A version of this document has been published in: *Ingénierie des Systèmes d'Information (ISI), Networking and Information Systems, 22 (1), pp. 65-107, 2017.*

Vers une ingénierie avancée de la sécurité des SI d'entreprise, Une approche conjointe de la sécurité, de l'utilisabilité et de la résilience dans les systèmes sociotechniques

Wilson Goudalo[1,2], **Christophe Kolski**[1], **Frédéric Vanderhaegen**[1]

1. LAMIH-UMR CNRS 8201, Université de Valenciennes
59313 Valenciennes, France
{wilson.goudalo, christophe.kolski; frederic.vanderhaegen}@univ-valenciennes.fr

2. Research and Innovation Department, Advanced Business Engineering
77400 Lagny, France
wilson.goudalo@abe-engineering.net

RESUME. A notre ère de l'industrie des services, des systèmes d'information jouent une place prépondérante. Ils tiennent même parfois une position vitale pour les entreprises, les organisations et les individus. Les systèmes d'information sont confrontés à de nouvelles menaces de sécurité, de façon continue ; celles-ci sont de plus en plus sophistiquées et de natures différentes. Dans ce contexte, il est important d'empêcher les attaquants d'atteindre leurs résultats, de gérer les failles inévitables et de minimiser leurs impacts. Les pratiques de sécurité doivent être menées dans un cadre d'ingénierie ; l'ingénierie de la sécurité doit être améliorée. Pour cela, il est proposé de développer des approches systémiques, innovantes sur de larges spectres et qui fonctionnent sur plusieurs axes de manière conjointe, en améliorant l'expérience utilisateur. Notre objectif est de traquer et résoudre de façon concomitante et harmonieuse les problèmes de la sécurité, de l'utilisabilité et de la résilience dans les systèmes d'information d'entreprise. Dans cet article, nous positionnons les systèmes sociotechniques au regard des systèmes d'information des entreprises et des organisations. Nous traitons les paradigmes de systèmes sociotechniques et nous portons une attention particulière sur les corrélations entre la sécurité, l'utilisabilité et la résilience. Une étude de cas illustre l'approche proposée. Elle présente l'élaboration de design patterns (modèles de conception) pour améliorer l'expérience utilisateur. L'article se termine par une discussion globale de l'approche, ainsi que par des perspectives de recherche.

ABSTRACT. In our era of the service industry, information systems play a prominent role. They even hold a vital position for businesses, organizations and individuals. Information systems are confronted with new security threats on an ongoing basis; these threats become more and more sophisticated and of different natures. In this context, it is important to prevent attackers from achieving their results, to manage the inevitable flaws, and to minimize their impacts. Security practices must be carried out within an engineering framework; Security engineering needs to be improved. To do this, it is proposed to develop systemic approaches, innovative on wide spectra and that work on several axes together, improving the user experience. Our goal is to jointly track down and resolve issues of security, usability and resiliency in enterprise information systems. In this paper, we position sociotechnical systems with regard to the information systems of companies and organizations. We address paradigms of sociotechnical systems and refocus on the correlations between security, usability and resilience. A case study illustrates the proposed approach. It presents the development of design patterns to improve the user experience. The article concludes with an overall discussion of the approach, as well as research perspectives.

MOTS-CLES : sécurité, utilisabilité, résilience, sémantique, métrique, modèle conceptuel, analyse conjointe, BPMN, UML, modèles de conception, expérience utilisateur, respect de la vie privée, SI d'entreprise, systèmes sociotechniques.

KEYWORDS: security, usability, resilience, semantics, metrics, conceptual model, joint analysis, BPMN, UML, design patterns, user eXperience, privacy, enterprise IS, socio-technical systems.

1. Introduction

Dans un passé récent, les systèmes étaient développés pour des utilisateurs avertis, dans le cadre d'un contexte d'utilisation bien défini. Ils étaient fournis avec de volumineuses documentations qui étaient souvent difficiles à exploiter. A l'ère de l'industrie des services, les systèmes, les produits et les services sont fournis pour être utilisés (consommés) par des utilisateurs lambda dans leur vie de tous les jours. L'industrie des services est caractérisée par un contexte socio-économique de "*time to market*", très concurrentiel et soumis à de fortes règlementations. Ces services (systèmes et produits) numériques envahissent toutes les sphères de la vie (vie privée, données de santé, activités professionnelles et personnelles, toutes les activités socio-économiques). De même, les problèmes de sécurité et de respect de la vie privée (privacy) sont essentiels dans de nombreux services (SBIC, 2008 ; IBM, 2014 ; KPMG, 2014 ; Umhoefer & *al.*, 2014). Comme un attribut de qualité, les appréhensions sur la

sécurité ont évolué, puis les technologies dans l'industrie, les normes et les travaux de recherche se sont adaptés à cette évolution (HSC, 2011).

La figure 1 illustre la vision classique de la sécurité informatique, essentiellement orientée risques. Quels que soient les risques et menaces qui s'exercent sur un système et quels que soient les besoins de sécurité exprimés pour ce dernier, le système de sécurité conçu et mis en place doit être suffisamment :

– Large, pour couvrir tout le périmètre du système informatique et pour empêcher les risques et menaces de le contourner ;

– Solide, pour résister à toute tentative de pénétration et pour ne pas se faire casser lui-même par les risques et menaces ;

– Concis, pour être en adéquation avec les besoins de sécurité du système informatique.

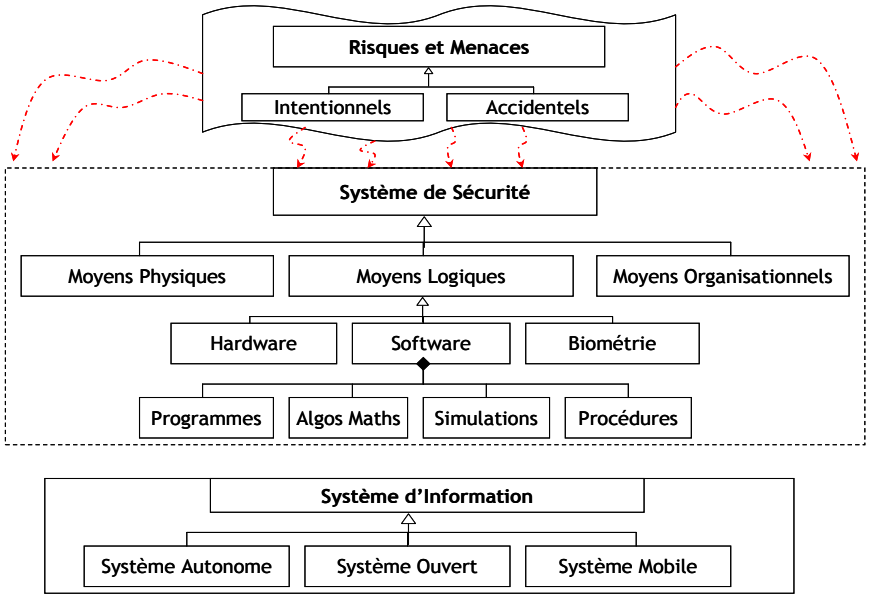


Figure 1. Vision classique sur la sécurité informatique

Dans le domaine des systèmes informatiques, les initiatives ont été principalement basées sur « la sécurisation du périmètre » pendant très longtemps. Dans le cas du système d'information et de l'entreprise étendue, des initiatives ont évolué vers une stratégie de sécurité en profondeur. Ce qui est illustré dans (Hafiz et Johnson, 2009 ; Murphy et Murphy, 2013 ; Jaeger, 2016). Au-delà des risques qui sont implicites au système d'information, il y en a qui sont induits par le fonctionnement même du système d'information : les applications d'entreprise et les activités quotidiennes des acteurs internes à l'entreprise ou à l'organisation. Pour améliorer la stratégie de sécurité en profondeur, Goudalo et Seret (2008) ont proposé une approche méthodologique qui fonctionne sur la construction d'un canevas d'adhésion pour tous les acteurs de l'entreprise. De nombreux progrès ont été réalisés aussi bien dans la communauté des chercheurs que dans l'industrie. Les pratiques et normes internationales ont évolué. Cependant les problèmes de sécurité persistent et causent des conséquences graves voire vitales pour les individus, les entreprises et les organisations. Les chercheurs de RAND Corporation estiment les coûts totaux d'événements cybernétiques à environ 8,5 milliards de dollars par année (Romanosky, 2016).

Le rapport de l'étude réalisée par le cabinet d'audit et de conseil PwC (PwC Etude Sécurité, 2016) confirme les mêmes observations sur l'état actuel de la sécurité informatique. Les cas d'attaques informatiques sont devenus considérables et causent des dommages très lourdes de conséquences ; année après année, les cyber attaques continuent de s'aggraver en fréquence, en gravité et en impact. Les méthodes de prévention et de détection se sont révélées largement inefficaces face à des agressions de plus en plus habiles ; ainsi de nombreuses organisations ne savent pas quoi faire ou n'ont pas les ressources pour combattre les cybercriminels hautement qualifiés et agressifs. Depuis quelques années, les universitaires et les industriels travaillent ensemble avec succès pour améliorer les technologies et les méthodes de sécurité. Cependant le nombre d'incidents de sécurité augmente en termes d'ampleur, d'impacts et de fréquences.

Ces renseignements (Romanosky, 2016 ; PwC Etude Sécurité, 2016) confirment que nous assistons à un défi crucial pour l'ensemble de l'économie numérique. Ce contexte actuel de la sécurité informatique constitue la principale motivation de nos travaux ; cela représente le principal verrou scientifique qu'il s'agit de contribuer à lever.

Aujourd'hui, nous sommes confrontés à un besoin urgent de nouvelles approches axées sur les aspects humains, y compris l'utilisabilité (Lewis, 2014) pour assurer la sécurité des systèmes. En effet les systèmes sont utilisés par les humains, bien que certains d'entre eux soient de plus en plus automatisés. Ferrary (2014) a montré que les ressources humaines sont maintenant au cœur du business modèle des organisations et a pointé « le facteur humain comme principale source du risque opérationnel dans le secteur bancaire ». Le livre de Cranor et Garfunkel (2005) indique les tendances de la recherche en matière de sécurité et d'utilisabilité. Le livre de Clarke et Furnell (2014) présente l'état de l'art sur « l'aspect humain dans la réussite de la sécurité ». Toutes ces initiatives sont menées sur des solutions de sécurité spécifiques. Aussi bien chez les universitaires que chez les

industriels, nous remarquons un manque de recherche sur l'ingénierie globale de la sécurité du point de vue de l'IHM (interaction homme-machine) et de l'ergonomie. L'étude de Ponemon Institute montre les causes de la violation de données en 2015 (Ponemon Institute LLC, 2015) : attaques malveillantes ou criminelles pour 47 %, anomalies du système (défaillances de la technique et des processus métier) pour 29 % et le facteur humain (employés négligents, erreurs humaines) pour 25 %. Ces chiffres confortent les objectifs de nos travaux : « rendre les services numériques fiables, protégés et sécurisés de façons efficaces, faciles d'utilisation et résilients ».

Dans cet article, étendant largement celui présenté dans l'atelier « Sécurité des SI : technologies et personnes » d'Inforsid 2016 (Goudalo *et al*., 2016), nous suggérons de présenter nos travaux sur l'ingénierie conjointe de la sécurité, l'utilisabilité et la résilience. Nous nous concentrons sur les systèmes socio-techniques (SST), sur la vie privée et sur la confiance. Dans la section suivante, nous rappelons l'état de l'art. Nous décrivons notre contribution dans la section 3. La section 4 présente une étude de cas dans le domaine médical. Enfin, la dernière section conclut nos travaux.

2. Ètat de l'art

Dans ce chapitre, nous présentons l'état de l'art sur les systèmes sociotechniques, la sécurité et ses indicateurs de suivi, l'utilisabilité et la résilience.

2.1. Systèmes socio-techniques

Le concept de système sociotechnique a été créé à la fin des années 1950, dans un contexte d'études menées par l'institut Tavistock à Londres (Trist *et al*., 1963 ; Emery, 1967). Sperber et Wilson traitent la pertinence de la communication (et cognition) dans le contexte social (Sperber et Wilson, 1995). Elayne Coakes définit le terme sociotechnique comme étant l'étude des relations et interrelations entre les parties sociales et techniques de tout système (Coakes, 2002). Les systèmes sociotechniques visent à modéliser ensemble les capacités humaines, sociales et technologiques dans l'utilisation et le traitement des services à valeur ajoutée. Singh définit les systèmes sociotechniques comme des systèmes physiques et cyber à plusieurs parties prenantes (Singh, 2013) (« multi-stakeholder cyber and physical systems »). En effet, les systèmes sociotechniques soutiennent la complexité et le changement à la fois dans les mondes physiques (sociaux) et cyber.

De nos jours, les relations sociales sont mélangées avec les relations de nature cybernétique. Les activités sur les principaux réseaux sociaux et leurs pendants dans la vie sociale en sont une preuve. De même, la vie privée, la vie professionnelle et la vie publique se rapprochent et se mélangent. C'est le cas notamment du consumérisme et de la BYOD (*Bring Your Own Device*). Les données de la vie privée des employés se retrouvent ensemble avec les données d'entreprise sur des média personnels et/ou des systèmes professionnels. Les SST traitent des données sensibles et fournissent des services de valeur[1]. Au même moment, les utilisateurs adoptent un comportement ubiquitaire et présentent une forte volatilité avec des attentes insaisissables. A notre ère actuelle de l'industrie des services, le succès des SST nécessite une réelle sécurité (confiance, respect de la vie privée, intégrité, confidentialité) avec la satisfaction de toutes les parties prenantes, dont les utilisateurs (IBM Corporation, 2014).

2.2. Sécurité

La famille des normes ISO 27000 (ISO/IEC 270xx, 2010) est dédiée à la sécurité de l'information et est devenue le principal cadre de référence de la sécurité dans le monde entier. Ces normes présentent comment établir, mettre en œuvre, maintenir et améliorer continuellement un système de gestion de la sécurité de l'information. Elles définissent la sécurité en termes de trois concepts fondamentaux : la confidentialité, l'intégrité et la disponibilité des informations, en appliquant un processus de gestion des risques. D'autres normes internationales et locales portent également sur la sécurité, ainsi que sur les risques de sécurité des SI. Internationales ou locales, toutes les normes opèrent sur ces trois critères fondamentaux de la sécurité. A ces derniers, sont rajoutés différents attributs et propriétés de sécurité tels que preuve, trace, non-répudiation, identification, authentification que nous suggérons de rassembler pour assurer le concept de l'imputabilité.

