Vers une ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience dans les systèmes socio-techniques

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, ABE - Advanced Business Engineering
77400 Lagny, France
wilson.goudalo@abe-engineering.net

RESUME. *A l'ère actuelle de l'industrie des services, les activités de conception de services (produits, systèmes) arbitrent en permanence avec les principes de "time to market", de la performance, la sécurité, la fiabilité, la robustesse, la flexibilité, l'adaptabilité, la convivialité, le respect de la vie privée, la traçabilité, la conformité, la transparence, dans le but de satisfaire les préoccupations de toutes les parties prenantes. Dans ce travail nous proposons de traiter les préoccupations relatives aux principes cités, ci-dessus, dans une perspective commune de la sécurité, de l'utilisabilité et de la résilience. Nous la désignons par l'ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience. Nous avons élaboré une étude de cas de système socio-technique dans le domaine de la santé qui illustre nos propositions.*

ABSTRACT. *In the current era of the service industry, design activities of services (products, systems) constantly mediate with the principles of "time to market", performance, security, reliability, robustness, flexibility, adaptability, usability, privacy, traceability, compliance, transparency, in order to satisfy the concerns of all stakeholders. In this work, we propose to address all these concerns and principles mentioned above, in a joint perspective of security, usability and resilience. We designate it by the joint engineering of security, usability and resilience. We developed a case study which shores our results.*

MOTS-CLES : *Sécurité ; Utilisabilité ; Résilience ; Sémantique ; Métrique ; Modèle Conceptuel ; Analyse Conjointe ; UML.*

KEYWORDS: *Security; Usability; Resilience; Semantics; Metrics; Conceptual Models; Joint Analysis; UML.*

1. Introduction

Autrefois, les systèmes étaient développés pour des utilisateurs avertis, dans le cadre d'un contexte bien défini. Ils étaient fournis avec de volumineuses documentations qui ne sont pas toujours agréables 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*", à la fois très concurrentiel et règlementaire. 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). Ils doivent être fiables, protégés et sécurisés de façons efficaces, faciles d'utilisation et résilients. 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%.

Cet article a pour objectif 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. Etat de l'art

2.1. Systèmes socio-techniques

La notion de système socio-technique a été créé dans le cadre des travaux de l'Institut Tavistock de Londres à la fin des années cinquante (Trist and al., 1963). Les systèmes socio-techniques visent à modéliser ensemble les capacités humaines, sociales et technologiques dans l'utilisation et dans le traitement des services à valeur ajoutée. Singh définit les systèmes socio-techniques (SST) comme étant des systèmes physiques (sociaux) et cyber à multiple parties prenantes (Singh, 2013).

De nos jours, les relations sociales sont mélangées avec les relations de type cyber. Les principaux réseaux sociaux en sont une preuve. La consumérisation et les tendances de BYOD ("Bring Your Own Device") rapprochent et mélangent la vie privée et la vie professionnelle. Les SST traitent des données sensibles et fournissent des services de valeur. Au même moment, les utilisateurs adoptent un comportement ubiquitaire et présentent une forte volatilité avec les 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 27000) est dédiée à la sécurité de l'information. 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 traitent également la sécurité, ainsi que les risques de sécurité des SI. Elles opèrent toutes sur ces trois critères fondamentaux de la sécurité. A ces derniers, sont rajoutés différents attributs et propriétés de sécurité tels que la preuve, trace, non-répudiation, identification, authentification que nous suggérons de rassembler pour assurer le concept de l'imputabilité.

Dans les SST, notamment pour le domaine des systèmes médicaux, les attributs du respect de la vie privée et de la confiance se joignent 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.

2.3. 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 9241-11 définit l'utilisabilité et explique les avantages de sa mesure, en termes de performance et de satisfaction des utilisateurs (ISO 9241-11). 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 ses collègues (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.

2.4. Résilience

Des travaux de Laprie (2008) et de 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. Woods (2015) définit quatre principaux axes sous le concept de la résilience : rebond; robustesse; extensibilité gracieuse; l'adaptabilité durable.

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), projet RAMBO (Resilient Architectures for Mission Assurance and Business Objectives dans le cadre du Programme d'innovation FY11 MITRE, initiatives ReSIST (Résilience for Survivability in IST) et les travaux de la Commission européenne sur les questions de résilience (European Commission, 2009 et 2013). Ouedraogo et ses collègues ont proposé des mesures sur la résilience (Ouedraogo et al., 2013).

3. Ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience

Dans cette section, nous proposons nos contributions en termes d'ingénierie conjointe opérant, d'une part sur la sécurité, l'utilisabilité et la résilience, et d'autre part sur leurs corrélations réciproques. Nous présentons, ci-dessous, l'analyse conjointe (le modèle conceptuel, les concepts, les sémantiques et les métriques) et les actes d'ingénierie conjointe (activités et tâches).

3.1. Modèle conceptuel

Nous suggérons le modèle conceptuel visible en Figure 1 qui est le résultat de l'analyse conjointe de la sécurité, de l'utilisabilité et de la résilience. Ses éléments constitutifs sont détaillés dans les paragraphes suivants.

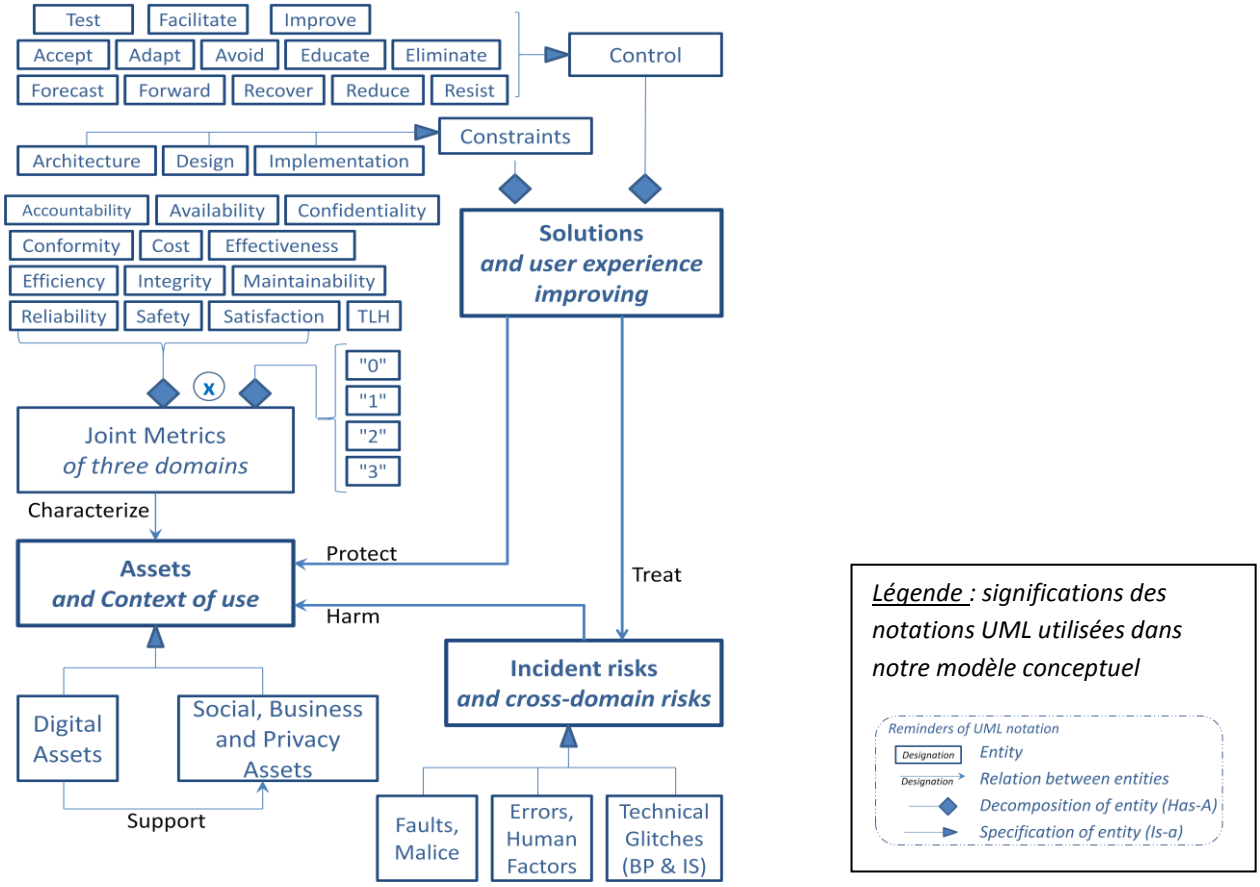

Figure 1. Modèle conceptuel de l'ingénierie conjointe

3.2. Concepts et sémantiques

Les principaux concepts et sémantiques utilisés dans le modèle conceptuel proposé sont les suivants :

