il a été président du comité d'organisation de la conférence CADUI'2002, co-président des comités scientifiques des conférences IHM'2003 et ERGO-IA'2006 et co-organisateur de plusieurs workshops ces dernières années. Il est auteur, co-auteur ou éditeur de nombreux livres, chapitres de livres, numéros spéciaux de revues, articles dans des revues et conférences nationales et internationales. Les derniers livres qu'il a édités sont « Interaction homme-machine dans les transports - personnalisation, assistance et informations du voyageur » (Hermes Science Publications) et « Human-Computer Interactions in Transport » (ISTE Ltd and John Wiley & Sons).

Dominique Luzeaux, directeur adjoint de la direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense

Diplômé de l'École Polytechnique (1987) et de l'École Nationale Supérieure des Techniques Avancées (1989), Docteur de l'Université de Paris XI (1991), chercheur invité à l'université de Berkeley jusqu'en 1992, Dominique Luzeaux est employé par le Ministère de la Défense depuis plus de vingt ans, où il est actuellement directeur adjoint de la direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense. Habilité à diriger des recherches (2001), il a encadré une douzaine de thèses de doctorat et a publié une centaine d'articles dans des conférences et revues nationales et internationales. Il enseigne l'ingénierie des systèmes de systèmes dans diverses écoles d'ingénieur et en formation continue, en France et à l'étranger, et est rattaché à la chaire ingénierie des systèmes complexes de l'École Polytechnique. Il est l'auteur de plusieurs ouvrages en français et en anglais sur les nanotechnologies, sur la simulation, sur l'ingénierie de systèmes, sur les systèmes de systèmes.

Frédéric Vanderhaegen, Professeur en Génie Informatique et Automatique.

Il a obtenu son doctorat en 1993 et son Habilitation à Diriger des Recherches en 2003 en Automatique Industrielle et Humaine à l'Université de Valenciennes et du Hainaut-Cambrésis (UVHC). Entre 1995 et 2005 il est Chargé de Recherche au CNRS. Depuis 2005, il est Professeur à l'UVHC. En 1994, il effectue un stage postdoctoral au Centre Commun de Recherche d'Ispra en Italie avec le Professeur Pietro-Carlo Cacciabue. De 2004 à 2014, il dirige l'équipe « Systèmes Homme-Machine » du Laboratoire d'Automatique, de Mécanique et d'Informatique industrielles et Humains (LAMIH). Il est directeur ou président de différents groupes d'animation de la recherche (GDR I HAMASYTI du CNRS; pôle HORTENS d'EURNEX ; GIS GRAISyHM ; IFAC TC HMS ; GT ASHM du GDR MACS). Il est rédacteur en chef avec Oliver Carsten de Leeds de la revue scientifique « Cognition Technology & Work ». Il gère plusieurs projets de recherche nationale ou internationale, et est auteur ou coauteur de nombreux articles dans des revues ou conférences scientifiques. Il est ou a été président de comités d'organisation ou de programme de plusieurs manifestations (Symposium international IFAC/IFIP/IFORS/IEA en Analyse, Conception et Évaluation des Systèmes Homme-Machine; Ateliers et Conférence en Ergonomie et Informatique Avancée, ERGO-IA ; Conférence du GIS 3SGS). Il est directeur d'un projet national du programme d'excellence IDEFI-UTOP sur la recherche pédagogique en formation à distance dans le domaine du ferroviaire et les transports guidés. Il est responsable pédagogique du parcours INERSYG (Ingénierie Ferroviaire et Systèmes Guidés) du Master Transport, Mobilité, Réseaux de l'UVHC.

Wilson Goudalo, ingénieur de recherche

Wilson Goudalo, ingénieur de recherche, directeur de projets de transformation numérique, expert en architecture d'entreprise et sécurité des systèmes d'information. Ingénieur de recherché en mathématiques appliquées à l'informatique, spécialisé en génie logiciel et sécurité à LETI (Saint-Pétersbourg, 1997), Wilson Goudalo a conçu le système d'authentification par la frappe au clavier lors de ses travaux de recherche à l'Académie des Sciences de Russie à Saint-Pétersbourg en 1996 et a élaboré l'ingénierie de la sécurité des SI lors de ses travaux à l'université Paris Descartes en 2008. Il a 18 ans d'expériences professionnelles dans les systèmes d'information des entreprises, où il est employé en tant que directeur de projets de transformation numérique et expert en architecture d'entreprise et en sécurité des systèmes d'information. À présent, il est directeur du département R&D et Innovation – Économie digitale et développement socio-économique, chez ABE (Advanced Business Engineering) et Doctorant au LAMIH-UMR CNRS 8201 - UVHC (Université de Valenciennes et Hainaut-Cambrésis). Il est co-auteur de plusieurs articles dans des conférences internationales et a été Industry Research co-Chair de la conférence internationale SECURWARE en 2009.