Dans les SST, notamment dans le domaine des systèmes médicaux, les attributs du respect de la vie privée et de la confiance sont liés indéniablement à la sécurité. Westin dans son remarquable livre *La vie privée et la liberté* (Westin, 1970) avait ouvert le champ moderne du droit et de la vie privée. Nous utilisons le respect de la vie privée (*privacy*) à la fois comme la confidentialité et l'intégrité des informations ; le respect effectif de la vie privée renforce la confiance des consommateurs. Dans (Cranor et Blase, 2015), les auteurs définissent différents aspects du respect de la vie privée. Pour réussir la sécurité des systèmes d'information dans les entreprises, Goudalo et Seret (2008) ont proposé une approche méthodologique opérant sur la construction d'un canevas d'adhésion de toutes les parties prenantes de l'organisation. Aussi les travaux de Clarke et Furnel (2014) se rapportent à l'aspect humain (dont l'utilisabilité) dans la réussite de la sécurité.

---

[1] *Services de valeur* - Services contribuant de façon essentielle à la chaîne de valeur (cf. Chaîne de valeur, Porter (1980) et Chaptal de Chanteloup (2015))

2.3. Métriques et indicateurs de suivi de la sécurité

Nous définissons les indicateurs de suivi de la sécurité, en introduisant la notion de la qualité de sécurité. Avec une première approche, la qualité est assimilée à l'ensemble des exigences fonctionnelles et non fonctionnelles (Bernardez *et al.*, 2005). La Qualité est un méta-concept qui présente différentes significations aux différentes parties prenantes (comme les Clients, les Partenaires, les Utilisateurs, les Manageurs, les Concepteurs, les Réalisateurs, les Exploitants). En d'autres termes, c'est un méta-concept qui s'affine et qui désigne différentes notions en fonction de l'objet qualifié. Pour conférer des définitions concrètes aux exigences de qualité en termes de la sécurité, nous utilisons une décomposition de la qualité sous la forme de modèle de qualité. Nous représentons un méta-modèle associé à la qualité de sécurité dans la Figure 2.

Nous avons présenté ce méta-modèle sous forme d'un diagramme de classes UML et nous y avons introduit les concepts suivants : aspects de sécurité, sous-aspects de sécurité, les critères et les métriques. Nous fournissons, ci-dessous, quelques exemples pour illustrer ce méta-modèle.

– Le contrôle d'accès présente des sous-aspects comme l'identification, l'authentification et l'autorisation ;

– L'intégrité présente des sous-aspects comme l'intégrité des applications, l'intégrité des communications, l'intégrité des données, l'intégrité des infrastructures, l'intégrité du personnel ;

– La disponibilité présente les sous-aspects comme la fiabilité, la robustesse (tolérance aux pannes ou haute disponibilité) et la performance (équilibrage de charges ou garantie de temps de réponse).

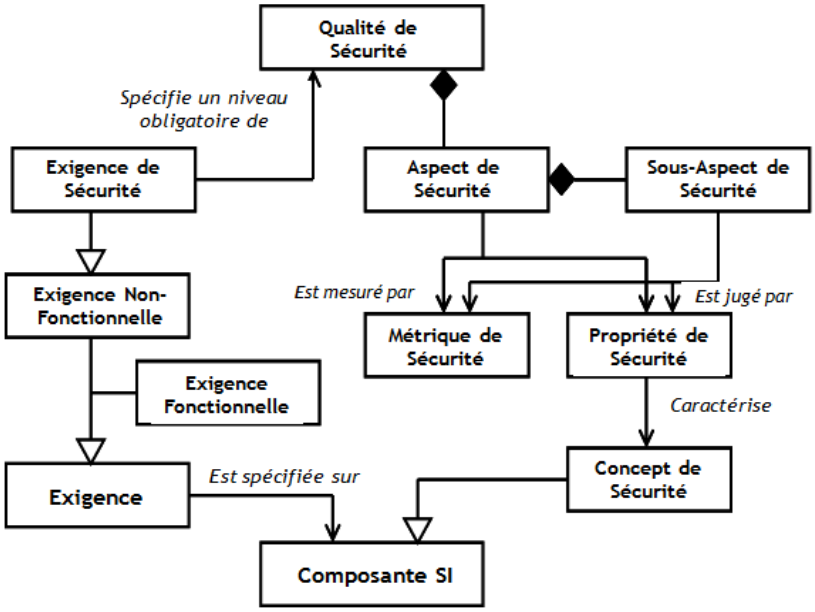


Figure 2. Méta-modèle de qualité de la sécurité (Goudalo et Seret, 2009)

Nous avons principalement mis en évidence les notions de critère (descriptible) et de métrique (mesurable) sur les aspects et les sous-aspects de la qualité de la sécurité, pour obtenir des indicateurs clairs sur l'amélioration de la qualité de la sécurité du système d'information.

Pour définir les règles de sécurité du système d'information, les chercheurs et les experts en sécurité utilisent habituellement les concepts de sujet et d'objet, introduits par Bell et La Padula (1975) et repris dans les travaux de Cuppens F. (1997). Pour assurer le suivi des indicateurs de sécurité dans un repère homogène, nous étendons ces deux concepts (standards de sujet et d'objet) par l'introduction d'un troisième groupe qui est la notion de solutions de sécurité. Pour protéger les actifs de l'entreprise, les solutions de sécurité doivent être efficaces. Nous reprenons la définition en précisant ce qui suit. Un système d'information sécurisé d'entreprise se compose des :

– Objets qui présentent des niveaux de sensibilité (suivant les critères de sensibilité) ;

– Sujets qui présentent des niveaux de confiance (suivant les critères de confiance) ;

– Solutions de sécurité qui présentent des niveaux d'efficacité (suivant les critères d'efficacité).

Pour tous les éléments d'une catégorie ou d'une autre, nous établissons les indicateurs de sécurité dans un système de métriques homogènes, à quatre niveaux quel que soit le critère choisi (sensibilité, confiance ou efficacité). Dans l'ordre croissant, les quatre niveaux du système métrique homogène sont : « 0 », « 1 », « 2 » et « 3 ». Ci-dessous, quelques exemples.

– Un système de contrôle d'accès avec badges biométriques, dans la mesure où il est bien géré, il correspond à « 3 » (Très efficace) pour la métrique d'indicateur de sécurité (Critère d'efficacité).

– Dans l'architecture technique d'un SI, un firewall installé à côté du routeur frontal et dont la configuration n'a pas tenu compte de la politique de sécurité de l'entreprise correspond à « 0 » (Pas efficace) pour la métrique d'indicateur de sécurité (Critère d'efficacité).

– Un jeune trader proposé au poste de directeur de salle de marché (alors qu'il sort tout juste de l'école de formation, sans expérience) correspond à la métrique de l'indicateur de sécurité (Critère de confiance) : « 0 », c'est-à-dire pas de confiance en ce sujet pour ce poste. Le poste lui-même correspond à la métrique de l'indicateur de sécurité (Critère de sensibilité) : « 3 », c'est-à-dire très sensible pour les enjeux de l'entreprise.

La mesure[2] de sécurité, consistant à faire former ce jeune, et de très près avec un directeur chevronné, et pendant quelques années, et dans une salle de marché, correspond à « 1 » (c'est-à-dire peu efficace) pour la métrique d'indicateur de sécurité (Critère d'efficacité).

2.4. Utilisabilité

La garantie de l'utilisabilité permet aux utilisateurs d'atteindre leurs buts et de satisfaire leurs besoins dans un contexte particulier d'utilisation. Le contexte d'utilisation est défini par l'ensemble des utilisateurs, tâches, équipements et environnements physiques, sociaux et cyber qui peuvent tous influer sur la facilité d'utilisation d'un service (produit ou système). La norme ISO 9241-41 (1998) définit l'utilisabilité sous l'angle de l'ergonomie, comme étant « la mesure dans laquelle un produit peut être utilisé par des utilisateurs spécifiques pour atteindre les objectifs spécifiés avec efficacité, efficacité et satisfaction dans un contexte d'utilisation spécifié ». La norme comprend aussi une explication de la manière dont l'utilisabilité d'un produit peut être spécifiée et évaluée dans le cadre d'un système de qualité. Sous l'angle de l'ingénierie logicielle, la norme ISO/IEC 9126 (1991), d'une part, définit l'utilisabilité comme étant « un ensemble d'attributs qui portent sur l'effort nécessaire pour l'utilisation, et sur l'évaluation individuelle d'une telle utilisation, par un ensemble d'utilisateurs déclarés ou implicites », ces attributs sont l'efficacité, la productivité, la sûreté, et la satisfaction. D'autre part, une version plus récente de la norme (ISO/IEC FDIS 9126-1, 2000) décrit six groupes de qualités de logiciel, pertinentes pendant le développement : le groupe relatif à la fonctionnalité (l'exactitude, la convenance, l'interopérabilité, la sécurité) ; le groupe de l'utilisabilité (la compréhensibilité, l'apprentissage, l'opérabilité, l'attractivité) ; le groupe de fiabilité (la maturité, la tolérance aux pannes, la capacité à recouvrer, la disponibilité) ; le groupe de l'efficience (le temps, le comportement, la ressource, l'utilisation) ; le groupe relatif aux capacités de maintenance (l'analysabilité, la capacité à être changée, la stabilité, la testabilité) et le groupe de portabilité (l'adaptabilité, la capacité à être installée, la coexistence, la capacité à être remplacée). Tous ces aspects et attributs se rapportent à la qualité de l'utilisation du produit (système ou service) fourni, dans le contexte d'utilisation. Shackel (2009) définit l'utilisabilité sur la base de trois critères : la performance de la tâche, la satisfaction des utilisateurs, et les coûts.

La maturité acquise au fil des décennies renforce notre évaluation de l'utilisabilité. Une simple mesure de l'utilisabilité ne serait pas suffisante, compte tenu de la complexité de tous les facteurs de contexte à prendre en considération et compte tenu de l'absence totale d'un *utilisabilité-mètre* (à l'instar d'un thermomètre). Bevan *et al.* (Bevan *et al.*, 2015) indiquent qu'il est maintenant plus appréciable d'évaluer l'utilisabilité au lieu de la mesurer, même si la norme ISO 9241-11 met l'accent sur sa mesure.

2.5. Résilience

La résilience est un concept du monde réel qui est utilisé dans plusieurs domaines. Ramenée aux systèmes d'information, la résilience est une préoccupation majeure de nos jours, afin de prévenir un incident et plus encore pour restaurer un état stable après un accident ou une faute intentionnelle (Laprie, 2008 ; ReSIST, 2015). En rapport à la préoccupation de l'accident (Hollnagel *et al.*, 2006), la résilience est appliquée dans de nombreux domaines tels que l'ingénierie des systèmes sociotechniques.

En écologie, la résilience est la capacité d'un écosystème ou d'une espèce à récupérer un fonctionnement et/ou un développement normal après avoir subi un traumatisme. En économie, la résilience est la capacité à revenir sur la trajectoire de croissance après avoir encaissé un choc. En psychologie, « la résilience est la capacité d'une personne ou d'un groupe à bien se développer, à continuer à se projeter dans l'avenir, en dépit d'événements déstabilisants, de conditions de vie difficiles, de traumatismes parfois sévères » (Colas et Sarron, 2009).

Luzeaux a écrit que « la résilience est obtenue grâce à la capacité de surveiller les conditions aux limites de l'enveloppe de performance et à la capacité d'adapter le comportement opérationnel du système aux développements potentiels de cette enveloppe » (Luzeaux, 2011). En d'autres termes, être résilient, c'est « rebondir pour retrouver son équilibre », c'est la poursuite de la viabilité, au mépris éventuel des performances. Afin d'éviter toute confusion, nous précisons que la robustesse est la capacité de pouvoir maintenir le niveau de performance alors que les conditions exogènes ont un peu changé.

La résilience est considérée comme une vertu active intégrée dans tous les systèmes et opérations actuels, notamment dans le domaine de la défense (Palin, 2013). Aujourd'hui, les stratégies géopolitiques et économiques intègrent simultanément les cinq

[2] NB. Nous précisons qu'il s'agit d'un cas illustratif maîtrisé qui ne peut survenir par hasard dans une vraie entreprise.

axes d'influence (cyber, espace, air, maritime et terre), pour réaliser les activités et opérations de prévention, protection, atténuation, réponse, rétablissement, correction et sauvetage. La protection de l'infrastructure et la continuité fonctionnelle sont alignées pour rendre une vertu active intégrée, c'est-à-dire la résilience. La vertu est définie comme « la capacité de prendre des mesures appropriées et correctes qui profitent à la fois l'acteur et les autres », par le philosophe Romain Lucius Annaeus Seneca (Stanford, 2016). Nous inspirant du professeur Laprie (2008), nous concluons par la définition de la résilience des systèmes d'information en précisant qu'il s'agit de la capacité du système d'information à garantir la persistance d'un niveau acceptable de services fournis, avec une confiance justifiable, et ce même face à une attaque, une défaillance, ou une perturbation quelle qu'elle soit (faute, erreur, etc.). Un système résilient doit être doté des fonctions de résilience.

Luzeaux (2011) a défini quatre fonctions de la résilience, qui sont « l'évitement (capacité d'anticipation), la résistance (la capacité d'absorption), l'adaptation (la capacité de reconfiguration) et la récupération (ou le recouvrement est la capacité de restauration) ». Woods a défini quatre principaux axes sous le concept de la résilience : rebond (des événements perturbateurs ou traumatiques, les systèmes rebondissent et retournent à des activités antérieures ou normales) ; robustesse (malgré les événements perturbateurs ou traumatiques, les systèmes maintiennent la qualité et la performance antérieures ou normales de leurs activités) ; extensibilité gracieuse (à la survenance des évènements fragilisant ou éprouvant les limites des systèmes, ces derniers étendent leur performance ou bien apportent une capacité d'adaptation supplémentaire pour surmonter les évènements) ; l'adaptabilité durable (au fur et à mesure que les conditions évoluent en bien ou en mal au fil du temps, les règles de gouvernance soutiennent la capacité des systèmes à continuer à bien fonctionner et à éviter de tomber dans des pièges du business ou autres) (Woods, 2015). Woods a indiqué avoir défini ces quatre concepts en vue d'une ingénierie éventuelle de la résilience dans les systèmes et réseaux dans le futur.

Au cours des dernières années, la communauté des chercheurs et les professionnels mettent un accent particulier sur la résilience dans les différents domaines de l'industrie des services. Tel est le cas des initiatives suivantes : projet IRIS (*Infrastructure for Resilient Internet Systems* - Infrastructure des systèmes Internet résilients) (IRIS, 2016), projet RAMBO (*Resilient Architectures for Mission Assurance and Business Objectives* - Architectures résilientes pour l'assurance de mission et objectifs d'affaires) dans le cadre du Programme d'innovation FY11 MITRE (RAMBO, 2012), l'initiative européenne ReSIST (*Resilience for Survivability in IST* - Résilience pour survivabilité dans les IST) [ReSIST, 2016], et les travaux de la Commission européenne sur les questions de la résilience (European Commission, 2010, 2012, 2013). Ouedraogo *et al.* ont proposé des mesures sur la résilience (Ouedraogo *et al.*, 2013). Ruault *et al.* ont proposé une intégration de la résilience avec la sécurité et la sûreté, afin de surveiller les systèmes et alerter les opérateurs pour naviguer à vue (Ruault *et al.*, 2016).