- *Assets*. 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 organisation) qui sont nécessaires pour la réalisation des objectifs de l'entreprise. 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 réalisation et utilisation correctes. Les actifs constituent les principaux éléments que la sécurité doit protéger. Les actifs sont traités 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.
- *Incident risks*. Les risques d'incident mettent en péril les actifs. Les risques sont spécialisés en fautes et malversations (commises délibérément par des hackers et des personnes malveillantes), en erreurs dues à des facteurs humains (difficultés d'utilisation, inadvertances, ingénierie sociale) et en problèmes techniques (sur les processus d'entreprise, les procédures, les composants matériels, les composants logiciels et matériels. 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.
- *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 (cross-domain). Les solutions traitent les risques d'incidents et ils 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, 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 autre : Accepter, Adapter, Améliorer, Eduquer, Eliminer, Eviter, Faciliter, Prévenir, Recouvrer, etc.

3.3. Métriques

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 les trois principales entités.

- 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 cross-domain. Les attributs identifiés sont les treize critères indiqués sur la figure (Imputabilité, Disponibilité, Confidentialité, Niveau de tolérance de préjudice ou TLH - Tolerance level of harm, Satisfaction, Sûreté et les autres). 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", "Elevé - 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. 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. Ces quatre niveaux de solutions sont: «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. Le développement de ces heuristiques mérite de faire l'objet d'un autre travail de recherche. Nous proposons à ce sujet ci-dessous quelques actes (activités et/ou tâches) représentatifs qui accompagnent l'analyse conjointe dans le cadre de l'ingénierie conjointe (de la sécurité, de l'utilisabilité et de la résilience).

3.4. Vers les actes de l'ingénierie conjointe

Nous proposons ici quelques 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 ; Evaluer 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, ...) ; Identifier et analyser les risques cross-domain (sécurité, utilisabilité et résilience) ; 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.

4. Etude de cas

4.1. Définition du périmètre de l'étude de cas

L'étude de cas est liée au SI d'un laboratoire médical 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 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. Cela dépend de l'authentification de l'utilisateur et de 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, ci-dessous, 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, ...), 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 quatre tableaux synthétisant respectivement : trois processus d'entreprise (business process) 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 fournis ici par manque de place et seront présentés durant l'atelier.

5. 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). Aujourd'hui, nous vivons déjà les systèmes ubiquitaires émergents et *transhumanistes (H+)* qui ont été promis. 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. Une autre forme d'ingénierie de sécurité avancée doit être conçue pour faire face à ce nouveau dilemme. Nous nous sommes efforcés de fournir notre contribution en suggérant cette analyse conjointe de l'utilisabilité, de la sécurité et de la résilience. Une étude de cas a illustré l'approche proposée.

Nos futurs travaux porteront sur le développement des actes de sécurité avancés qui opèrent sur le modèle conceptuel proposé, dans le but d'étoffer l'ingénierie conjointe de la sécurité, de l'utilisabilité et de la résilience.

Bibliographie

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

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.

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

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, (2013). "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". JOIN (2013) 1 final.

Goudalo W. and 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. Pages 248-256. IEEE Computer Society Washington, DC, USA.

Goudalo, W. and 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) - Volume 2, pages 400-411, ISBN: 978-989-758-187-8

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

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

ISO 9241-11, "Part 11 : Guidance on usability", 1998.

ISO/IEC 27000:201i Information technology -- Security techniques.

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, 2008.

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

Ouedraogo K., Enjalbert S., Vanderhaegen F. (2013). How to learn from the resilience of Human-Machine Systems? Engineering Applications of Artificial Intelligence, volume 26, issue 1, pp. 24-34, 2013.

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

RAMBO (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 2012.

ReSIST (Resilience for Survivability in IST). [http://www.resist-noe.org/].

Shackel B, (2009). "Usability—Context, Framework, Definition, Design, and Evaluation", Interacting with Computers archive, Volume 21 Issue 5-6, December, 2009, Pages 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. Volume 5 Issue 1, December 2013. New York, NY, USA.

Trist E.L., Higgin G.W., Murray H., and 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, 1963.

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

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