2.6. Analyse critique sous l'angle d'approches conjointes

Dans cette section, nous avons présenté l'état de l'art des concepts de la résilience, de l'utilisabilité, de la sécurité et des indicateurs de suivi de la sécurité. Les travaux sont généralement centrés sur un domaine ; il nous semble donc important d'effectuer une étude critique sous l'angle d'approches conjointes.

Clarke et Furnell (2014) présentent dans leur livre (Clarke et Furnell, 2014) l'état de l'art sur « l'aspect humain dans la réussite de la sécurité ». Yee a proposé des patterns d'utilisabilité qui sont adaptés à la conception des systèmes de sécurité pour des fonctions spécifiques (Yee, 2002). Toutes ces initiatives sont menées sur des solutions de sécurité spécifiques. Aussi bien chez les universitaires que chez les industriels, nous remarquons un manque de recherche sur l'ingénierie globale de la sécurité du point de vue de l'IHM (interaction homme-machine) et de l'ergonomie.

Le risque zéro n'existe pas, quels que soient les efforts effectués, des problèmes surviennent. La prise en compte de la résilience dans les travaux de sécurité devient nécessaire à l'ère de l'économie numérique. La thèse de doctorat de Ludovic Piètre-Cambacédès (2010) évoque les relations entre la sûreté et la sécurité, sans proposer un cadre méthodologique pour adresser la sécurité et la résilience de manière conjointe. Les travaux sur les systèmes cyber et physiques (CPS – Cyber Physical Systems) commencent à intégrer la sécurité et la résilience. La récente étude réalisée par Siddhartha K. Khaitan et James D. McCalley sur les techniques de conception et applications des systèmes cyber et physiques (Khaitan et McCalley, 2015) présente un état de l'art sur l'intégration de la résilience et de la sécurité dans ces systèmes. Dans la conception de systèmes de commandes résilients pour les systèmes de transport et de distribution d'énergie, Quanyan Zhu et Tamer Basar ont eu recours à la théorie des jeux, afin d'utiliser la théorie des jeux pour traiter les compromis fondamentaux entre robustesse, résilience et sécurité des systèmes (Zhu and Basar, 2015). Dans (Giani and al., 2009), les auteurs ont travaillé sur la sécurité et la résilience des systèmes de transport et de distribution d'énergie aussi ; ils ont proposé des modèles et des techniques pour comprendre les vulnérabilités des systèmes de contrôle et leur impact sur les systèmes de transport et de distribution d'énergie électrique ; les auteurs ont proposé des solutions pour atténuer ces vulnérabilités spécifiques. Dans (Musman, 2016), Scott Musman a présenté les travaux de son équipe de chercheurs. Ces derniers ont utilisé une définition quantitative de la résilience et l'ont appliquée dans une approche inspirée de la théorie des jeux, considérant que plusieurs cyber-attaques sont en cours d'exécution. Cette approche permet de déterminer les actions des défenseurs comme une analyse de portefeuille, afin d'identifier une sélection prescriptive du meilleur emploi des méthodes de sécurité et de résilience à utiliser.

Le cadre méthodologique du NIST, dans ces récentes versions, sur l'amélioration de la cybersécurité dans les infrastructures critiques (NIST, 2016) intègre explicitement des aspects de la résilience du point de vue de la récupération après sinistre. Il intègre cinq fonctions majeures : identifier, protéger, détecter, répondre, récupérer. Les travaux de la Commission européenne sur la « protection de l'Europe contre les cyber-attaques et les perturbations à grande échelle » recommandent de concevoir la sécurité et la résilience dans tous les réseaux TIC (European Commission, 2010). Le programme européen ReSIST (ReSIST, 2016) prend en

compte ces recommandations à travers ses initiatives de recherche sur un cadre global de sûreté et de sécurité (« Towards a global dependability and security framework »). Le projet européen CAMINO (CAMINO, 2017) a pour objectif principal de fournir une feuille de route concrète pour améliorer la résilience contre la cybercriminalité et le cyber-terrorisme. Dans (Choras *et al*., 2015), les auteurs ont présenté les directions de recherche qui pourraient aborder les problèmes et atténuer les lacunes dans la lutte contre la cybercriminalité et le cyberterrorisme dans un délai jusqu'à 2025. Ils ont décrit l'approche « CAMINO THOR », considérant la cybersécurité de façon globale selon quatre dimensions : technique, humaine, organisationnelle et réglementaire. Aujourd'hui en France, nous distinguons les OIV, opérateurs d'importance vitale dont la cybersécurité rentre dans le dispositif de la loi de programmation militaire (ANSSI, 2016). Au-delà d'Ebios (EBIOS, ANSSI, 2016), aucun autre cadre méthodologique n'est encore publié par l'ANSSI, notamment en ce qui concerne l'ingénierie conjointe de la sécurité et de la résilience.

À ce stade, nous notons deux manques cruciaux :

– Absence d'initiatives qui intègrent la sécurité, l'utilisabilité et la résilience ;

– Absence d'approche méthodologique de type ingénierie globale de la sécurité, de l'utilisabilité et de la résilience, de manière conjointe.

Dans la section suivante, nous suggérons notre approche d'ingénierie avancée de la sécurité qui opère de manière conjointe sur la sécurité, l'utilisabilité et la résilience. La section d'analyse conjointe (3.2) exploite l'état de l'art d'une part, et d'autre part, étend celui-ci, afin d'opérer efficacement sur la sécurité, l'utilisabilité, la résilience et leurs corrélations réciproques dans les systèmes sociotechniques.

Dans la présentation du cadre de notre ingénierie conjointe, nous utilisons des patterns pour décrire les problèmes et les solutions adaptées aux problèmes de sécurité, d'utilisabilité et/ou de résilience. Les patterns sont largement adoptés dans de nombreuses activités humaines qui requièrent une combinaison de compétences et d'entraînements. Dans les années 1970, l'architecte Alexander a été le pionnier de la reconnaissance, du nommage et de l'utilisation de modèles lors de ses travaux de planification urbaine (Alexander *et al*., 1977). À la fin des années 1980, les informaticiens travaillant dans le domaine de la conception orientée objet ont découvert les travaux effectués par Alexandre et les ont adaptés au génie logiciel (Gamma *et al*., 1995 ; Salloway et Trott, 2002). Schumacher (2003) a fait valoir que l'ingénierie de la sécurité peut tirer bénéfice de l'utilisation des patterns, mais il ne parvint à présenter des patterns spécifiques pour atteindre cet objectif. Open Group a édité un livre sur les *design patterns* de la sécurité (Blakley *et al.*, 2004), mais n'a pas adressé l'alignement entre la sécurité et l'utilisabilité.

3. Ingénierie avancée de la sécurité des systèmes d'information

Face à la sophistication des attaques et à la banalisation des outils et procédés d'attaques, les pratiques de sécurité doivent être menées suivant des frameworks d'ingénierie et l'ingénierie de la sécurité devra s'améliorer dans un cycle vertueux. Dans ce travail, nous proposons une contribution en termes d'ingénierie avancée de la sécurité qui opère sur quatre concepts ensemble : les actifs d'entreprise, les risques auxquels ils sont exposés, les solutions de sécurité et les indicateurs de suivi dans une démarche d'amélioration continue. D'une part, notre approche d'ingénierie porte principalement sur la sécurité, mais de façon conjointe avec l'utilisabilité et la résilience des systèmes d'information. D'autre part, elle vise à adresser les corrélations réciproques de la sécurité, de l'utilisabilité et de la résilience.

Dans cette section, nous suggérons d'élaborer une approche systémique, large et innovante qui opère sur ces différents axes, afin d'améliorer l'expérience utilisateur de toutes les parties prenantes. Pour ce faire, nous recherchons et traitons, de façon conjointe, les problèmes de sécurité, d'utilisabilité et de résilience dans les systèmes d'information des entreprises et organisations.

3.1. Le positionnement du SST (système sociotechnique) dans la nouvelle industrie des services numériques, sous le regard de la sécurité et de l'expérience utilisateur

Comme il transparaît dans l'état de l'art sur les systèmes sociotechniques (paragraphe 2.1), les approches sociotechniques appréhenderaient davantage les subtilités des structures organisationnelles humaines, avec les multitudes de processus d'entreprise (*business process*) et les complexités des systèmes techniques géographiquement répartis à travers le monde. Nous présentons dans la suite notre représentation du système sociotechnique.

3.1.1. Le positionnement du SST (système sociotechnique) et ses composantes

Les concepts des systèmes et approches sociotechniques ont été succinctement présentés dans les sections précédentes. Il est communément reconnu que les systèmes développés en utilisant une approche sociotechnique sont plus susceptibles d'être acceptés par les utilisateurs finaux et de fournir des valeurs réelles aux parties prenantes. Nous notons des différences notables entre la modélisation des systèmes informatiques ou IT (*Information Technologies* – technologies de l'information) et celle des systèmes sociotechniques. Les approches d'ingénierie en termes d'interactions diffèrent pour les uns (systèmes IT) et pour les autres (systèmes sociotechniques). Nous proposons ci-dessous notre positionnement des systèmes sociotechniques au regard des systèmes d'information, en commençant par les systèmes informatiques. La figure 3 illustre notre représentation des systèmes sociotechniques.

1) La modélisation des systèmes informatiques IT se concentre sur la description technique des composantes des systèmes et les interactions entre elles, afin de fournir un certain service.

2) Les systèmes sociaux comprennent toutes les interactions humaines et coopération, sur la base des valeurs sociales et culturelles.

3) Les systèmes d'information comprennent toutes les interactions des utilisateurs avec les systèmes informatiques, en intégrant leurs organisations, implémentations et gestion.

4) Les systèmes sociotechniques fournissent une façon de comprendre toutes les interactions humaines avec les différents systèmes informatiques, leurs composants, ainsi que la coopération avec d'autres systèmes. Les systèmes sociotechniques abordent aussi les interactions entre les systèmes, les parties prenantes, leur organisation et l'ensemble de l'environnement social, à la fois les mondes physiques et le cyber.

Ces dimensions définissent l'information en termes d'interaction entre les acteurs, dans le cadre d'une dépendance sociale (les uns comptent sur les autres pour atteindre leurs objectifs respectifs) et/ou d'un échange d'information (les acteurs échangent des informations qu'ils jugent pertinentes, à certains moments, pour certaines raisons). De nombreux problèmes conflictuels pourraient résulter des interactions entre acteurs, et de la façon dont on accède aux informations. À titre d'exemple, les systèmes d'information des laboratoires d'analyses médicales, d'une part, sont ouverts aux partenaires et fournisseurs, et d'autre part, offrent des interfaces d'interactions avec les patients et clients. Les systèmes d'information des hôpitaux et des centres de santé sont dans le même contexte. Les questions du respect de la vie privée et de la confiance y sont cruciales ; elles doivent être traitées comme telles. En France, ces systèmes opèrent dans un cadre règlementaire, normatif et légal très strict. Avec ces contraintes, les systèmes doivent satisfaire les objectifs business des entreprises et organisations, tout en se prémunissant contre les attaques ; ce qui consiste un véritable défi pour la science.

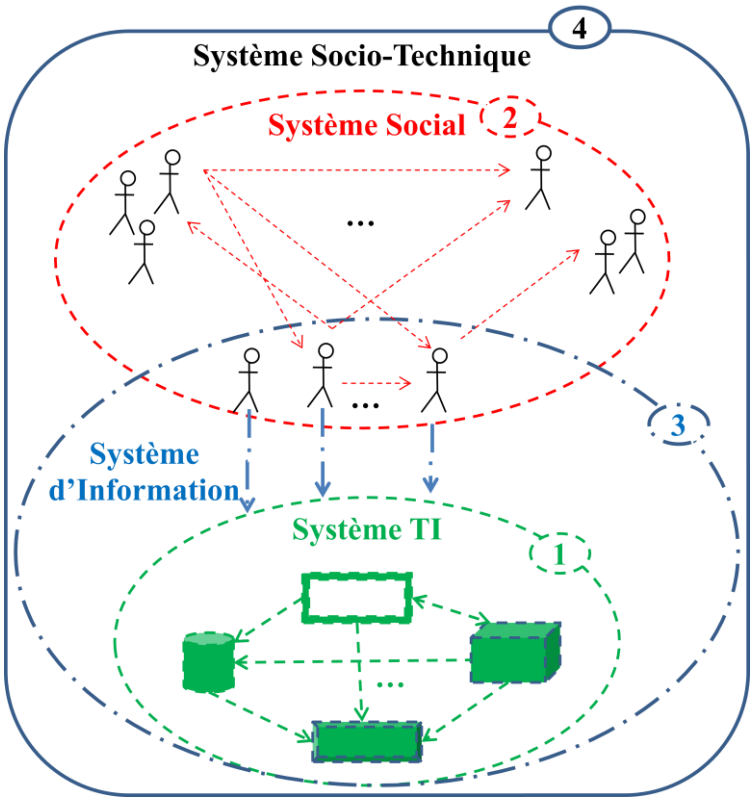


Figure 3. Représentation de système sociotechnique (Goudalo et Kolski, 2016)

Ce défi scientifique tel un nœud complexe se dénoue harmonieusement grâce à l'approche de systèmes sociotechniques. La contingence de complexités se décompose en sous-systèmes hétérogènes avec des acteurs et groupes d'acteurs ayant des compétences, préoccupations et enjeux respectifs, dans un ensemble d'interactions et de corrélations. La recherche de l'amélioration de l'expérience utilisateur pour chaque partie prenante pourrait constituer la préoccupation majeure dans la recherche de la sécurité optimale et pérenne.

3.1.2. L'expérience utilisateur dans les systèmes sociotechniques appréhendée sous l'angle de la sécurité

Dans cette section, nous appréhendons l'expérience utilisateur sous l'angle de la sécurité. Les systèmes sociotechniques traitent des données sensibles et fournissent des services à fortes valeurs. Dans le même temps, les utilisateurs adoptent un comportement ubiquitaire, ils changent très souvent leurs façons de consommer les services et on n'arrive pas toujours à appréhender les raisons de ces changements. Les fournisseurs de services s'évertuent à établir une véritable confiance et améliorer l'expérience utilisateur des consommateurs de services. Comme nous l'avons précisé dès l'introduction, cela s'avère nécessaire

pour le succès des systèmes sociotechniques, dans notre ère de l'industrie des services (IBM, 2014 ; KPMG, 2014 ; Umhoefer *et al.*, 2014).

L'approche des systèmes sociotechniques facilite l'identification et la formulation de l'expérience utilisateur pour chacune des parties prenantes, du point de vue de la sécurité et de la satisfaction de leurs objectifs respectifs. Une expérience utilisateur positive est généralement basée sur la commodité (épargne de temps, réduction du travail physique ou diminution de l'effort de réflexion), la confiance que le système sociotechnique « fonctionne correctement », et la perception de son utilité. Le concept de « fonctionner correctement » implique la confiance dans le résultat rendu et la confiance dans les données et étapes qui y ont contribué. Ce terme subjectif pour chaque partie prenante met en évidence les exigences de disponibilité, intégrité, sûreté, résilience et sécurité. Selon Sasse (2007), l'expérience utilisateur prend en compte tous les critères d'utilisabilité avec des facteurs additionnels (Cranor et Blase, 2015). Birge souligne le manque de recherche sur la conception de solutions techniques pour la communication et pour la technologie de l'information dans le domaine de « l'expérience utilisateur et la confiance » (*Trust and User eXperience* - TUX), (Birge, 2009). ISO 9241-210 définit l'expérience utilisateur comme « les perceptions et les réponses des personnes résultant de l'utilisation réelle et/ou de l'utilisation prévue d'un produit, système ou service ».

En synthèse, l'amélioration de l'expérience utilisateur fait recours aux améliorations simultanées et optimales de : la confiance, le respect de la vie privée, l'intégrité, la confidentialité des données, la disponibilité, la sûreté, la résilience, la sécurité et la véritable satisfaction de l'ensemble des parties prenantes (utilisateurs finaux, responsables, participants, organes de règlementations et organes de tutelle).

En conclusion, nous notons que l'objectif de la sécurité est d'évaluer, d'éliminer et de prévenir les erreurs, les fautes et les attaques. En cas d'occurrences de risque d'incident, l'objectif de la résilience est de tolérer et de surpasser les impacts, et de garantir des services en mode dégradé conformément les conditions des accords de service (SLA - *Service Layer Agreement*). Les objectifs de sécurité et de résilience doivent être assurés, tout en maintenant une expérience utilisateur positive. De même, nous précisons qu'une expérience utilisateur positive (bonne utilisabilité, IHM efficace, satisfaction de chacun) devrait promouvoir le succès de la sécurité et de la résilience, et *vice versa.*

Dans la section suivante, nous proposons de modéliser de façon conjointe la sécurité, la résilience et l'utilisabilité, dans le but d'améliorer l'expérience utilisateur (Goudalo *et al*., 2016).

3.2. Analyse conjointe et modèle conceptuel avancé du SST

Dans cette section, nous suggérons de présenter notre modèle conceptuel avancé qui modélise de façon conjointe la sécurité, la résilience et l'utilisabilité, dans le but d'améliorer l'expérience utilisateur de toutes les parties prenantes. Le modèle conceptuel résultant de l'analyse conjointe de la sécurité, de la résilience et de l'utilisabilité opère :

– Sur les trois principaux concepts d'actifs d'entreprise, de risques d'incidents et de solutions ;

– Et sur un système métrique homogène qui gère ces trois concepts du point de vue de la sécurité, de la résilience et de l'utilisabilité ensemble.

3.2.1. Eléments d'analyse conjointe de la sécurité, de la résilience et de l'utilisabilité

Dans toutes les normes de sécurité (locales et internationales), les trois critères invariants sont les mêmes : la confidentialité, l'intégrité et la disponibilité (ISO/IEC 2700x, 2010 ; EBIOS, 2016). À ces trois critères fondamentaux, sont rajoutés différents attributs et propriétés de sécurité tels que la preuve, la trace, la non-répudiation, l'identification, l'authentification que nous assemblons pour assurer le concept d'imputabilité (comme indiqué en section 2.2). Dans les systèmes socio-techniques, et notamment pour le domaine des systèmes médicaux (nous servant de cas d'étude, cf. §4), les attributs de respect de la vie privée et ceux de la confiance (*Trust*) se joignent indéniablement à la sécurité.

Comme indiqué dans l'état de l'art (section 2.4), le respect de la vie privée (*privacy*) fait appel à la fois la confidentialité et l'intégrité des informations. La présence de règles et politique de *privacy* et leur respect effectif renforcent la confiance des consommateurs.

Rousseau *et al.* (Rousseau *et al.*, 1998) définissent la confiance comme condition psychologique, y compris l'intention d'accepter la vulnérabilité basée sur les attentes positives des intentions ou des comportements d'une autre. La fiabilité définit la propriété d'un système qui exécute uniquement ce qui est nécessaire (à l'exception d'une interruption de l'environnement, les erreurs des utilisateurs ou des opérateurs humains et les attaques par des parties hostiles) et ne fait rien d'autre (Schneider, 1998).

La perte de l'imputabilité, la confidentialité, l'intégrité ou la disponibilité provoque un impact potentiel. Nous rappelons dans le tableau 1, la synthèse des principales solutions fournies par l'industrie et la recherche pour se prémunir contre ces pertes. Les solutions conventionnelles sont bien établies, mais il faut une autre maturité pour réussir vraiment à gérer au mieux les incidents tels que les attaques de sécurité. Dans la perspective de gérer tout type d'incidents, nous mettons en œuvre dans la section 3.3 une ingénierie avancée de la sécurité qui inclut la résilience et l'utilisabilité.

Tableau 1. Impacts de sécurité et solutions correspondantes

Objectifs de protection	Impacts potentiels	Solutions de sécurité
Imputabilité	Perte des traces, des pistes d'audit et de la transparence. Perte d'image de marque et pénalités pour la non-conformité règlementaire.	PKI, protection des traces, signature numérique, solution AAA.
Disponibilité	Perte d'exploitation directe et perte de part de marché	Application des patches sur les solutions des fournisseurs. Solutions de *backup*, of haute disponibilité, d'anti-virus, d'anti-spoofing, anti-DDOS.
Confidentialité	Divulgation d'informations sensibles, pénalités pour non-conformité, perte d'image et de part de marché.	Solution de chiffrement, zones de sécurité de confinement, PKI, VPN.
Intégrité	Corruption de données, inconsistance des services, perte d'image et de part de marché.	PKI, Signature numérique, authenticité des messages, authentification des messages et des services, solution d'anti-virus.

La norme ISO 9241-11 explique les bénéfices de la mesure de l'utilisabilité en termes de la performance des utilisateurs et de leur satisfaction (ISO 9241-11, 1998). Elle précise que la mesure de la performance et de la satisfaction des utilisateurs tient compte de : la façon dont les objectifs d'utilisation initialement prévus sont atteints ; la nature et la quantité de ressources qui doivent être déployées pour atteindre les objectifs visés ; et la façon dont l'utilisateur trouve lui-même acceptable l'utilisation du produit ou du service. Les produits et services utilisables peuvent être conçus en incorporant directement dans leurs spécifications (caractéristiques) les attributs connus au bénéfice des utilisateurs dans des contextes particuliers d'utilisation. Comme rappelé dans la section 2.4, Shackel (2009) évalue l'utilisabilité sur la base de trios critère : la performance dans la réalisation de la tâche, la satisfaction de l'utilisateur, et le coût engendré. Comme indiqué dans l'introduction, l'industrie des services numériques caractérise aujourd'hui le contexte d'utilisation. L'utilisabilité doit être assurée pour fournir des services (systèmes ou produits) qui sont utilisés dans des contextes personnels et professionnels, en fixe et en mobilité. Ces services numériques traitent les données sensibles et non sensibles, sur les appareils aussi bien personnels que professionnels. Les services fournis peuvent être utilisés ou consommés par un utilisateur final à travers l'interface utilisateur ergonomique ou bien ces services peuvent être utilisés ou invoqués en orchestrant un système de haut niveau ou d'un produit, telles les problématiques d'intégration d'applications ou de bus de services. Ainsi, l'ingénierie d'utilisabilité prend toute sa place dans le contexte de l'utilisation des services, produits ou systèmes à cette nouvelle époque de l'industrie des services numériques. L'ingénierie d'utilisabilité se réfère à un processus de conception qui traite, qualitativement, quantitativement et de façon prédictive, la facilité d'utilisation d'un produit, système ou service. À l'ère de l'industrie des services numériques, l'ingénierie d'utilisabilité considère aussi bien la réponse collective des groupes d'utilisateurs ou de leurs représentants que l'expérience de chaque utilisateur.

Tableau 2. Impacts d'utilisabilité et solutions correspondantes

Objectifs d'utilisabilité	Impacts potentiels	Solutions d'utilisabilité
Coût d'utilisation (dans la réalisation d'une tâche)	Source d'erreurs	Mesures d'adaptation (éducation, concision, compatibilité)
Efficacité de la réalisation des tâches	Source de contournement et/ou d'abandon	Recherche de compromis dans les préoccupations générales de tous les intervenants (test, ergonomie et durcissement)
Efficience de la réalisation des tâches	Source d'erreurs et/ou de failles de sécurité	Recherche de compromis dans les préoccupations générales de tous les intervenants (test, ergonomie et durcissement)
Satisfaction de l'utilisateur dans la réalisation des tâches	Source de rejet et/ou de recherché de contournement	Recherche d'amélioration de l'expérience utilisateur dès les phases amont

Les préoccupations d'utilisabilité sont appropriées dès les étapes initiales de l'élaboration de solutions ou de produits. Planifier l'utilisabilité comme partie intégrante de la conception et du développement de produits, implique l'identification systématique

des exigences en matière d'utilisabilité, y compris les mesures d'utilisabilité et les descriptions vérifiables du contexte d'utilisation. Afin de spécifier ou de mesurer l'utilisation, ISO 9241-11 recommande d'identifier les objectifs et de décomposer l'efficacité, l'efficience et la satisfaction et les composantes du contexte d'utilisation en sous-composants avec des attributs mesurables et vérifiables (ISO 9241-11, 1998). S'il n'est possible d'obtenir des mesures objectives de l'efficacité et de l'efficience, la norme ISO 9241-11 recommande l'utilisation de mesures subjectives basées sur la perception de l'utilisateur et qui peuvent fournir une indication de l'efficacité et de l'efficience.

À l'instar de ce qui est indiqué par Bevan *et al.* (Bevan *et al*., 2015), nous suggérons d'évaluer l'utilisabilité. En nous inspirant de ces éléments d'analyse et notamment de (Seffah *et al.*, 2006) et de (Vanderhaegen, 2010), nous proposons dans le tableau 2 une synthèse des objectifs d'utilisabilité, des risques potentiels et des solutions d'utilisabilité.

En psychologie sociale, dans l'industrie ou dans les affaires, la notion de résilience présente la capacité de « retour élastique » quelle que soit la nature de l'incident (Engle *et al*., 1996 ; Hamel et Välikangas, 2003 ; Hollnagel, 2006). Dans différents domaines, la notion d'incident représente les concepts tels que : l'adversité, les changements de risque, les forces de circonstance. Dans l'industrie des services numériques, les incidents sont liés à trois concepts : attaque de sécurité, problème technique, erreur (facteur humain). Au cours des dernières années, la communauté de la recherche et les professionnels mettent l'accent sur la résilience dans les différents domaines de l'industrie des services. Comme nous l'avons expliqué en section 2.5, c'est le cas des projets IRIS, RAMBO, ReSIST, et de nombreux travaux de la Commission européenne).

À partir des travaux de Laprie (2008) et de Luzeaux (Luzeaux, 2011), nous définissons la résilience comme un processus dynamique conférant la capacité à fournir des services de confiance justifiable, d'une part, en évitant les défaillances trop fréquentes ou trop sévères, et d'autre part, en assurant la persistance de la prestation de services fiables même en cas d'incident de tout type.

Nous basant sur les références de cette analyse et nous inspirant de (Laprie, 2008), nous proposons dans le tableau 3 une synthèse des objectifs de la résilience, les risques potentiels et les solutions.

Nous définissons la résilience, comme étant la capacité d'un système sociotechnique de continuer à remplir sa mission opérationnelle malgré les éventuelles contraintes, conditions difficiles, événements imprévus, et d'éviter des conséquences graves. Cette définition prend en compte le temps de réponse, le coût de la récupération et de la gravité des dégâts. Dans la plupart des cas, les incidents provoquant des menaces (conditions pouvant empêcher l'atteinte des objectifs) sur un système sociotechnique sont de trois principales sources (problème technique, erreur humaine, attaque ou malversation). La gravité des conséquences de ces conditions difficiles devrait être traitée et limitée par la résilience. Une façon de limiter avec succès la gravité des conséquences serait d'empêcher la survenance de tout incident entraînant des conditions difficiles ou des changements. Comment pourrions-nous protéger tous les actifs et composantes contre tout incident potentiel ?

Tableau 3. Techniques et moyens de garantie de la résilience

Objectifs de résilience	**Techniques dr résilience**	**Solutions de résilience**
Eviter les incidents inacceptables, du point de vue de la fréquence et du point de vue de la sévérité, en cas de changement	Évolutivité (adaptabilité)	Prévention, tolérance, traitement complet et prévision des incidents
Assurer la persistance de la prestation de services de confiance	Évaluation et vérification	Eradication et prévision des incidents
Tenir compte des changements des systèmes	Utilisabilité (pour les utilisateurs humains et système)	Prévention et tolérance des incidents
Tenir compte de la complexité des systèmes	Diversité (accroître la diversité de moyens et profiter des moyens alternatifs afin d'éviter le SPOF)	Tolérance des incidents

À l'ère actuelle de l'industrie de services numériques, chacun des trois types d'incidents prend une autre ampleur :

– Risque très élevé de problème technique (complexité des interconnexions, des équipements et dispositifs ; Pluralité des applications et des services provenant de sources différentes ; orchestration des processus d'affaires avec des activités disparates, organisations et transfrontalières, avec des impacts socio-économiques et géopolitiques accrus) ;

– Sophistication des attaques de sécurité (de très fortes motivations et des intérêts élevés pour des individus bien qualifiés et pour des groupes bien organisés qui commettent des attaques de forte intensité et des abus de toute sorte afin d'atteindre leurs objectifs ; disponibilité d'importantes ressources et kits pour les pirates et les attaquants ; volonté à ouvrir de plus en plus les différents systèmes) ;

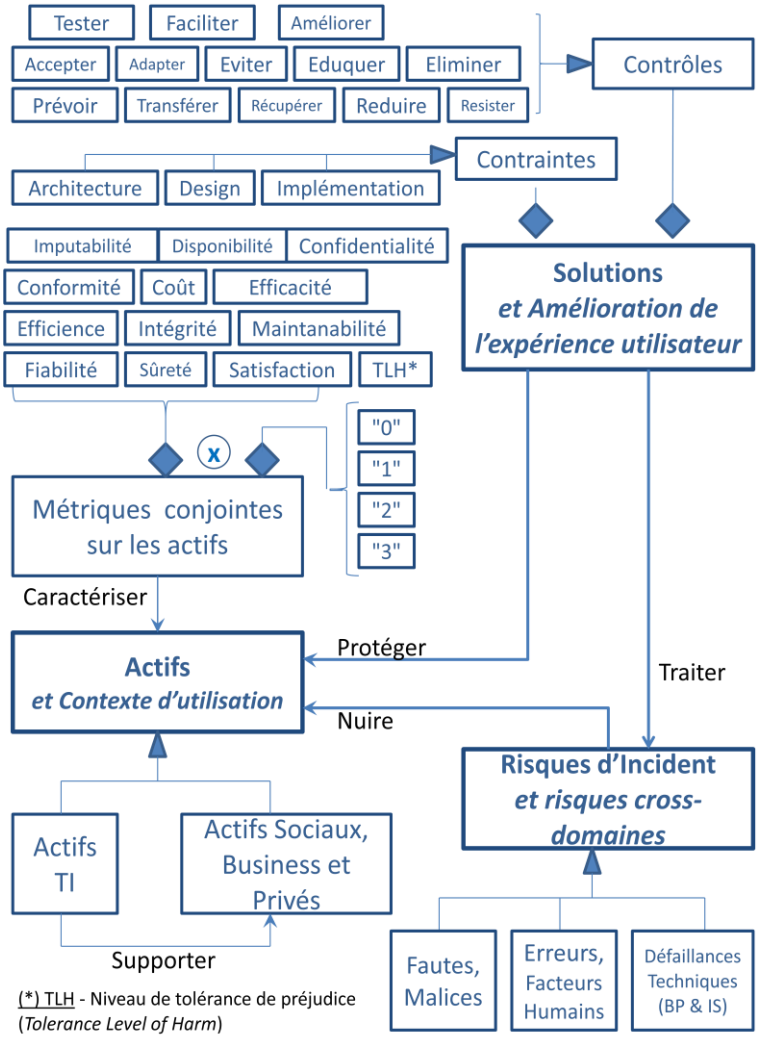
– Risques plus élevés concernant les facteurs humains et les erreurs associées (consumérisme des technologies de l'information ; BYOD ; de plus en plus de souhaits d'immédiateté ; de plus en plus d'extension sur la dépendance de la consommation de services numériques dans les activités personnelles, sociales, administratives et professionnelles, la disparition progressive des barrières entre les réseaux sociaux, systèmes privés, les réseaux d'entreprise).

Aujourd'hui, nous vivons déjà les systèmes ubiquitaires émergents qui ont été promis. Les systèmes continueront à être attaqués de plus en plus, les erreurs humaines et les problèmes techniques se produiront inévitablement dans les systèmes. Le processus de résilience présente un facteur qui est à la fois dynamique et intelligent, pour comprendre, anticiper et adapter à toute situation depuis les étapes en amont jusqu'aux étapes d'exploitation des produits, systèmes et services.

Afin d'améliorer l'expérience utilisateur de l'ensemble des parties prenantes des systèmes sociotechniques, nous avons effectué l'analyse conjointe de la sécurité, de la résilience, de l'utilisabilité et de leurs corrélations réciproques. Le modèle conceptuel qui en résulte est présenté dans la section suivante.

3.2.2. Modèle conceptuel résultant de l'analyse conjointe

La figure 4 présente le modèle conceptuel qui est le résultat de l'analyse conjointe de la sécurité, de l'utilisabilité, de la résilience et de leurs corrélations réciproques. Les éléments constitutifs du modèle conceptuel sont détaillés dans les sections suivantes.



Légende : significations des notations UML utilisées dans notre modèle conceptuel

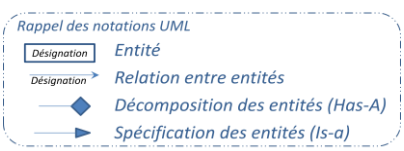


Figure 4. Modèle conceptuel de l'ingénierie conjointe

3.3. Concepts et Sémantiques

Nous suggérons de clarifier ci-après les principaux concepts et sémantiques utilisés dans ce modèle conceptuel.

3.3.1. Assets – les actifs

Les actifs sont nécessaires à la réalisation des objectifs de toutes les parties prenantes. Le concept d'actifs d'entreprise définit tous les biens de valeur de l'entreprise ou de l'organisation qui sont nécessaires pour la réalisation des objectifs de l'entreprise (Salehie *et al.*, 2012). Dans l'industrie des services numériques, un actif peut signifier des biens personnels comme des données médicales d'un patient ou un smartphone de l'utilisateur. Dans un sens général, les actifs sont des données, produits, services et/ou systèmes, et tout ce qui contribue à leur réalisations et utilisations correctes. Les actifs constituent les principaux éléments que la sécurité doit protéger. Les actifs sont pris en compte aussi bien que les interactions des utilisateurs et des contextes d'utilisation. Les actifs peuvent correspondre à des actifs sociaux, des actifs d'entreprise, des actifs personnels et des actifs de la vie privée. Il peut aussi s'agir d'actifs numériques (SI et SST) qui soutiennent d'autres types d'actifs. La figure 5 indique un aperçu du modèle conceptuel recentré sur les actifs.

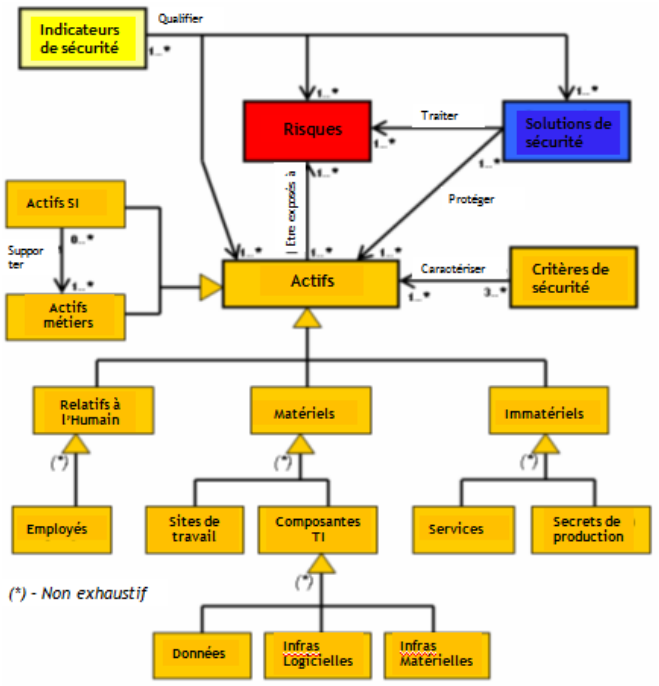


Figure 5. Modèle conceptuel des actifs

3.3.2. Incident risks – risques d'incident

Les risques d'incident mettent en péril les actifs. De par leurs natures, les risques sont définis en fautes et malversations (commises délibérément par des hackers et des personnes malveillantes), en erreurs dues à des facteurs humains (difficultés d'utilisation, inadvertances, sources d'ingénierie sociale) et en problèmes techniques (sur les processus d'entreprise, les procédures, les composants matériels, les composants logiciels et les composants matériels/logiciels – communément appelé *appliances* en anglais). Le risque d'incident dépend de l'exposition des actifs, de la probabilité de la survenance d'un événement et de l'impact des dommages réels sur ces actifs.

3.3.3. Solutions

Les solutions sont constituées de contraintes (contraintes de conception, d'architecture et de mise en œuvre) et de contrôles. Nous avons défini les contrôles de chacun des trois domaines (sécurité, utilisabilité et résilience) et des corrélations réciproques de domaines. Qu'elles consistent à éradiquer, atténuer, transférer ou les supporter, les solutions traitent les risques d'incidents et elles protègent les actifs, dans le but d'améliorer l'expérience utilisateur pour toutes les parties prenantes. Le concept de solutions de sécurité définit les mécanismes mis en œuvre (architecture, organisation, conception et/ou implémentation) pour protéger les biens contre les risques d'incidents auxquels ils sont exposés. Les contrôles qui accompagnent ces mécanismes sont entre autres : accepter, adapter, améliorer, éduquer, éliminer, éviter, faciliter, prévenir, recouvrer, etc.

3.4. Système de métriques homogènes

L'ingénierie doit être soutenue par des métriques et des processus d'évaluation appropriés. Les métriques bien définies favorisent la communication avec les parties prenantes, afin de prendre en compte les préoccupations de chacun. Notre ingénierie

conjointe opère sur des concepts qui sont mesurés et évalués quantitativement et qualitativement au sein d'un système métrique, afin d'en assurer une bonne gestion. Nous proposons quatre types de mesures : techniques (liées aux technologies et aux processus métier), organisationnelles, coûts et satisfaction. Nous exprimons les valeurs associées aux métriques en termes quantitatifs, qualitatifs ou semi-quantitatifs.

Sur le modèle conceptuel de l'analyse conjointe, les métriques caractérisent, de façon homogène, les trois principales entités. À l'instar du système métrique de suivi des indicateurs de la sécurité présenté dans la section 2.3, nous proposons ici un système métrique homogène, opérant sur trois axes : les actifs, les risques et les solutions. L'axe des risques d'incidents présente en soi la résultante des risques d'incidents de sécurité, risques d'incidents techniques et des risques d'incidents relatifs aux facteurs humains.

– Dans le cas des actifs, nous avons élaboré des métriques comme produits cartésiens d'attributs et de valeurs, tels des couples (attribut, valeur). Nous avons défini les attributs de chacun des trois domaines (sécurité, utilisabilité et résilience) et du domaine croisé. Les attributs identifiés sont les treize critères indiqués sur la figure 4 (imputabilité, disponibilité, confidentialité, conformité, coût, efficacité, efficience, intégrité, maintenabilité, fiabilité, sûreté, satisfaction et niveau de tolérance de préjudice ou TLH - *Tolerance Level of Harm* en anglais). Pour des raisons d'homogénéité et pour des raisons d'efficacité de manipulation, nous proposons de normaliser les valeurs en quatre catégories : « Non applicable – 0 », « Faible – 1 », « Élevé – 2 » et « Très élevé – 3 ».

– Sur les risques d'incidents, nous proposons de normaliser les métriques en quatre niveaux, en relation avec la probabilité d'occurrence, la surface d'exposition et la gravité de l'impact. Ces quatre niveaux de risques d'incidents sont les suivants : « Sans objet – 0 », « Faible – 1 », « Elevé – 2 » et « Très élevé – 3 ».

– Quant aux solutions, nous proposons quatre niveaux qui définissent leur efficacité en fonction des niveaux de risques d'incidents et des mesures sur les actifs concernés. Que les solutions soient des contrôles et/ou des contraintes, les quatre niveaux de solutions restent les mêmes : « Sans objet – 0 », « Inefficace – 1 », « Efficace – 2 » et « Très efficace – 3 ».

Pour l'analyse conjointe, nous avons défini un système métrique en trois dimensions (Actifs, Risques d'incidents et Solutions). Chaque axe est gradué en quatre niveaux homogènes (0, 1, 2, 3). Sur chaque axe, les niveaux sont des valeurs normalisées qui sont évaluées en fonction des heuristiques bien connues. Le développement approfondi de ces heuristiques fait l'objet des actes (activités et/ou tâches) de l'ingénierie avancée de la sécurité, plus détaillés dans la section suivante ; nous proposons d'y présenter notre approche d'ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience dans les systèmes sociotechniques.

3.5. Vers les actes de l'ingénierie conjointe

Encore aujourd'hui, nous rencontrons trop souvent des systèmes de sécurité qui ne sont pas faciles d'utilisation et qui ne présentent pas non plus une appétence naturelle aux parties prenantes (Hansen *et al.*, 2011). Les principaux utilisateurs qui devraient utiliser les systèmes sont amenés à chercher des alternatives de contournement ou à boycotter les solutions trop contraignantes. Ce comportement génère des failles de sécurité et/ou engendre des manques à gagner. Il s'agit donc de substituer les approches classiques de construction de systèmes de sécurité par des approches d'amélioration de l'expérience utilisateur pour l'ensemble des parties prenantes du système sociotechnique.

Dans cette section, nous proposons d'introduire les actes de sécurité avancée de notre approche d'amélioration de l'expérience utilisateur pour l'ensemble des parties prenantes du système sociotechnique, sur la base des patrons de conception. Cette approche sociotechnique opère sur l'interdépendance entre la sécurité, l'utilisabilité et la résilience.

Nous suggérons ici les principales activités et tâches qui feront l'objet d'un développement futur de l'ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience, intégrant leurs corrélations réciproques : définir le SST (système socio-technique) ; définir les interactions d'utilisation du SST ; évaluer les actifs et définir les objectifs sur les actifs ; identifier et analyser les risques d'utilisabilité ; identifier et analyser les risques de sécurité ; mettre en évidence les risques d'incidents de problèmes techniques (panne, erreur de conception, d'incohérence procédurale, etc.) ; identifier et analyser les risques cross-domaines (du point de la sécurité, de l'utilisabilité, de la résilience et de leurs corrélations réciproques) ; réaliser la cartographie des risques globaux, du point de vue de la résilience ; définir des solutions basées sur l'amélioration de l'expérience utilisateur qui répondent aux préoccupations de toutes les parties prenantes ; valider les solutions, dans l'optique de la résilience. Nous regroupons ces activités et tâches en trois étapes qui constituent la synoptique de notre approche d'ingénierie avancée. La figure 6 illustre le processus sous-jacent.

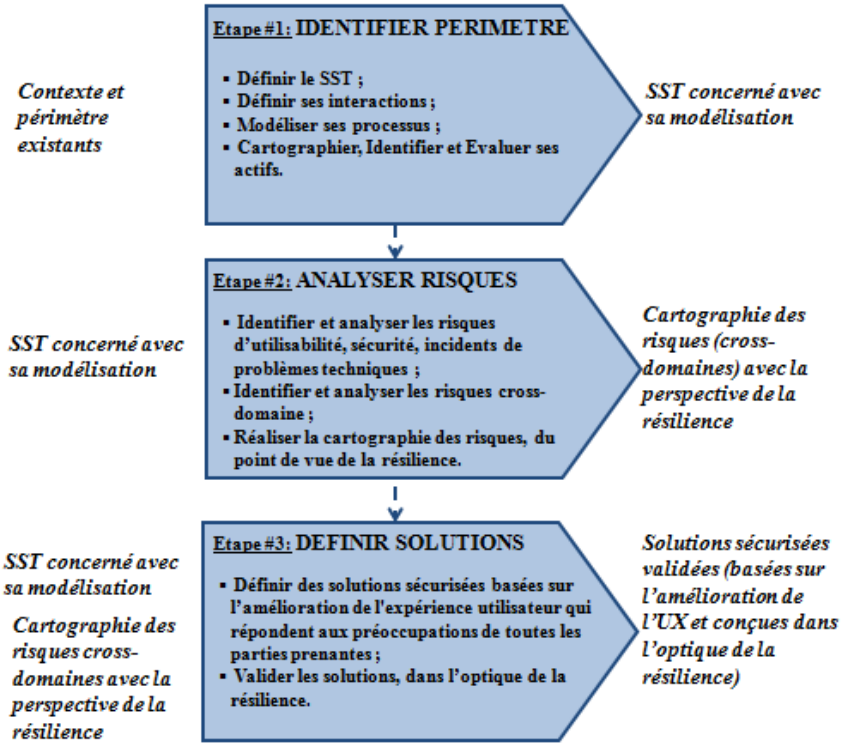


Figure 6. Approche d'ingénierie avancée de la sécurité, basée sur l'amélioration de l'expérience utilisateur (Goudalo et Kolski, 2016)

Dans le cadre de notre ingénierie conjointe, nous utilisons des patterns pour décrire les problèmes et les solutions adaptées aux problèmes de sécurité, d'utilisabilité et/ou de résilience. Les travaux de design patterns sont rappelés à la fin de l'état de l'art, fin de la section 2.6.

Ce processus est constitué des trois étapes suivantes :

– Étape #1 – Identifier le périmètre du système sociotechnique concerné. Cette étape consiste à circonscrire le périmètre du système sociotechnique, incluant l'ensemble de l'environnement social et les différents acteurs. Nous intégrons leurs interactions dans les mondes cyber et physiques, en utilisant BPMN (*Business Process Modelling Notation*) pour modéliser les processus, les activités (sous-processus) et les tâches réalisées par chaque acteur impliqué dans les processus. Nous effectuons la description détaillée des interactions entre les composantes des systèmes d'informations, au moyen des diagrammes UML (les *use cases* notamment). Les liens entre les diagrammes BPMN et UML (*misuse cases*) sont décrits à cette étape (Piètre-Cambacèdés, 2010). Grâce à cet exercice, tous les actifs du système sociotechnique doivent être mis en évidence et identifiés.

Nous évaluons les actifs et définissons les objectifs d'entreprise sur les actifs suivant la perspective conjointe de la sécurité, de l'utilisabilité et de la résilience.

– Étape #2 – Effectuer l'analyse de risques cross-domaines du système sociotechnique. Cette étape produit la liste des problèmes potentiels. Nous recourrons à plusieurs méthodes pour analyser la description du système socioéconomique effectuée à l'étape précédente. De ces méthodes, nous notons entre autres : cognitive *walkthrough* (Wharton *et al.*, 1994 ; Mahatody *et al.*, 2010) ; les réseaux de Petri marqués ; les méthodes d'analyse de risques classique et cross-domaines (DCSSI, 2009). Les risques incluent, d'une part, les menaces de sécurité (comme les attaques, les failles, les fraudes, les chantages, les usurpations d'identité), et d'autre part, les défaillances techniques et problèmes d'utilisabilité. Ils conduisent au dysfonctionnement, au déni de service ou à la destruction de certaines parties du système sociotechnique.

L'étude se concentre sur les problèmes, leurs origines et leurs raisons ainsi que les conséquences de ne pas améliorer les contextes qui engendrent des irritants. Cette étude met en évidence les relations de proximité et d'interdépendance entre l'IHM, le respect de la vie privée et la sécurité. Notre approche se distingue sur deux points importants : d'une part, elle utilise une approche de risque cross-domaines et d'autre part, elle se recentre sur les facteurs humains. Nous documentons les problèmes en utilisant notamment une approche de description, désignée par « Storytelling », qualifiée aussi de narration descriptive et détaillée (Kumar *et al.*, 2006 ; Rao, 2006). Cette approche de description détaille l'expérience utilisateur, ses échecs et ses points d'amélioration possible pour chaque partie concernée, d'autres approches existent dans la littérature (Pavel *et al.*, 2013). La documentation d'un problème repose sur l'apprentissage et la rétro inspection opérationnelle sur n'importe quel autre type d'incidents qui auraient un rapport avec ses risques.

– Etape #3 – Définir les solutions adéquates. Dans cette troisième et dernière étape, nous avons recours à l'expérience utilisateur afin de définir les solutions adéquates aux risques soulevés lors de la deuxième étape. En fait, nous cherchons la meilleure amélioration de l'expérience utilisateur qui sous-tend les points identifiés. La question importante abordée ici est de savoir ce qui rend une solution considérée comme étant la meilleure – ou la pire – conception, dans une perspective de sécurité utilisable. Ainsi, il faut détecter toutes conceptions de solutions non adaptées et les corriger. De préférence ce contrôle et cette

correction devraient être effectués avant qu'une partie prenante ne manifeste son mécontentement, avant que les utilisateurs ne cherchent des chemins alternatifs ou ne boycottent ce qui est mis en œuvre.

Nous notons quatre types de traitement des risques : acceptation des risques, évitement des risques, réduction des risques et de transfert des risques (Hedrick, 2007 ; Yeo *et al.*, 2014). Suite à la décision sur le type de traitement des risques, nous devons évaluer les risques résiduels. Les risques résiduels sont appréciés par rapport aux objectifs de l'organisation. Les contrôles appliqués dans les solutions de sécurité sont de quatre natures : corrective, détective, dissuasive et préventive. Une bonne solution de sécurité doit veiller à l'adéquation entre les trois composantes du triplet (nature du contrôle, le type de traitement, les objectifs de sécurité). Nous basons les actions de cette étape sur diverses expériences de recherches universitaires et industrielles. Dans des travaux précédents, nous avons défini sept actes de sécurité constituant l'ingénierie de la sécurité de l'information (Goudalo, 2011). Parmi les nombreux chercheurs qui ont travaillé sur la conception de sécurité utilisable, Kai-Ping Yee (2002) a proposé une liste de lignes directrices pour résoudre certains problèmes spécifiques dans la conception de sécurité utilisable : chemin de moindre résistance, l'autorisation active, révocabilité, la visibilité, la conscience de soi, chemin de confiance, l'expressivité, les limites pertinentes, identifiabilité et prévoyance.

Cette étape consiste également à documenter chaque *design pattern* en utilisant le formalisme suivant :

– Nom du design pattern ;

– Description du problème (ou classe de problèmes) ;

– Description de la solution ;

– Conséquences de l'application de la solution de conception ;

– Validité de la solution. Qualitativement, chaque pattern devrait améliorer l'expérience utilisateur, par exemple selon l'une des orientations données par Kai-Ping Yee. Quantitativement, les patterns devraient améliorer de façon mesurable, d'une part le compromis entre la facilité d'utilisation et de sécurité, d'autre part l'expérience utilisateur.

Les design patterns des systèmes sociotechniques résilients intégreront désormais les préoccupations conjointes d'utilisabilité et de sécurité, afin de concevoir des systèmes de sécurité à la fois simples, efficaces et utilisables. Ces design patterns complèteront également d'autres travaux traitant la résilience intégrée de la sécurité et de la sûreté des systèmes (Ruault *et al.*, 2016).

4. Étude de cas

4.1. Définition du périmètre de l'étude de cas

L'étude de cas est liée au SI du laboratoire médical Fi MedLab qui réalise des analyses de sang, en reprenant celle décrite dans (Goudalo et Kolski, 2016). La norme internationale en usage aujourd'hui pour l'accréditation des laboratoires médicaux est ISO 15189 – « Laboratoires de biologie médicale – exigences particulières en matière de qualité et de compétence ». Le SI permet de collecter de données sur les patients, gérer les dossiers d'analyses et traiter l'interprétation des résultats des analyses. Les risques de sécurité de l'information et de la vie privée augmentent avec la croissance rapide du nombre et des catégories de personnes qui ont un rôle légitime d'accéder, d'utiliser et de transformer (modifier) les informations et les dossiers médicaux. Souvent, il existe une tension à concilier la sécurité, les contrôles de confidentialité, les besoins d'utilisabilité (exigences d'urgence et du confort d'utilisation) et la garantie de la persistance de la prestation de services de confiance, dans ce cadre règlementaire exigeant. Le laboratoire d'analyse médical illustre réellement un SST qui implique les patients, les opérateurs internes et externes, des laboratoires ou des partenaires médicaux, fournisseurs d'équipements médicaux, les organismes de réglementation, ainsi que les services informatiques et les fournisseurs d'applications et de Datacenters. Ce SST comprend divers processus d'entreprise et des activités opérationnelles.

4.2. Artéfacts produits par l'ingénierie conjointe

Certains opérateurs ont accès à une catégorie d'informations, mais pas à d'autres, suivant l'authentification de l'utilisateur et ses autorisations. Ainsi, au sein des organisations, doivent être correctement définis des groupes d'utilisateurs ayant des rôles, des responsabilités et des habilitations. Le tableau 1 présente trois actifs avec leur métrique :

– Le dossier du patient (l'opérateur administratif saisit des informations dans le SST, pour la création et/ou la mise à jour du dossier du patient) ;

– Les résultats d'analyses médicales (après analyses médicales et validation, les résultats sont communiqués de trois façons – envoi au médecin, envoi au patient par courrier électronique, mise à disposition sur le site sécurisé du laboratoire d'analyses médicales) ;

– Appareils médicaux (Le gestionnaire médical initialise et paramètre les appareils médicaux pour réaliser des analyses médicales).

Les risques d'incidents sont dus à l'utilisabilité, la sécurité, les problèmes techniques et les interdépendances entre eux. Les utilisateurs ont besoin d'accéder aux informations (services, données, produits et systèmes), en fonction de leur rôle et leurs tâches. Mais la modalité d'accès à l'information dépend du contexte de la tâche (accès interne/externe, urgence temporelle, niveau d'anxiété, etc.), la qualité du dispositif de sécurité, son adéquation à la tâche et au contexte. Pour illustration, nous avons décrit

des scénarios de trois risques d'incidents relatifs à l'expérience utilisateur et avons élaboré des solutions appropriées aux trois scénarios de risques d'incidents et aux actifs sélectionnés.

Nous avons élaboré une dizaine de tableaux qui synthétisent : les trois processus d'entreprise (*business processes*) et les activités opérationnelles ; les trois actifs sélectionnés et leurs métriques ; l'analyse conjointe sur les scénarios de risque par rapport aux actifs ; les solutions adaptées. Ils ne sont pas tous fournis ici par manque de place.

4.2.1. Étape #1 – Identifier le périmètre du système sociotechnique concerné

Le laboratoire d'analyse médical Fi MedLab illustre réellement un système sociotechnique qui implique les patients, les opérateurs internes et externes, des laboratoires partenaires médicaux, des fournisseurs d'équipements médicaux, les organismes de réglementation, ainsi que les services informatiques et les fournisseurs d'applications et de Datacenters. Ce système sociotechnique comprend divers processus d'entreprise (*business processes* ou processus métier) et des activités opérationnelles.

Nous regroupons les processus métier de Fi MedLab en trois catégories : les processus pré-analytiques, analytiques et post-analytiques. Le tableau 4 synthétise trois processus métier de Fi MedLab et leurs activités.

Tableau 4. Trois business process de FI MEDLAB

1	**Préparer les analyses médicales**
1.1.	*Gérer le dossier patient (Créer, Mettre à jour ou Archiver) (voir tableau 7)*
1.2.	Enregistrer une demande d'analyses médicales
1.3.	Payer la demande d'analyses médicales
1.4.	Prélever et échantillonner le sang du patient
1.5.	Recevoir des échantillons de sang prélevés dans n'importe quel service partenaire
1.6-	Traiter et stocker les échantillons de sang avant analyses
2.	**Réaliser les analyses médicales**
2.1.	*Mettre en marche et calibrer les appareils (voir tableau 7)*
2.2.	Passer une série de tests d'analyses médicales
2.3.	Valider une série de tests d'analyses médicales
2.4.	Effectuer la maintenance des équipements
3.	**Conclure les tests d'analyses médicales**
3.1.	Interpréter la validation biologique des tests
3.2.	Archiver les échantillons de sang
3.3.	*Communiquer les résultats (voir Tableau 7)*
3.4.	Archiver les résultats

La sensibilité de l'information est déterminée lors de la cotation des actifs. Le tableau 5 présente trois actifs concernés par les activités opérationnelles avec leurs cotations respectives : dossier du patient, résultats d'analyses médicales, appareils médicaux.

Tableau 5. Trois actifs sélectionnés et leurs métriques

Attributs des actifs	Dossier patient	Résultat d'analyse médicale	Appareils médicaux
Imputabilité	"2"	"2"	"3"
Disponibilité	"2"	"2"	"3"
Confidentialité	"2"	"2"	"2"
Conformité	"2"	"2"	"2"
Coût d'utilisation	"2"	"2"	"2"
Efficacité	"2"	"2"	"2"
Efficience	"2"	"2"	"2"
Intégrité	"2"	"2"	"3"
Maintenabilité	"2"	"2"	"2"
Fiabilité	"2"	"2"	"2"
Sûreté	"2"	"2"	"2"
Satisfaction	"2"	"2"	"2"
TLH (niveau de tolérance des préjudices - *Tolerance Level of Harm*)	"2"	"2"	"3"

La figure 7 montre un modèle simplifié de ces processus métier en utilisant BPMN (*Business Process Modeling Notation*). Nous y mettons en évidence les activités (sous-processus) que nous développons dans l'analyse des risques.

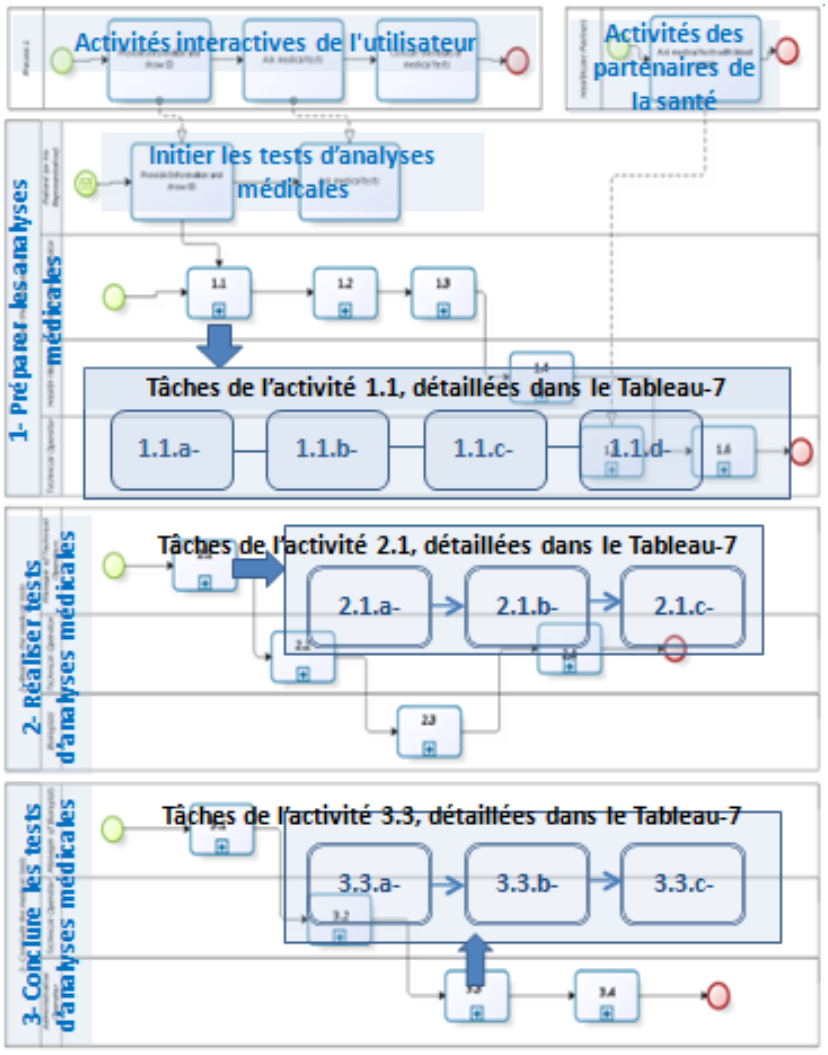


Figure 7. Modélisation des Business Processes (mise en évidence des tâches ayant des problèmes potentiels)

4.2.2. Étape #2 – Effectuer l'analyse de risques cross-domaines du système sociotechnique

Nous synthétisons les trois risques d'incidents et leurs métriques dans le tableau 6.

Le tableau 7 présente la description détaillée de trois des sous-processus indiqués dans le tableau 4 (processus métier de FI Medlab). Nous utilisons cette description pour illustrer comment nous effectuons l'analyse des risques de sécurité, d'utilisabilité et de résilience dans le système sociotechnique de FI MedLab.

Tableau 6. Risques d'incident et leurs métriques

Caractéristiques	**T1**	**T2**	**T3**
Risques d'utilisabilité	"2"	"3"	"0"
Risques de sécurité	"1"	"2"	"0"
Défaillances techniques	"1"	"0"	"2"
Impacts sur l'actif « Dossier patient »	"2"	"0"	"0"
Impacts sur l'actif « Résultat d'analyse médicale »	"2"	"2"	"1"
Impacts sur l'actif « Appareils médicaux »	"0"	"3"	"0"
Métriques sur les risques	"2"	"3"	"1"
Observation	Des solutions doivent être adressées pour les trios scenarios		

Tableau 7. Trois activités détaillées

	Gérer le dossier patient (créer, mettre à jour ou archiver)
1.1	*En entrée : Pièce d'identité du patient ou de son représentant légal* *En sortie : Dossier patient (créé, mis à jour ou archivé)* *Tâches:*
1.1.a	Le patient ou son représentant légal renseigne les informations nécessaires à l'opérateur administrative de FI MedLab, y compris l'adresse d'envoi des résultats d'analyses médicales.
1.1.b	L'opérateur administratif de FI MedLab entre les informations dans le système socio-technique de FI MedLab, pour la création et/ou mise à jour du dossier patient.
1.1.c	Un événement planifié déclenche et avertit l'opérateur administratif d'archiver certains dossiers patients.
1.1.d	L'opérateur administratif effectue le traitement administratif adéquat et archive les dossiers patients correspondants.
	Mettre en marche et calibrer les appareils médicaux
2.1	*En entrée : Présence du responsable des opérateurs techniques.* *En sortie : Appareils mis en marche et calibrer pour procéder aux tests médicaux.* *Tâches :*
2.1.a	Le responsable s'authentifie, avec une exigence d'authentification biométrique, basée sur la rétine et sur le scan de la pièce d'identité.
2.1.b	Le responsable authentifié active et calibre les appareils.
2.1.c	Les appareils s'initialisent et chargent les signatures des responsables biologistes qui interprètent la validation biologique des résultats d'analyses médicales.
	Communiquer les résultats
3.3	*En entrée : Résultats validés et interprétés.* *En sortie : Résultats communiqués, par 3 canaux (envoyés au médecin concerné, envoyé au patient par mail, rendus disponibles sur le site web sécurisé de FI MeddLab.* *Tâches :*
3.3.a	L'opérateur administratif envoie les résultats au médecin concerné.
3.3.b	L'opérateur administratif envoie les résultats au patient, par mail.
3.3.c	L'opérateur administratif upload les résultats sur le site web sécurisé de FI MedLab.

4.2.3. Étape #3 – Définir les solutions adéquates

Les trois scénarios de risque d'incident décrivent la notion d'expérience utilisateur ; chacun d'eux met en évidence un problème d'utilisabilité, de la résilience, de la sécurité ou du respect de la vie privée.

Le scénario T1, en occurrence, détaille un problème typique du respect de la vie privée et de la confidentialité, en raison de l'incompréhension de l'utilisation faite des informations demandées à l'utilisateur (le patient ou responsable). Le tableau 8 présente les solutions élucidées pour ce problème.

Tableau 8. Solution de Design Pattern pour le problème T1

Nom	Prise de conscience et vigilance
Description du problème	Méconnaissance ou connaissance insuffisante de l'usage qui devrait être effectué avec les renseignements d'adresse fournis par le patient ou son représentant.
Description de la solution Design Pattern	Fournir aux utilisateurs l'explication, la compréhension et l'analyse de tous les renseignements collectés dans le système socio-technique et qui les concernent. Cela nécessitera un soutien et une pédagogie individualisés. Sur le plan opérationnel, nous suggérons de mettre des prospectus et des terminaux d'information (interactifs et captifs) dans le hall d'entrée de FI MedLab. Une solution alternative devrait être « d'envoyer tous les courriers des résultats via paquet postal recommandé AR ».
Conséquences	Une autre solution plus technique consiste à : – ajouter un label « renseignements personnels confidentiels » dans l'objet du courriel et une note rappelant la loi dans le texte du message, afin d'alerter l'assistant et « d'accroître » sa vigilance ; – utiliser du courriel sécurisé et chiffré (le code de déchiffrement sera le même que le code d'accès au site web sécurisé de consultation des résultats).

5. Discussion

De nos jours, la sécurité ne doit pas être traitée au détriment de l'utilisabilité. Plusieurs études montrent comment prendre en compte l'utilisabilité dans la mise en œuvre des fonctions de sécurité spécifiques. Divers outils ont été proposés pour fournir des interfaces utilisateur plus utilisables et ergonomiques pour une fonction spécifique de sécurité, ou pour rendre des technologies de sécurité plus faciles d'utilisation. Des approches ont été proposées pour concevoir et assurer des compromis entre la sécurité et l'utilisabilité (Yee, 2002). Cependant, il existe encore un besoin crucial d'une approche globale de la sécurité, une approche d'ingénierie de la sécurité qui peut prendre en compte l'utilisabilité. Le juste équilibre entre la sécurité et l'utilisabilité favorise la confiance des utilisateurs et améliore l'expérience utilisateur. Dans le cadre des nouvelles menaces auxquelles les organisations doivent faire face, la résilience est une préoccupation majeure afin d'éviter un risque d'incident majeur et de pouvoir restaurer un état sûr après un accident ou une faute intentionnelle (Laprie, 2008 ; ReSIST, 2016). En cas de survenance de risque d'incident, l'objectif de résilience est de tolérer et de surpasser les impacts, afin de garantir des services en mode dégradé selon les conditions contractuelles de niveau de services (SLA – *Service Layer Agreements*). Dans ce travail, nous avons proposé une approche d'ingénierie avancée qui traite de façon conjointe la sécurité, l'utilisabilité et la résilience dans les systèmes d'information d'entreprise.

Notre proposition d'ingénierie avancée n'a pas pour objectif de remplacer les méthodes ISRAM (*Information Security Risk Assessment Methods* - Méthodes d'évaluation et de gestion de risques de sécurité de l'information) existantes (Behnia, 2012). Bien au contraire, nous les utilisons et les étendons, notamment :

– L'identification d'actifs et de cotation des actifs se produisent dans la perspective axée sur les enjeux d'entreprise (cf. Étape # 1 - Identifier le périmètre du système sociotechnique), comme les processus métier, des principaux services métier. Son premier avantage est l'identification des réelles ressources critiques clés (par graphe de dépendance). Son deuxième avantage est de faciliter l'adhésion des dirigeants d'entreprise aux préoccupations de sécurité.

– L'analyse des risques se produit à travers l'analyse cross-domaines ; et elle utilise des approches d'évaluation qualitatives et quantitatives. Afin de mettre en évidence les risques potentiels d'incidents, nous détaillons les activités métiers et opérationnelles ; cela se rapproche à la méthode des scénarios. L'un de ses avantages est la capacité à se recentrer sur les aspects les plus importants, à chaque fois, en fonction du contexte. Dans ce travail, nous ne nous attardons pas sur les formules théoriques de calcul des probabilités d'occurrence des risques ou les notions de facteur d'exposition, l'espérance de perte annualisée ou taux annualisé des événements.

– L'élucidation de solutions est guidée par la recherche de l'amélioration optimale de l'expérience utilisateur inhérente à tous les scénarios de risques identifiés préalablement (en Étape # 2 – Analyser de risques cross-domaines). Le formalisme de modèles de conception (design patterns) inspire une combinaison de compétences et d'entrainements. L'amélioration de l'expérience

utilisateur doit être continue, pour réduire le risque (atténuation des dommages, l'inhibition de propagations, diminution des occurrences, correction des vulnérabilités, la sensibilisation des utilisateurs, l'amélioration des interfaces utilisateur).

La valeur de l'information aux organisations croît de façon spectaculaire. Cependant, pour certains types d'informations, comme les dossiers médicaux, où une seule corruption des données pourrait engendrer une question de vie ou de mort, la valeur des données sécurisées ne peut pas être mesurée en termes de valeur monétaire tout simplement. En conséquence, il est nécessaire de mettre au point et de partager une approche d'ingénierie avancée qui traite la sécurité, l'utilisabilité et la résilience, de façon conjointe.

6. Conclusion et perspectives

Les services, produits et systèmes numériques ont déjà envahi tous les domaines socio-économiques de notre vie quotidienne. Ils couvrent à la fois les activités de divertissement et les activités sensibles ayant un impact sur la vie humaine ou sur des activités administratives, financières et médicales, très sensibles. Et au même moment, les pirates deviennent plus structurés, mieux formés et équipés. Leurs motivations ont changé de nature. Dans ce contexte, inévitablement les systèmes seront attaqués, les erreurs humaines et les problèmes techniques surviendront dans les systèmes. La sécurité est l'une des questions les plus importantes pour les réalisations des promesses de l'industrie des services, pour le présent et pour les générations à venir. Une autre forme d'ingénierie de sécurité avancée doit être conçue pour faire face à ce nouveau dilemme (entre les promesses de l'industrie des services et l'inévitabilité des risques informatiques). En France, nous distinguons les OIV, Opérateurs d'Importance Vitale dont la cyber sécurité rentre dans le dispositif de la loi de programmation militaire (ANSSI, 2016).

Dans ce travail, nous nous sommes proposé de traiter la sécurité de l'information au moyen d'une méthode d'ingénierie qui réunit toutes les parties prenantes de l'organisation. Cette méthode d'ingénierie est une méthode innovante et fonctionne sur les processus d'entreprise (processus métier, *business process*), leur décomposition et variantes opérationnelles, afin de : découvrir les principaux actifs dans leur contexte d'utilisation, identifier la valeur réelle et la sensibilité des actifs avec leurs interdépendances, identifier et évaluer les incidents de risque de sécurité, d'utilisabilité, de défaillances techniques et de résilience. L'approche proposée traite de façon conjointe les problèmes de sécurité, d'utilisabilité et de résilience. Les solutions élucidées sont basées sur les design patterns (modèles de conception) pour améliorer de façon continue l'expérience utilisateur pour l'ensemble des parties prenantes. Les risques ne sont pas traités de manière isolée, mais dans leurs corrélations. En effet, nous avons pris en compte la dépendance fonctionnelle des actifs, l'évaluation des risques inter-domaines et les corrélations entre la sécurité, l'utilisabilité et la résilience. Le facteur humain et l'expérience utilisateur sont des aspects essentiels pris en compte dans notre ingénierie avancée de la sécurité des systèmes d'information d'entreprises. Notre ingénierie avancée de la sécurité apporte des réponses concrètes au manque d'entrainement et d'expérience en matière de sécurité aujourd'hui, au manque de sécurité en termes de procédures, opérations et stratégies d'entreprise et aux difficultés de communication sur les problématiques de la sécurité.

Dans cet article, nous avons utilisé le cas des laboratoires d'analyses médicales pour illustrer notre propos. Le domaine de la santé est considéré comme un domaine particulièrement sensible. Afin d'éviter toute poursuite liée à la divulgation d'information, nous avons présenté un exemple générique, mais représentatif, dont l'objectif est d'illustrer le cadre d'ingénierie avancée proposé. Dans nos futurs travaux, nous envisageons de mettre en place des partenariats afin de travailler sur des cas réels d'entreprises avec des informations d'entreprises autorisées à des fins de recherches scientifiques.

Nos futurs travaux porteront sur le développement des actes de sécurité avancés dans le cadre d'un véritable projet de partenariat de recherche industrie-université. Telle une invitation à une extension d'Ebios au sein de ce projet, il s'agira d'analyser plus en détail notre approche spécifiquement par rapport à Ebios qui est la méthode communément utilisée en France.

En termes de perspective, nous suggérons également d'étendre le principe de système métrique des indicateurs de suivi de la sécurité indiqué dans l'état de l'art, pour la sécurité avancée dans le cadre des futurs travaux de notre ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience. Nous suggérons également d'étudier le noyau d'un outil de calcul de risques existant sur le marché et de l'étendre aux risques cross-domaines de la sécurité, de l'utilisabilité et de la résilience, afin de mettre en évidence la normalisation des valeurs qui concourt au système de métriques homogènes.

Remerciements

Les auteurs remercient très cordialement le Jean-René Ruault et le Professeur Ahmed Seffah, pour les échanges fructueux en lien avec différentes parties de cet article. Les auteurs remercient les relecteurs anonymes pour leurs observations et leurs conseils ayant permis d'enrichir cet article et d'améliorer sa qualité.

Bibliographie

Alexander C., Ishikawa S., Silverstein M. (1977). *A Pattern Language: Towns, Buildings, Construction*, Oxford University Press, New York.

ANSSI (2014). Publication des premiers arrêtés sectoriels relatifs à la sécurité des systèmes d'information des opérateurs d'importance vitale, Internet resources https://www.ssi.gouv.fr/publication/publication-des-premiers-arretes-sectoriels-relatifs-a-la-securite-des-systemes-dinformation-des-operateurs-dimportance-vitale/ [Dernier accès en novembre 2016].

Behnia A., Rashid R., Chaudhry J. A. (2012). Survey of information security risk analysis methods. *Smart Computing Review*,vol. 2, n° 1, p. 79-94.

Bell D. E., La Padula L. J. (1975). Secure Computer Systems: Unified Exposition and Multics Interpretation. Technical Report ESD-TR-75-306, MTR-2997, MITRE, Bedford, Mass.

Bernardez B., Duran A., Genero M. (2005). Metrics for use cases: a Survey of Current Proposals. *Metrics for Software Conceptual Models*, M. Genero, M. Piattini, C. Colero Editors. Imperial College Press, p. 59-98.

Bevan N., Carter J., Harker S. (2015). ISO 9241-11 revised: What have we learnt about usability since 1998? *Human-Computer Interaction, Part 1,* M. Kurosu (Ed.): HCII 2015, LNCS 9169, p. 143-151.

Birge C. (2009). Enhancing Research into Usable Privacy and Security, *SIGDOC'09: Proceedings of the 27th ACM International conference on Design of communication*, October 2009.

Blakley B., Heath C., & members of The Open Group Security Forum, (2004). 'Security design patterns', Technical Report G031, The Open Group, Apr. 2004. URL http://www.opengroup.org/publications/catalog/g031.htm, [Accessed: 13/11/2015].

CAMINO (2017). Comprehensive Approach to cyber roadMap coordINation and develOpment, http://www.fp7-camino.eu/ [dernier acces en février 2017]

Chaptal de Chanteloup C., (2015). "La chaîne de valeur de l'offre". Paris, De Boeck.

Choras M., Kozik R., Pilar M., Bruna T., Yautsiukhin A., Churchill A., Maciejewska I., Eguinoa, I., Jomni, A. (2015). Comprehensive Approach to Increase Cyber Security and Resilience - CAMINO Roadmap and Research Agenda, Published in: *Availability, Reliability and Security (ARES), 10th International Conference*, Toulouse, France, 2015

Clarke N. and Furnell S. (2014). *Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014).* Nathan Clarke, Steven Furnell (Eds.), Plymouth, UK, July 8-9, 2014.

Coakes E. (2002). Knowledge Management: A Sociotechnical Perspective *Knowledge Management in the Sociotechnical World*, E. Cokes, D. Willis & S. Clarke (Eds), (Chap 2, p. 4-14). London, Springer-Verlag.

Colas C. et Sarron J.-C. (2009). Résilience des hommes et des systèmes militaires. Document interne, Juillet.

Cranor L.F., Garfinkel S. (2005). *Security and Usability: Designing Secure Systems that People Can Use*, Ed. O'Reilly, ISBN-13: 978-0596008277.

Cranor L., Blase Ur. (2015). Usable Privacy and Security. Lecturer materials, Courses January 2015. Carnegie Mellon University, CyLab. [http://cups.cs.cmu.edu/courses/ups-sp14/]

Cuppens F. (1997). Conception d'Applications Sécurisées. ONERA-CERT, Toulouse.

DCSSI (2009). Fiche d'expression rationnelle des objectifs de sécurité', http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_1982.pdf [Accessed: 14/11/2015].

EBIOS ANSSI, (2016). EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité, https://www.ssi.gouv.fr/guide/ebios-2010-expression- des-besoins-et - identification-des-objectifs-de-securite/ [Dernier accès en septembre 2016]

Emery E. (1967). The next thirty years: concepts, methods and anticipation, *Human relations* #20, p. 199-237.

Engle P. L., Castle S., Menon P. (1996). Child development: vulnerability and resilience. *Social Science and Medicine*, vol. 43, n° 5, 1996, p. 621-635.

European Commission (2009). Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, COM(2009) 149 final (2010/C 255/18).

European Commission (2009). Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, COM(2009) 149 final (2010/C 255/18)

European Commission (2012). Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internet market.

European Commission (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN (2013).

Ferrary M. (2014). *Management des ressources humaines: Marché du travail et acteurs stratégiques*, Ed. Dunod, Paris, France, ISBN-13: 978-2100713172.

Gamma E. Helm R., Johnson R., Vlissides J. (1995). *Design Patterns – Elements of Reusable Object-Oriented Software*. Addison-Wesley.

Giani A., Sastry S., Johansson K., Sandberg H. (2009). The VIKING project: An initiative on resilient control of power networks, *in Proc. Int. Symp. Resilient Control Syst.*, p. 31-35.

Goudalo W., Seret D. (2008). Towards the Engineering of Security of Information Systems (ESIS): UML and the IS Confidentiality. *Proceedings of the 2008, Second International Conference on Emerging Security Information, Systems and Technologies.* p. 248-256. IEEE Computer Society Washington, DC, USA.

Goudalo W., Seret D. (2009). The Process of Engineering of Security of Information Systems (ESIS): The Formalism of Business Processes. *SECURWARE 2009, 3rd International Conference on Emerging Security Information, Systems and Technologies, IARIA*, p. 105-113.

Goudalo W. (2011). Toward Engineering of Security of Information Systems: The Security Acts, *Proc. 5th Int'l Conf. Emerging Security Information, Systems and Technologies, IARIA*, p. 44-50.

Goudalo W., Kolski C. (2016). Towards Advanced Enterprise Information Systems Engineering - Solving Resilience, Security and Usability Issues within the Paradigms of Socio-Technical Systems. *In Proceedings of the 18th International Conference on Enterprise Information Systems (ICEIS 2016)*, vol. 2, p. 400-411, ISBN: 978-989-758-187-8.

Goudalo W., Kolski C., Vanderhaegen F. (2016). Vers une ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience dans les systèmes socio-techniques. Atelier "Sécurité des SI : technologies et personnes", *Inforsid 2016, INFormatique des ORganisation et Systèmes d'Information et de Décision*, Grenoble, France, juin.

Hafiz M., Johnson R.E. (2009). Improving perimeter security with security-oriented program transformations, in *IWSESS'09 Proceedings of the 2009 ICSE Workshop on Software Engineering for Secure Systems*, p. 61-67, IEEE Computer Society Washington, DC, USA.

Hamel G., Välikangas L. (2003). *The quest for resilience.* Harvard Business Review, Sept.

Hansen S., Robertson T., Wilson L., Thinyane H., Gumbo S. (2011). Identifying stakeholder perspectives in a large collaborative project: an ICT4D case study, in *OzCHI'11 Proceedings of the 23rd Australian Computer-Human Interaction Conference*, Pages 144-147, Canberra, Australia, November, ACM New York, NY, USA

Hedrick A. (2007). Cyberinsurance: a risk management tool?, *in InfoSecCD'07 Proceedings of the 4th Annual Conference on Information Security Curriculum Development*, Article No. 20, Kennesaw, Georgia, September 2007, ACM New York, NY, USA

Hollnagel E., Woods D. D., Leveson N. (2006). *Resilience Engineering. Concepts and Precepts*, Ashgate, Aldershot

HSC - Hervé Schauer Consultants (2011). Normes en Sécurité. http://www.hsc.fr/ressources/presentations/normesISO-SSI2-11/normesISO-SSI2-11.pdf.

IBM Corporation (2014). Understanding big data so you can act with confidence. Produced in USA, Copyright IBM Corporation, June 2014.

IRIS (2016). Infrastructure for Resilient Internet Systems project. https://pdos.csail.mit.edu/archive/iris/ [Dernier accès en novembre 2016]

ISO/IEC 9126 (1991). Software product evaluation - Quality characteristics and guidelines for their use.

ISO 9241-11 (1998). Part 11 : Guidance on usability.

ISO/IEC 2700x (2010). Information technology Security techniques.

ISO/IEC FDIS 9126-1 (2000). Software Engineering - Product quality - Part 1: Quality model.

Jaeger T. (2016). Configuring Software and Systems for Defense-in-Depth, in SafeConfig'16 Proceedings of the *ACM Workshop on Automated Decision Making for Active Cyber Defense*, p. 1-1, Vienna, Austria, October 2016, ACM New York, NY, USA ©2016.

KPMG International (2014). Managing the data challenge in banking. Why is it so hard?, published on June 2014, http://www.kpmg.com.

Kumar D., Ramakrishnan N., Helm R. F., Potts M. (2006). Algorithms for storytelling, *KDD'06 Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, p. 604-610, Philadelphia, PA, USA, August, ACM New York, NY, USA.

Laprie JC. (2008). About Resilience - From Dependability to Resilience. *IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance, 54th meeting*, Alyeska, Alaska, USA.

Lewis J.R. (2014). Usability: Lessons Learned… and Yet to Be Learned', *International Journal of Human-Computer Interaction*, vol. 30, n° 9, p. 663-684.

Luzeaux D. (2011). Ingénierie des grands systèmes complexes. *Maîtrise de l'ingénierie des systèmes complexes et des systèmes de systèmes*, Luzeaux D., Ruault J.-R. & Wippler J.-L. (Eds.), Hermes-Lavoisier, Paris.

Mahatody T., Sagar M. Kolski C. (2010). State of the Art on the Cognitive Walkthrough method, its variants and evolutions, *International Journal of Human-Computer Interaction*, vol. 26, n° 8, p. 741-785.

Murphy D.R., Murphy R.H. (2013). Teaching Cybersecurity: Protecting the Business Environment, in *InfoSec CD'13 Proceedings of the 2013 on InfoSec CD'13: Information Security Curriculum Development Conference*, Kennesaw GA, USA, October 12.

Musman S. (2016). Assessing Prescriptive Improvements to a System's Cyber Security and Resilience, *Published in IEEE Annual Systems Conference (SysCon'16)*, Orlando, Florida.

Ouedraogo K., Enjalbert S., Vanderhaegen F. (2013). How to learn from the resilience of Human-Machine Systems? *Engineering Applications of Artificial Intelligence*, vol. 26, n° 1, p. 24-34.

Palin P.J. (2013). Resilience: Cultivating the virtue. Internet resources http://www.hlswatch.com/2013/08/29/resilience-cultivating-the-virtue/. [accessed 22.07.2016]

Pavel D., Holweg M., Trossen D. (2013). Experiencing your life: increasing self-awareness through a story-inspired paradigm, in *Pervasive Health'13 Proceedings of the 7th International Conference on Pervasive Computing Technologies for Healthcare*, Venice, Italy, May, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) ICST, Brussels, Belgium, p. 311-312.

Piètre-Cambacedes L. (2010). Des relations entre sûreté et sécurité. Thèse de Doctorat, Télécom ParisTech, Paris

Ponemon Institute LLC (2015). Cost of Data Breach Study: Global Analysis. Benchmark research sponsored by IBM, Independently conducted by Ponemon Institute LLC, May.

Porter M., (1986). "L'avantage concurrentiel". Paris, InterEditions

RAMBO (2012). Resilient Architectures for Mission Assurance and Business Objectives Project, under FY11 MITRE Innovation Program. Deb Bodeau, Rich Graubart, Len LaPadula, Peter Kertzner, Arnie Rosenthal, Jay Brennan. Cyber Resiliency Metrics. The MITRE Corporation, Project No: 05MSR160-JT, April.

Rao K. (2006). Storytelling and puzzles in a software engineering course. *SIGCSE'06 Proceedings of the 37th SIGCSE technical symposium on Computer science education*, p. 418-422, Houston, Texas, USA, March, ACM New York, NY, USA

ReSIST (2015). Resilience for Survivability in IST. A European Network of Excellence, http://www.resist-noe.org [Dernier accès en novembre 2015]

Romanosky S. (2016). Examining the Costs and Causes of Cyber Incidents. (http://cybersecurity.oxfordjournals.org/) (2016) [Lastest access in octobre 2016]

Ruault J., Kolski C., Luzeaux D., Vanderhaegen F., Goudalo W. (2016). Résilience intégrée de la sécurité et de la sûreté des systèmes, Surveiller le système et alerter les opérateurs pour naviguer à vue. *Génie Logiciel*, 117, p. 2-12.

Rousseau DM, SitkinS, B, Burt R.S., Camerer C. (1998). Not So Different After All: A Cross-Discipline View Of Trust, *Academy of Management Review*, vol. 23, n° 3 p. 393-404.

Salehie M., Ali R., Omoronyia I., Nuseibeh B. (2012). On the role of primary and secondary assets in adaptive security: an application in smart grids, *in SEAMS'12 Proceedings of the 7th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, p. 165-170, Zurich, Switzerland, June, IEEE Press Piscataway, NJ, USA

Salloway A., Trott J.R. (2002). *Design patterns par la pratique*, Eyrolles, Paris.

Sasse M.A. (2007). Red-Eye Blink, Bendy Shuffle, and the Yuck Factor: A User Experience of Biometric Airport Systems, *IEEE Security & Privacy*, vol. 5, n° 3, May/June 2007, p. 78-81.

SBIC - Security for Business Innovation Council, (2008). *The Time is now: making information security strategic to business innovation,* RSA Security, Bedford MA.

Schneider FB (1998). *Trust in Cyberspace', Committee on Information Systems Trustworthiness*, National Research Council, Washington, D.C.

Schumacher M. (2003). *Security engineering with patterns: origins, theoretical models, and new applications,* Springer, 2003, LCNS 2754

Seffah A., Donyaee M., Kline R.B., Padda H.K. (2006). Usability measurement and metrics: A consolidated model, *Software Quality Journal*, vol. 14, p. 159-178.

Shackel B. (2009). Usability - Context, Framework, Definition, Design, and Evaluation, *Interacting with Computers archive*, vol. 21 n° 5-6, December, p. 339-346.

Singh M.P. (2013). Norms as a basis for governing sociotechnical systems. *ACM Transactions on Intelligent Systems and Technology (TIST) - Special Section on Intelligent Mobile Knowledge Discovery and Management Systems and Special Issue on Social Web Mining archive*. vol. 5, n° 1, December, New York, NY, USA.

Sperber D., Wilson D. (1995). *Relevance: Communication and Cognition*, 2nd Edition, ISBN: 978-0-631-19878-9, December 1995, Wiley-Blackwell.

Stanford Encyclopedia of Philosophy (2016). Seneca, chapter the Vertue. Internet resources http://plato.stanford.edu/entries/seneca/#Vir [accessed 22.07.2016]

Trist E.L., Higgin G.W., Murray H., Pollock A.B. (1963). *Organizational Choice: Capabilities of Groups at the Coal Face Under Changing Technologies. The Loss, Rediscovery & Transformation of a Work Tradition.* Tavistock Pubs, London.

Umhoefer C, Rofé J., Lemarchand S (2014). Le big data face au défi de la confiance, Document published on June 2014 http://www.bcg.fr, [Accessed: 13/11/2015].

Vanderhaegen F. (2010). Human-error-based design of barriers and analysis of their uses, *Cognition Technology & Work*, vol. 12, n° 2, p. 133-142.

Westin A. (1970). *Privacy and Freedom*; 19C7. The Bodley Head Ltd, First Edition of hardcopy April 16.

Wharton C., Rieman J., Lewis C., Polson P. (1994). The cognitive walkthrough method: A practitioner's guide, *Usability Inspection Methods*, J. Nielsen & R. L. Mack (Eds.), John Wiley & Sons, New York, p. 105-140.

Woods D.D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety*, 141, p. 5-9 Elsevier Ltd.

Yee K.P. (2002). User Interaction Design for Secure Systems, *Proc. 4th International Conference on Information and Communications Security*, Springer-Verlag, p. 278-290.

Yeo M. L., Rolland E., Ulmer J. R., Patterson R. A. (2014). Risk Mitigation Decisions for IT Security, in *Journal ACM Transactions on Management Information Systems (TMIS)* TMIS Homepage archive, vol. 5, n° 1, April, Article n° 5, ACM New York, NY, USA.

Zhu Q., and Basar T. (2015). Game-Theoretic Methods for Robustness, Security, and Resilience of Cyberphysical Control Systems: Games-in-Games Principle for Optimal Cross-Layer Resilient Control Systems, *IEEE Control Systems*, vol. 35, n° 1, Feb., p. 46-65.